Facultad de Matemáticas
Departamento de Álgebra

Capítulo 1

Visión de conjunto sobre códigos y cuerpos finitos

En estas notas hacemos una exposición rigurosa de parte de la teoría de códigos correctores de errores. Habrá teoremas de teoría de códigos, los necesarios. Habrá, sobre todo, aplicaciones prácticas de los teoremas en forma de programas Maple.

La teoría de códigos correctores de errores tiene dos fundamentos matemáticos esenciales:

1. el álgebra lineal elemental
2. la aritmética, en particular la de cuerpos finitos.

El primer requisito los damos por supuesto. Toda persona que haya estudiado un primer año de ciencias o técnicas, en la Universidad, ha pasado necesariamente por un curso de álgebra lineal, que le es más que suficiente para entender lo que vamos a explicar.

Un tema más vidrioso ha sido el de los cuerpos finitos. Son extraordinariamente sencillos para trabajar con ellos, y muy agradables para programar. Se les puede describir muy bien con palabras del lenguaje ordinario. Sin embargo, dar una fundamentación rigurosa requiere "muchas palabras matemáticas". Hemos tomado una solución salomónica. En este texto el manejo de los cuerpos finitos está explicado sobre la marcha, sin datos técnicos ningunos, con profusión de programas Maple para poder calcular lo que se desee. Se explica un uso exclusivamente práctico. Aún así hemos añadido una parte en que la fundamentación matemática se expone de manera rigurosa, con la escrupulosidad propia de esta disciplina. Así pues, a quien

UNIVERSIDAD DE SEVILLA

le interese sólo el manejo (es decir, el "cómo"), olvide la parte de fundamentación; quien quiera saber el "porqué" debe leerla.

1.1. Los problemas a abordar

En estas notas vamos a tratar algunos problemas de almacenamiento y transmisión de la información, en el aspecto de la corrección de los errores que se producen en el proceso de transmisión.

Suponemos una situación en la que se está produciendo una cierta cantidad de información. Para su manejo informático, debemos proceder a los siguientes pasos:

1. Diseñar un alfabeto y un procedimiento para escribir la información como palabras sobre el alfabeto.

2. Una vez escrita la información, hay que almacenarla o transmitirla a través de un canal. En verdad, desde el punto de vista teórico, ambos procesos se confunden, pues almacenar es transmitir desde una unidad de memoria (quizás la interna de un computador) a un medio físico.

3. Después viene un proceso de recuperación de las palabras en que hemos escrito la información, bien del medio físico en que están almacenadas, bien del extremo receptor del canal utilizado.

4. Finalmente viene un proceso de lectura, o sea, interpretación de las palabras, para recuperar la información original.

En estas notas no nos vamos a ocupar de nada de eso, salvo ocasionalmente (y en ejemplos), de alfabetos y escritura de la información. Nuestro objetivo es otro.

Nuestro punto de partida son las palabras. En el proceso de transmisión y recuperación se producen errores. Nosotros vamos a ocuparnos del problema de recuperar la palabra original transmitida a partir de la recibida, que posiblemente no sea igual que aquélla. Éste es un problema real de la máxima actualidad. ¿Nos hemos preguntado por qué se oye tan bien un CD de audio o se ve perfectamente uno de vídeo (DVD)?. Aún suponiendo que las palabras en que están escritos los sonidos y las imágenes estén correctamente grabadas en el CD[1], en la lectura en nuestro equipo casero habrá grandes cantidades de errores: suciedad del CD o del lector, variaciones

[1]Jamás haremos esta suposición: es irreal. También en el proceso de grabación se producen errores.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

infinitesimales de la tensión eléctrica, y un largísimo etcétera. ¿Por qué no se oyen ruidos de fondo o se ven perturbaciones de la imagen? La respuesta es que, aparte de las palabras grabadas en el CD, también hay grabadas "muchas Matemáticas" que permiten corregir. El cómo corrigen las Matemáticas es el objeto de estas notas.

Así pues, nuestro esquema es teóricamente simple: tenemos palabras transmitidas, palabras recibidas y hemos de "crear Matemáticas" para identificar las primeras a partir de las últimas. Otra tarea es implementar en un computador los algoritmos en los que actúan "esas Matemáticas". Trataremos este último aspecto extensamente, pero no a nivel productivo. Es decir, en estas notas se encontrarán algoritmos que harán todo lo que se dice teóricamente. Estarán escritos en lenguaje Maple. Servirán para el estudio, es decir, para que se comprendan bien los conceptos explicados. Sin embargo, no se podrán utilizar en la vida real, porque serán, en general, demasiado lentos. La implementación de estos algoritmos "en la realidad" requiere, ante todo, un lenguaje de programación compilado ultrarápido y un diseño de estructuras de datos que den primacía a la velocidad. Porque, sin dudarlo, el problema es la velocidad de proceso.

En resumen, en este libro crearemos las Matemáticas que corrigen, y las implementaremos en algoritmos para la enseñanza.

1.2. ¿Por qué los cuerpos finitos?

Tratemos un momento de las palabras en que se escribe la información existente. Necesitamos, lo pimero, un alfabeto. Si la información a transmitir o a almacenar fuese recopilaciones de textos legales, podríamos pensar en el alfabeto ordinario. Pero sería una mala idea porque, ¿cómo podríamos hacer actuar las Matemáticas sobre el alfabeto ordinario? Necesitamos alfabetos en que las Matemáticas puedan operar con las letras. Para ello, la primera intuición (¡y la buena!) es volverse hacia la aritmética. La pregunta es: ¿aritmética de los enteros?

Vamos a ver si es buena idea usar la aritmética de enteros. Siguiendo con el ejemplo de los textos legales, la cuestión sería traducir las letras a números. Pongamos un ejemplo, que supone una simplificación enorme. Supongamos que escribimos sólo con letras minúsculas, sin signos de puntuación, y sin números. Hagamos una tabla sencilla de traducción:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

ñ	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26

En principio, no hemos hecho más que cambiar las letras de nombre. Si queremos introducir las Matemáticas, necesitamos poder usar la cuatro reglas básicas de la aritmética sobre las letras: suma, resta, multiplicación y división. Aquí vemos que no podemos: la suma de dos letras puede no ser una letra. Por ejemplo, si queremos sumar "s" con "t" tomamos $19 + 20 = 39$, que no es una letra.

Sin embargo, las Matemáticas proveen solución. Interpretamos los números del 0 al 26 como congruencias módulo 27. En congruencias, sumar y multiplicar consiste en hacerlo como enteros ordinarios, y dar como resultado el resto de dividir por el módulo. Por ejemplo, como congruencias módulo 27, $19 + 20 = 12$ y $3 \cdot 9 = 0$. Esto significa que, módulo 27, no hay más que 27 congruencias, numeradas del 0 al 26 (que son los restos posibles). Así, la suma, la diferencia y el producto de dos letras es simpre una letra. La aritmética modular (es decir, la de congruencias), lleva trazas de arreglar nuestro problema. Sin embargo, en nuestro ejemplo con congruencias, no podemos en general dividir letras. Vamos a ver que no podemos dividir b entre d, es decir, 1 entre 3. Dividir 1 entre 3 sería hallar una congruencia x tal que $3x = 1$. Vamos a ver que esta congruencia no existe, multiplicando 3 por cada una de las congruencias existentes en las dos tablas siguientes:

$x =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$3 \cdot x =$	0	3	6	9	12	15	18	21	24	0	3	6	9	12

$x =$	14	15	16	17	18	19	20	21	22	23	24	25	26
$3 \cdot x =$	15	18	21	24	0	3	6	9	12	15	18	21	24

Vemos que, en las segundas líneas de cada una de las tablas, donde están los resultados de $3x$ no aparece el 1 por parte alguna. Sin embargo, hay congruencias por las que sí se puede dividir. Por ejemplo, $1/4 = 7$ porque, en enteros, $7 \cdot 4 = 28 = 1 \cdot 27 + 1$, luego en congruencias, $4 \cdot 7 = 1$. Esto de que a veces se puedan dividir congruencias y a veces no, no es nada bueno para aplicar las Matemáticas. hay que ingeniárselas de otras formas.

Las congruencias son algo que conocen bien quienes han estudiado un primer curso universitario de ciencia o técnica. No obstante, la referencia universal para

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

congruencias de enteros (y de polinomios, que vamos a tratar en un momento), es la sección 4.4 y siguientes. Aquí nos bastará decir que, fijado un módulo m, las congruencias son los números $\{0, 1, \ldots, m-1\}$ con las reglas de operación siguientes: para sumar o multiplicar dos congruencias, se suman o multiplican los enteros correspondientes y se da como resultado el resto de dividir por m. Cada entero poseee una congruencia asociada, que es el resto de dividirlo por m, como veremos ampliamente en ola sección 4.4.

Un cuerpo es una entidad en la que se puede sumar, restar, multiplicar y dividir por elementos distintos de cero. Es bien conocido que las congruencias de enteros forman un cuerpo si y sólo si el módulos es primo (cf. teorema 4.4.5). Así, una posible solución para nuestro problema sería añadir dos "letras" más, el espacio en blanco separador de palabaras con el número 27 y el punto con el 28. De esta forma tendríamos las congruencias módulo 29 que ya forman un cuerpo por ser 29 un número primo. Los cuerpos de congruencias de enteros se llaman *cuerpos primos*.

1.3. Cuerpos finitos no primos

Sin embargo, hay soluciones más astutas al problema de las letras de la sección 1.2, provistas por las congruencias polinómicas, que también son conocidas por quienes han estudiado un primer curso de universidad. La referencia que arregla las deficiencias es el teorema 6.2.3 y resultados siguientes de esa sección, junto con un capítulo sobre cuerpos finitos que le sigue.

¿Qué son las congruencias polinómicas? Formalmente algo análogo a las enteras, como vamos a ir explicando. Partamos de un cuerpo de congruencias de enteros, y vayamos introduciendo notaciones. Las congruencias de enteros módulo $p > 0$ se designan por $\mathbb{Z}/\mathbb{Z}\,p$. Si p es primo, $k = \mathbb{Z}/\mathbb{Z}\,p$ es un cuerpo. Tomamos una indeterminada X y consideramos el conjunto $R = (\mathbb{Z}/\mathbb{Z}\,p)[X] = k[X]$ de los polinomios en X con coeficientes en k. Se pueden sumar, restar y multiplicar polinomios. También hay una división de polinomios, pero (al igual que en los enteros), no da un general un polinomio, sino un cociente y un resto. El resto es, bien cero, bien de grado estrictamente menor que el divisor.

Pongamos un ejemplo, que nos permitirá ir introduciendo programas Maple. Sea $k = \mathbb{Z}/\mathbb{Z}\,3$ y consideremos en $k[X]$ los polinomios $f = X^3 + 2\,X^2 + X + 1$, $g = 2\,X^2 + X + 1$; la división es:

$$X^3 + 2\,X^2 + X + 1 = (2\,X)(2\,X^2 + X + 1) + (2\,X + 1)\,,$$

donde $2\,X$ es el cociente y $2\,X + 1$ el resto.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

En el teorema 6.1.2 damos el algoritmo general mediante el que se calculan cociente y resto de polinomios en la división ordinaria. Ese algoritmo es directamente programable en Maple, como se ve fácilmente. Al programarlo, damos a la función que lo realiza un nombre , por ejemplo, `divpolcp`. Esta función toma tres argumentos: el dividendo, el divisor y el primo que marca el módulo. En nuestro caso, la llamada a la función se efectuaría así:

```
> divpolcp(X^3+2*X^2+X+1,2*X^2+X+1,3,X);
```

y obtendríamos como respuesta una lista de dos polinomios: cociente y resto. En nuestro caso la respuesta sería:

$$[2\,X, 2\,X + 1]\,.$$

Ya que podemos escribir un programa que divide polinomios sobre un cuerpo de la forma $k = \mathbb{Z}/\mathbb{Z}\,p$, decimos brevemente algo sobre divisibilidad. En $k[X]$ hay polinomios irreducibles, que son los que no se pueden escribir como producto de dos polinomios de grados estrictamente menores que el dado. Más aún, todo polinomio de $k[X]$ se descompone en producto de factores irreducibles. Esta descomposición la calcula el sistema Maple con la orden `Factors`. Por ejemplo, si continuamos con $k = \mathbb{Z}/\mathbb{Z}\,3$, la sesión

```
> Factors(2*X^9-2*X) mod 3;
                                  2
[2, [[X + 1, 1], [X + 2, 1], [X  + 2 X + 2, 1],
   2                 2
 [X  + X + 2, 1], [X  + 1, 1], [X, 1]]]
```

produce una respuesta enrevesada que vamos a aclarar. Tratamos de descomponer $2\,X^9 - 2\,X$ en producto de factores irreducibles en $(\mathbb{Z}/\mathbb{Z}\,3)[X]$. El algoritmo interno de Maple da una respuesta que es una lista. Como actúa sobre polinomios mónicos (coeficiente de la máxima potencia igual a 1), el primer elemento de la lista es el coeficiente de la máxima potencia sacado factor común. Los restantes elementos de la lista son listas de dos elementos: el factor irreducible y su exponente (multiplicidad). O sea, en nuestro caso

$$2\,X^9 - 2\,X = 2\,(X+1)(X+2)(X^2+2\,X+2)(X^2+X+2)(X^2+1)\cdot X\,.$$

No hay problema cuando aparecen factores múltiples: el entero que va con cada sublista indica la multiplicidad. Por ejemplo, la sesión

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

```
> h := 2*X^5+2*X^4+2*X^3+X^2+X+1:
> Factors(h) mod 3;
                          [2, [[X + 2, 5]]]
```

significa que, en $(\mathbb{Z}/\mathbb{Z}\,3)[X]$, es

$$2\,X^5 + 2\,X^4 + 2\,X^3 + X^2 + X + 1 = 2\,(X+2)^5\,.$$

Sea $m(X) \in k[X]$ un polinomio cualquiera, de grado $e > 0$. Como en enteros, definimos una *congruencia* en $k[X]$ como el conjunto de los polinomios que al dividirlos por $m(X)$ dan un resto fijo. Como en los enteros, representamos cada congruencia por su resto. Por ejemplo, si $m(X) = X^3 + 2\,X^2 + 1 \in (\mathbb{Z}/\mathbb{Z}\,3)[X]$, la congruencia que contiene al polinomio $X^{99} + X^{98}$ es

```
> divpolcd(X^99+X^98,X^3+2*X^2+1)[2];
                                 2
                              X + 2 X
```

es decir, es la congruencia $X^2+2\,X$. Hay que notar que hemos seleccionado, mediante `[2]`, el segundo elemento de la lista de salida de `divpol`. El primero es el cociente y nos nos interesa en este aspecto.

La primera consecuencia de esto es que cada congruencia, al venir representada por su resto módulo $m(X)$, aparece como un polinomio de grado $e-1$ a lo sumo. ¿Cuántas congruencias hay? Como un polinomio de grado menor o igual que $e-1$ tiene e coeficientes (¡hay que contar el término independiente!) y cada coeficiente puede tomar p valores, que son las congruencias de $\mathbb{Z}/\mathbb{Z}\,p$, en total hay p^e congruencias en $\mathbb{Z}/\mathbb{Z}\,p[X]$. Su conjunto se representa por $R = k[X]/k[X]\cdot m(X)$, con $k = \mathbb{Z}/\mathbb{Z}\,p$.

Para sumar, restar y multiplicar congruencias, se hace la operación en los restos, como si fuesen polinomios, y se vuelve a tomar el resto si se sobrepasa el grado e. Por ejemplo, para elevar al cuadrado la congruencia anterior tendríamos que

```
> expand((X^2+2*X)^2) mod 3;
                              4    3    2
                             X  + X  + X
```

o sea que, en $(\mathbb{Z}/\mathbb{Z}\,3)[X]$ el polinomio $(X^2+2\,X)^2$ es igual a $X^4+X^3+X^2$. Pero esta representación no nos interesa para las congruencias, porque sobrepasa el grado, 3, del módulo. La representación que necesitamos nos viene, de nuevo, por la división:

```
> divpol(X^4+X^3+X^2,X^3+2*X^2+1)[2];

                                2 X + 1
```

Así, como elementos de R o congruencias, $(X^2+2\,X)^2 = 2\,X+1$.

La notación, en este punto, queda un poco confusa porque representamos de la misma forma a polinomios y congruencias. Para deshacer esta confusión procederamos así: los polinomios se representarán por letras mayúsculas, y las congruencias por la minúscula correlativa. Así, como antes, $(x^2+2\,x)^2 = 2\,x+1$. Pero esto es algo más que una representación: hay que darse cuenta de que $m(x)=0$, es decir, que la congruencia que contiene al módulo es la cero, porque $m(X) = 1\cdot m(X)+0$ es la división. La relación $m(x)=0$ nos permite despejar todas las potencias de x en función de la $e-1$ primeras. El ejemplo anterior, como $x^3+2\,x^2+1=0$, es $x^3 = x^2+2$, luego, por ejemplo:

$$\begin{aligned} 1 &= 1\\ x &= x\\ x^2 &= x^2\\ x^3 &= x^2+2\\ x^4 &= x\cdot x^3 = x(x^2+2) = x^3+2\,x = x^2+2+2\,x\\ x^5 &= x(x^2+2\,x+2) = x^3+2\,x^2+2\,x\\ &= x^2+2+2\,x^2+2\,x = 2\,x+2 \end{aligned}$$

Fácilmente se ve que así se pueden calcular todas las potencias de x en función de $\{1=x^0, x=x^1, x^2\}$.

Al igual que en las congruencias de enteros, el anillo R de las congruencias polinómicas es un cuerpo si y sólo si el módulo $m(X)$ es irreducible en $(\mathbb{Z}/\mathbb{Z}\,p)[X]$. Éste es el caso del ejemplo anterior. La comprobación de que $m(X) = X^3+2\,X^2+1$ es irreducible en $(\mathbb{Z}/\mathbb{Z}\,3)[X]$ se hace inmediatamente con Maple:

```
> Factors(X^3+2*X^2+1) mod 3;
                              3      2
                [1, [[X  + 2 X  + 1, 1]]]
```

El que hay un único factor irreducible, igual al propio polinomio de entrada, indica que éste es irreducible.

Esto arregla el problema de las letras. Teníamos 27 y acabamos de construir un cuerpo con 27 elementos, que es

$$R = (\mathbb{Z}/\mathbb{Z}\,3)[X]/\mathbb{Z}/\mathbb{Z}\,3[X]\cdot(X^3+2\,X^2+1)\,.$$

La lista de sus elementos es:

$$[0, 1, 2, x, x+1, x+2, 2\,x, 2\,x+1, 2\,x+2, x^2, x^2+1, x^2+2, x^2+x,$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$x^2+x+1, x^2+x+2, x^2+2\,x, x^2+2\,x+1, 2\,x+x^2+2, 2\,x^2,$
$2\,x^2+1, 2\,x^2+2, 2\,x^2+x, x+2\,x^2+1, 2\,x^2+x+2, 2\,x^2+2\,x,$
$2\,x^2+2\,x+1, 2\,x^2+2\,x+2]$.

Ahora podemos codificar las letras de otra forma, con los elementos de ese cuerpo, en la forma siguiente:

a	b	c	d	e	f	g	h	i
0	1	2	x	$x+1$	$x+2$	$2\,x$	$2\,x+1$	$2\,x+2$

j	k	l	m	n	ñ
x^2	x^2+1	x^2+2	x^2+x	x^2+x+1	x^2+x+2

o	p	q	r	s	t
$x^2+2\,x$	$x^2+2\,x+1$	$2\,x+x^2+2$	$2\,x^2$	$2\,x^2+1$	$2\,x^2+2$

u	v	w
$2\,x^2+x$	$x+2\,x^2+1$	$2\,x^2+x+2$

x	y	z
$2\,x^2+2\,x$	$2\,x^2+2\,x+1$	$2\,x^2+2\,x+2$

Ahora que tenemos representadas las letras por elementos de un cuerpo, vamos a ver cómo operar con ellas.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

1.4. Maple y cuerpos finitos

En las secciones 1.2 y 1.3 hemos visto cuerpos finitos primos y no primos. Los no primos son cuerpos de congruencias de un anillo de polinomios $k[X]$ con $k = \mathbb{Z}/\mathbb{Z}\,p$.

El resultado sorprendente es que éstos son todos los cuerpos finitos posibles. Esto se demuestra matemáticamente con todo rigor, y no poco esfuerzo. Es el contenido del teorema 6.2.7, cuyo enunciado adelantamos aquí:

Teorema 1.4.1.– *Sea K un cuerpo finito; existe un primo p y un polinomio mónico irreducible $m(X) \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$ tales que K es isomorfo a*

$$(\mathbb{Z}/\mathbb{Z}\,p)[X]/(\mathbb{Z}/\mathbb{Z}\,p)[X] \cdot m(X)\,.$$

Este teorema es uno de los pequeños milagros de las Matemáticas. Se listan todos los posibles objetos de un determinado tipo, en este caso los cuerpos finitos. La manera de hacer esto es un uso muy refinado de la aritmética entera y de polinomios. El sentar las bases para demostrar este teorema, y hacerlo efectivamente, matemáticamente duro. Tendremos ocasión de verlo más adelante.

Ya hemos visto en la sección 1.3 cómo el cuerpo finito

$$(\mathbb{Z}/\mathbb{Z}\,p)[X]/(\mathbb{Z}/\mathbb{Z}\,p)[X] \cdot m(X)$$

tiene p^e elementos, donde e es el grado de $m(X)$. Esto significa que no hay cuerpos finitos con 30 elementos, por ejemplo, pero sí con $32 = 2^5$.

Bueno, ésa es otra cuestión, extraordinariamente interesante. Una cosa es decir que un cuerpo finito tiene p^e elementos y otra completamente distinta es decir que, dado un primo p y un entero positivo e, existe un cuerpo con p^e elementos. La existencia de un cuerpo con p^e elementos es equivalente a la de un polinomio mónico, irreducible, de grado e, en $(\mathbb{Z}/\mathbb{Z}\,p)[X]$. La respuesta es afirmativa, y ésta constituye una de las páginas más bonitas y más sólidas de la aritmética, que veremos en su momento.

Sabiendo que, dados el primo p y el exponente $e > 1$ existen siempre polinomios irreducibles mónicos $m(x) \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$, de grado e, que hacen que

$$(\mathbb{Z}/\mathbb{Z}\,p)[X]/(\mathbb{Z}/\mathbb{Z}\,p)[X] \cdot m(X) = (\mathbb{Z}/\mathbb{Z}\,p)[x]\,, \quad m(x) = 0\,,$$

sea un cuerpo, la cuestión clave es hallar esos polinomios irreducibles. La manera menos complicada de hacerlo es usar Maple para crear un polinomio al azar del grado requerido, y luego aplicarle el test de factorización que vimos en la sección

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

1.3. Esto puede requerir múltiples ensayos porque los polinomios al azar pueden n o satisfacer las condiciones que nosotros les exigimos. Damos un ejemplo de sesión para construir el módulo polinómico para un cuerpo con $2^8 = 256$ elementos. El poder lograr el polinomo satisfactorio que damos nos ha costado 14 ensayos:

```
> f:=randpoly(X,degree=8,dense);

            8     7     6     5      4     3     2
f :=-67-81 X -95 X +63 X -24 X - 63 X -36 X +85 X  +35 X

> f mod 2;

                      8    7    6    4    2

                1 + X  + X  + X  + X  + X  + X

> Factors(f) mod 2;

          [   [[     8    7    6    4    2       ]]]
          [1, [[1 + X  + X  + X  + X  + X  + X, 1]]]
```

A este cuerpo se le llama el *cuerpo de los bytes* porque sus elementos son los polinomios en x de grado 7 a lo más, con coeficientes 0 ó 1. Ordenados, por ejemplo, en grados decrecientes, un polinomio

$$a_0x^7 + a_1x^6 + a_2x^5 + a_3x^4 + a_4x^3 + a_5x^2 + a_6x + a_7$$

$a_i = 0, 1, \forall i = 0, \ldots, 7$ se puede identificar con la lista de 8 bits

$$[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7]\,,$$

que es un byte. Recordemos que

$$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1 = 0\,.$$

A este nivel, y sin más estudios, ¿qué podemos hacer con ese cuerpo? La respuesta es clara: operaciones aritméticas. La operación fundamental es hallar la congruencia de un polinomio, que es el resto de su división por el módulo polinómico

$$m(X) = X^8 + X^7 + X^6 + X^4 + X^2 + X + 1 = 0\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Así por ejemplo, si usamos la función `divpolcp` de la página 6, y teniendo en cuenta que sólo nos interesa la segunda componente de la salida, vemos que la congruencia de x^{10000} es

```
> divpolcp(x^10000,x^8+x^7+x^6+x^4+x^2+x+1,2,x)[2];
                          4
                         x
```

Esto significa que x^{10000}, expresado como combinación lineal de las primera potencias, es x^4. Ya se puede sumar y multiplicar elementos del cuerpo de los bytes, sumando o multiplicando los polinomios corrrespondientes y hallando el resto de dividir por $m(X)$. La división de elementos dentro del cuerpo de los bytes es más complicada. Por ahora nos contentaremos con el método más grosero: para hallar $1/\alpha$, donde α es un byte, se multiplica α ordenadamente por los otros bytes hasta que encontremos aquél que nos dé 1.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 2

Códigos: primeros pasos

En el capítulo 1 desarrollamos apenas unas ideas sencillas, de las apuntadas en la sección 1.1. Se pueden resumir estas ideas en los puntos siguientes:

1. Necesitamos un alfabeto con el que escribir palabras que traduzcan la información que poseemos.
2. Este alfabeto debe ser algo con lo que se pueda operar matemáticamente en un computador.
3. La solución es utilizar como símbolos del alfabeto los elementos de un cuerpo finito adecuado.
4. Los cuerpos finitos se pueden manejar con Maple.

En el presenta capítulo vamos a abordar la construcción de palabras con nuestro alfabeto, siempre sin perder de vista el objetivo básico: corregir errores de transmisión.

2.1. Las palabras

Nos colocamos en un plano muy general. En el lenguaje natural, cuando el alfabeto es el ordinario, hay palabras de distinta longitud (de distinto número de letras). Esto no ocurre en teoría de códigos. Igualamos la longitud de las palabras a utilizar introduciendo, si es necesario, "caracteres nulos" para completar. Esto equivaldría, en el ejemplo del lenguaje natural, a tomar la palabra más larga del diccionario

UNIVERSIDAD DE SEVILLA

y a igualar el número de letras de las demás por la adición a la derecha de esos caracteres nulos.

Fijada una longitud n de palabras (la máxima en el idioma castellano, si se quiere), no cualquier combinación de n letras significa algo, es decir, contiene información. Sólo las que figuran en el diccionario tienen contenido semántico. El diccionario es un código, porque con sus palabras se escribe la información de la cultura humana. La situación con los computadores es análoga.

Definición 2.1.1.– *Un alfabeto es un conjunto finito de símbolos. Si $\mathcal{A}$ es un alfabeto, se designará por $\mathcal{A}^n$ al conjunto de las sucesiones de n elementos de $\mathcal{A}$, que se llaman las palabras de longitud n construidas con el alfabeto $\mathcal{A}$. Se llama un código a todo subconjunto de $\mathcal{P}(\mathcal{A})$.*

Ejemplo 2.1.2.– Hace años, los españoles estábamos identificados por un código, que era un simple número, el del Documento Nacional de Identidad. El alfabeto eran los dígitos del 0 al 9 y las palabras tenían longitud 8. ASí, el número más alto de DNI era 99,999,999. Para intentar paliar el problema de los errores en la transmisión del número de DNI[1], sobre todo a efectos fiscales, se creó el llamado NIF (Número de Identificación Fiscal). EL NIF se forma añadiendo al número de DNI algo llamado en teoría de códigos *un byte de paridad*, que en este caso es una letra del alfabeto. Este byte de paridad se añade según la regla siguiente: se divide el número de DNI por 23, produciendo un resto entre 0 y 22. La letra se asigna al resto según la tabla:

resto	letra	resto	letra	resto	letra	resto	letra	resto	letra
0	T	5	M	10	X	15	S	20	C
1	R	6	Y	11	B	16	Q	21	K
2	W	7	F	12	N	17	V	22	E
3	A	8	P	13	J	18	H		
4	G	9	D	14	Z	19	L		

Cuadro 2.1: Letras del NIF

¿Para qué se añade el byte de paridad? Para detectar un error, es decir, para que, si en cualquier proceso de transmisión, se cambia una sola cifra, la letra indique

[1]Transmisión que puede ser, por ejemplo, incluirlo en un formulario que se rellena a mano

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

que esto ha ocurrido. ¿Cuál es la explicación? Cambiar una sola cifra del número significa:

1. si la variación se produce en la primera por la derecha, se añaden o se restan a lo más 9 unidades.

2. si la variación se produce en la segunda por la derecha, se añaden o se restan a lo más 9 decenas.

3. Así sucesivamente hasta las decenas de millón.

Para que una variación de una sola cifra produjese la misma letra, lo que se añade o se quita debería ser mútiplo de 23. Esto no ocurre, porque 23 no puede dividir ni a un número de una cifra, ni a uno de una cifra seguido de ceros. El caso del número de una cifra es evidente. El del número de una cifra seguida de ceros también es sencillo. Basta darse cuenta de que:

1. en la descomposición factorial de un número de una cifra seguida de ceros intervienen sólo los primos $2, 3, 5, 7$,

2. el número 23 es primo, luego no puede dividir al anterior.

En resumen, la no concordancia del byte de paridad significa que se ha cometido un error (¡o más!). La concordancia no significa nada: la trasnmisión ha podido ser correcta o se ha podido cometer más de un error (muy especiales, eso sí, pero posibles). A esto se llama en teoría de códigos detectar un error.

La enseñanza que nos da este ejemplo es que para dar alguna capacidad de reacción frente al error a la información original (número de DNI) hay que añadirle bytes de paridad.

2.2. Las palabras eficaces

Vamos a comenzar con un ejemplo, que es puramente ficticio, al menos en lo que se refiere al tratamiento en España de la situación descrita en él. En un cierto país se efectúa diariamente un sorteo de lotería. El sistema consiste en poner a la venta boletos numerados consecutivamente desde al 00000 hasta el 99999 y sacar por sorteo al azar unos cuantos premios.

La cuestión está en que el centro de lotería tiene una red de puntos de venta dotados de computadores conectados a un ordenador central. Se pretende que cada

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

boleto pueda ser leido en cualquier punto de venta, respondiendo el ordenador central si está o no premiado, y con qué cantidad si lo está. En abstracto, esto implica un tráfico de números entre 00000 y 99999 entre puntos de la red, que puede dar problemas si hay errores. Por tanto, hay que hacer algo con respecto al problema de los errores.

Lo primero a hacer es diseñar un alfabeto y unas palabras en ese alfabeto, de longitud fija, que describan los números de la lotería. Como ya estamos comvencidos de que el alfabeto debe ser un cuerpo finito, para ser operativo, un primo p y un exponente e, para construir un cuerpo de p^6 elementos. Se trata de tomar un número primo bajo (para facilidad de cálculo) y una potencia de él que sobrepase a 100,000, pero no por mucho, para que el código sea lo más compacto posible. Hacemos unos intentos.

$$\begin{array}{rr} 2^{16} = 65536 & 2^{17} = 131072 \\ 3^{10} = 59049 & 3^{11} = 177147 \\ 5^{7} = 78125 & 5^{8} = 390625 \\ 7^{5} = 16807 & 7^{6} = 117649 \end{array}$$

Vemos que la mejor aproximación por exceso de 100,000 lograda con estos ensayos es $7^6 = 117{,}649$, que satisface unas condiciones razonables. Esto significa que vamos a poder escribir nuestros cien mil números de lotería con 7^6 elementos y los restantes representarán boletos nulos.

Tenemos la opción de construir el cuerpo con 7^6 elementos como alfabeto y representar cada número de boleto de lotería por una letra de ese alfabeto. Sin embargo, hay soluciones mejores. El cuerpo con 7^6 es demasiado grande para manipularlo con nuestro modestos medios de cálculo. Parece mejor solución tomar como alfabeto $\mathcal{A}$ el cuerpo k con $7^2 = 49$ elementos y considerar las palabras con tres letras, es decir, los elementos de $\mathcal{A}^3$, para representar nuestros números de lotería.

Aquí entra de lleno el álgebra lineal. Tenemos un cuerpo K con 49 elementos y el espacio vectorial K^3.Vamos a representar algunos números decimales dentro de ese espacio vectorial. El procedimiento es sencillísimo.

Comenzamos con el cuerpo, que debe ser de la forma $k[x]$, donde $k = \mathbb{Z}/\mathbb{Z}7$ y x verifica una ecuación irreducible de segundo grado. Tomamos como ecuación, por ejemplo, $x^2 + 5\,x + 5 = 0$ y preguntamos a Maple si es irreducible:

```
> Factors(x^2+5*x+5) mod 7;

                    [   [[ 2          ]]]
```


Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

```
[1, [[x  + 5 x + 5, 1]]]
```

Como lo es, continuamos. La lista de los elementos del cuerpo $K = k[x]$ con $x^2 + 5\,x + 5 = 0$ es:

$$
\begin{array}{l}
0\,,1\,,2\,,3\,,4\,,5\,,6\,,\\
x\,,x+1\,,x+2\,,x+3\,,x+4\,,x+5\,,x+6\,,\\
2\,x\,,2\,x+1\,,2\,x+2\,,2\,x+3\,,2\,x+4\,,2\,x+5\,,2\,x+6\,,\\
3\,x\,,3\,x+1\,,3\,x+2\,,3\,x+3\,,3\,x+4\,,3\,x+5\,,3\,x+6\,,\\
4\,x\,,4\,x+1\,,4\,x+2\,,4\,x+3\,,4\,x+4\,,4\,x+5\,,4\,x+6\,,\\
5\,x\,,5\,x+1\,,5\,x+2\,,5\,x+3\,,5\,x+4\,,5\,x+5\,,5\,x+6\,,\\
6\,x\,,6\,x+1\,,6\,x+2\,,6\,x+3\,,6\,x+4\,,6\,x+5\,,6\,x+6\,.
\end{array}
$$

Detengámonos a observar con detalle la lista de elementos. Da toda la impresión de que, si en ella, sustituimos las x por 7 obtenemos todos los números, escritos en forma polinómica, con argumento 7, desde 0 a 48. A esto se llama *escribir un número en base* 7. En efecto, sustituyendo x por 7 ordenadamente en la lista anterior, obtenemos los números

$$
\begin{array}{l}
0\,,1\,,2\,,3\,,4\,,5\,,6\,,\\
7\,,8\,,9\,,10\,,11\,,12\,,13\,,\\
14\,,15\,,16\,,17\,,18\,,19\,,20\,,\\
21\,,22\,,23\,,24\,,25\,,26\,,27\,,\\
28\,,29\,,30\,,31\,,32\,,33\,,34\,,\\
35\,,36\,,37\,,38\,,39\,,40\,,41\,,\\
42\,,43\,,44\,,45\,,46\,,47\,,48
\end{array}
$$

Para un programador el construir la lista de elementos de K no es ninguna sorpresa: ha construido la lista de números pasando a base 7 los números decimales desde 0 hasta 48 y luego cambiando 7 por x, es decir, el proceso inverso.

Seguimos con los sistemas de numeración, que parecen dar buen juego. ¿Y si ahora pasamos todos los números desde el 0 hasta el $7^6 - 1 = 117648$ a base 49? Bueno, esto va a rellenar demasiado texto. Nos contentaremos con pasar el mayor, que nos va a dar suficientes pistas: $117649 = 48 + 48 \cdot 7 + 48 \cdot 7^2$. O sea, que al pasar a base 49 los números desde el 0 hasta el 117648, vamos a obtener números de tres cifras siempre, contando con los ceros a izquierda. Cada cifra es menor que 49, luego

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

la podemos pasar a base 7 y obtendremos dos cifras:

$$117684 = (6 + 6 \cdot 7) + (6 + 6 \cdot 7) \cdot 7 + (6 + 6 \cdot 7) \cdot 7^2 \,.$$

Cambiando 7 por x, el número 117648 se escribe como el vector de K^3

$$(6 + 6\,x, 6 + 6\,x, 6 + 6\,x) \in K^3$$

Naturalmente, en este sistema hay números que no corresponden a boletos de lotería, pero todo número de lotería está representado en este sistema. Por ejemplo, ¿qué elemento de K^3 corresponde al número 48231 de boleto? La solución la obtenemos por divisiones sucesivas:

$$\begin{array}{rcl} 48231 & = & 984 \cdot 49 + 15 \\ \dfrac{48231 - 15}{49} & = & 984 = 20 \cdot 49 + 4 \\ \dfrac{\dfrac{a - 15}{49} - 4}{49} & = & \dfrac{48231 - (15 + 4 \cdot 49)}{49^2} = 20 \end{array}$$

luego

$$48231 = 15 + 4 \cdot 49 + 20 \cdot 49^2 = (1 + 2 \cdot 7) + (4 + 0 \cdot 7)49 + (6 + 2 \cdot 7)49^2$$

de donde el número 48231 viene representado por el vector $(1+2\,x\,, 4\,, 6+2\,x) \in K^3$.

Ya están escritos en otra forma los números de la lotería. El código sería aquí el mismo K^3, aunque contuviese palabras carentes de información (es decir, números que no corresponden a boletos). Sin embargo, desde el punto de vista del problema de los errores, no hemos avanzado nada.

2.3. La repetición

La primera idea ingenua que se le ocurre a cualquiera es: si se quiere transmitir el número de lotería 48231, escrito como $(1 + 2\,x\,, 4\,, 6 + 2\,x)$, ¿por qué no transmitirlo repetido? Malo será que, aun habiendo error, no pueda identificar el número en una doble transmisión. Esta idea se formula matemáticamente así: se trasmite el vector

$$(1 + 2\,x\,, 4\,, 6 + 2\,x\,, 1 + 2\,x\,, 4\,, 6 + 2\,x) \in K^6\,,$$

que consta de dos copias del vector original. Ahora los presupuestos varían algo. Ya estamos operando con el conjunto K^6 de las palabras de 6 letras. Este conjunto es

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

un K-espacio vectorial de dimensión 6 y designaremos por $(x_1, x_2, x_3, x_4, x_5, x_6)$ a las coordenadas de un vector genérico. Como cada coordenada puede tomar 49 valores, K^6 tendrá $49^6 = 13841287201$ vectores. Si ese número de vectores fuera tiempo en segundos, representaría casi 439 años.

Sin embargo, no nos interesan todas esas palabras; sólo aquéllas en que las tres últimas coordenadas sean iguales a las tres primeras. Es decir, nuestro código será el subespacio vectorial de K^6 de ecuaciones implícitas:

$$x_4 - x_1 = 0\,,\ x_5 - x_2 = 0\,,\ x_6 - x_3 = 0\,,$$

que es de dimensión 3 y, por tanto, sigue teniendo $49^3 = 117649$ vectores.

Si queremos estar más seguros, podemos tomar más repeticiones, por ejemplo, tres copias del vector original. En lugar de transmitir, como antes, el vector $[1 + 2\,x, 4, 6 + 2\,x]$ lo hacemos con el vector

$$(1 + 2\,x\,, 4\,, 6 + 2\,x\,, 1 + 2\,x\,, 4\,, 6 + 2\,x\,, 1 + 2\,x\,, 4\,, 6 + 2\,x)\,.$$

Ahora estamos en K^9, del cual el código es el subespacio de ecuaciones implícitas:

$$\begin{aligned} x_4 - x_1 = 0\,,\quad x_5 - x_2 = 0\,,\quad x_6 - x_3 = 0 \\ x_7 - x_1 = 0\,,\quad x_8 - x_2 = 0\,,\quad x_9 - x_3 = 0\,, \end{aligned}$$

que sigue teniendo dimensión 3 y 117649 vectores. Es evidente que podemos tomar más y más copias, pero hay dos problemas clave:

1. ¿Hasta dónde permitirá el computador diponible procesar vectores cada vez mayores? Esta pregunta no tiene, evidentemente, respuesta general.

2. ¿Qué se gana con repetir? La solución en la sección 2.4

Terminamos esta sección con una defínción, que delimitará el marco en el que vamos a operar de ordinario.

Definición 2.3.1.– *Sea K un cuerpo finito. Un código lineal $\mathcal{C}$ es un subespacio vectorial de K^n. Al número n se le llama la longitud del código, porque es el número de símbolos del alfabeto que contiene cada palabra. Sea $s = \dim_K(\mathcal{C})$ la dimensión del código; una matriz generadora de $\mathcal{C}$ es cualquier matriz $s \times n$ cuyas filas constituyen una base de $\mathcal{C}$. Si $r = n - s$, una matriz de control o de test de paridad es cualquier matriz N de dimensiones $n \times r$ tal que $\mathbf{x}N = 0$ para cualquier $\mathbf{x} \in \mathcal{C}$. El número r se llama la redundancia del código. Con frecuencia se escribirá traspuesta la matriz*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

de control, simplemente por facilidad tipográfica; en cualquier caso, no habrá posible lugar confusión.

Notas 2.3.2.–

2.3.2.1. Las columnas de una matriz de control de un código son los coeficientes de un sistema de ecuaciones implícitas independientes del código.

2.3.2.2. El nombre de *redundancia* dado al entero r viene de lo siguiente (no perdamos de vista los números de lotería para entender mejor). Las palabras del código son las que contienen información relevante. El código es isomorfo linealmente a K^s. Se encuentra un isomorfismo concreto de manera muy sencilla. Se fija una matriz M generadora del código. La correspondencia

$$(x_1, \ldots, x_s) \longrightarrow (x_1, \ldots, x_s)M$$

es uno de esos isomorfismos. Por tanto, para fijar el código, se necesitan s coordenadas. Las $r = n - s$ restantes son redundancia, es decir, coordenadas extra que se introducen para el tratamiento de los errores.

2.3.2.3. Conservamos una terminología clásica, siguiendo el apartado 2.3.2.2. Fijamos una matriz generadora M de $\mathcal{C}$. Las palabras con la información son las de K^s. El paso de $(x_1, \ldots, x_s) \in K^s$ a $(x_1, \ldots, x_s)M \in K^n$ se llama *codificar la información.* La *descodificación* sería el paso contrario.

2.3.2.4. En el ejemplo de las repeticiones en la lotería, el código es K^3. Cuando repetimos, introducimos una redundancia de 3. En k^6 una matriz generadora del código sería:

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

y una matriz de control

$$N = \begin{pmatrix} 1 & 0 & 0 & 6 & 0 & 0 \\ 0 & 1 & 0 & 0 & 6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 6 \end{pmatrix}$$

donde el superíndice ^{t} representa a la matriz traspuesta[2]. Está claro que $MN = 0$. De forma análoga se operaría con más repeticiones.

[2]La escribimos como traspuesta de una horizontal para ahorrar espacio de texto simplemente

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

2.4. Distancias y bolas

Hay que dar un significado unívoco, no intuitivo sino formal, a los conceptos de detectar n errores o corregir n errores, aunque el "corregir" sea, por ahora, solamente una buena intención. ¿Qué significa que se haya transmitido una palabra y se haya recibido otra con 3 errores? Que la recibida difiere de la transmitida en 3 símbolos. Así, la medida del número de errores es la distancia de Hamming, que definimos a continuación.

Definición 2.4.1.– *Sea $\mathcal{A}$ un alfabeto y $\mathcal{P}_n = \mathcal{A}^n$ el conjunto de palabras de longitud n. Se llama distancia de Hamming (o simplemente distancia porque no se empleará otra) entre dos palabras $\mathbf{a}, \mathbf{b} \in \mathcal{P}_n$ al número de posiciones en que estas palabras difieren (es decir tienen símbolos del alfabeto que son distintos). Si $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$ y designamos por $d(\mathbf{a}, \mathbf{b})$ a la distancia entre $\mathbf{a}$ y $\mathbf{b}$, es*

$$d(\mathbf{a}, \mathbf{b}) = \operatorname{card}\{i \mid 1 \leq i \leq n\,,\ a_i \neq b_i\}\,.$$

Si $\mathcal{C}$ es un código, se llama distancia mínima de $\mathcal{C}$ al número

$$d(\mathcal{C}) = \min\{d(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{C}\,, \mathbf{a} \neq \mathbf{b}\}\,.$$

Se llama distancia mínima relativa de un código al número $d(\mathcal{C})/n$. Si $\mathcal{C}$ es un código lineal, se llama peso $w(\mathbf{a})$ de una palabra $\mathbf{a} \in \mathcal{C}$ a su distancia a la palabra cero, es decir el número de posiciones en que $\mathbf{a}$ tiene elementos distintos de cero. Se llama peso del código, y se designa por $w(\mathcal{C})$ al mínimo peso de las palabras distintas de cero. Si $\mathcal{C} \subset \mathcal{P}_n$ es un código y $\mathbf{a} \in \mathcal{P}_n$ es una palabra, se llama distancia de $\mathbf{a}$ a $\mathcal{C}$ al número

$$d(\mathbf{a}, \mathcal{C}) = \min\{d(\mathbf{a}, \mathbf{x}) \mid \mathbf{x} \in \mathcal{C}\}\,.$$

Proposición 2.4.2.– *La función $d : \mathcal{P}_n \times \mathcal{P}_n \to \mathbb{Z}_0$ es una distancia en el sentido topológico, es decir, verifica las siguientes propiedades:*

1. $d(\mathbf{a}, \mathbf{b}) = 0 \Longleftrightarrow \mathbf{a} = \mathbf{b}$.
2. $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{b}, \mathbf{a})$ *para todo* $\mathbf{a}, \mathbf{b} \in \mathcal{A}^n$.
3. $$d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}) \geq d(\mathbf{a}, \mathbf{c}) \quad \forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{A}^n\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Demostración: De las tres propiedades de la distancia, la única que no es inmediata de ver es la tercera. Podemos imaginar la distancia de **a** a **c** como el número de posiciones en las que hay que cambiar el símbolo de **a** para obtener **c**. Este número será siempre inferior o igual al número de cambios para pasar de **a** a **b** más el número de cambios para pasar de **b** a **c**. □

Proposición 2.4.3.– *Si $\mathcal{C}$ es un código lineal, entonces $d(\mathcal{C}) = w(\mathcal{C})$.*

Demostración: Como estamos en conjuntos finitos, los mínimos siempre se alcanzan. Al ser $w(\mathcal{C})$ una distancia entre palabras, es $w(\mathcal{C}) \geq d(\mathcal{C})$. Recíprocamente, sean $\mathbf{a}, \mathbf{b} \in \mathcal{C}$ tales que $d(\mathbf{a}, \mathbf{b}) = d(\mathcal{C})$; entonces $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b})$ y $\mathbf{a} - \mathbf{b} \in \mathcal{C}$ porque se trata de un código lineal. Así $d \leq w(\mathcal{C})$. Esto prueba el lema. □

Ejemplo 2.4.4.– En el ejemplo de los números de lotería repetidos, veíamos en 2.3.2.4 que una matriz generadora del código es:

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Fácilmente podemos razonar que el peso del código es 2. Cada fila es una palabra de peso 2. No puede haber palabras de peso 1 porque, esté donde esté un símbolo distinto de cero, debe repetirse en la primera terna de coordenadas o en la segunda, según sea el caso.

Notas 2.4.5.–

2.4.5.1. La proposición 2.4.3, aunque muy sencilla, es enormemente útil. Si $\mathcal{C}$ es un código arbitrario (con m palabras), la determinación de $d(\mathcal{C})$ implica la comparación de todos los pares posibles de palabras de $\mathcal{C}$. Esto, en términos de barrido, significa m^2 pasadas de programa. Sin embargo, la determinación del peso mínimo en un código lineal, significa m pasadas solamente, aún en términos de barrido, porque se comparan todas las palabras con el vector **0**. De todas maneras, la determinación de peso por barrido no da con frecuencia resultados, por el número tan elevado de palabras por las que tiene que pasar el programa.

2.4.5.2. Se puede hacer un programa en Maple que determine el peso mínimo de un código lineal definido por una matriz generadora. Por ejemplo, sobre $\mathbb{Z}/\mathbb{Z}11$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

consideramos el código de matriz generadora

$$\begin{pmatrix} 1 & 2 & 3 & 10 & 5 & 6 \\ 5 & 1 & 9 & 4 & 4 & 8 \\ 1 & 0 & 5 & 4 & 2 & 2 \end{pmatrix}$$

Al ser de dimensión 3, el código tendrá $11^3 = 1331$ palabras, luego un barrido de esas palabras de dos en dos para calcular sus distancias dará $1331^6 = 1771561$ pasadas. En cambio, el dar 1331 pasadas para determinar el peso es muchísimo más corto. Maple nos dice que $d(C) = 3$ en este caso.

Definición 2.4.6.– *Sea* $\mathbf{a} \in \mathcal{P}_n$*; la bola cerrada (o esfera)* $B(\mathbf{a}, d)$ *de centro* $\mathbf{a}$ *y radio* d *es el conjunto de las palabras de* $\mathcal{P}_n$ *cuya distancia de Hamming a* $\mathbf{a}$ *es menor o igual que* d*.*

Notas 2.4.7.– La formulación precisa de la frase "detectar t errores" se puede hacer ahora fácilmente.

2.4.7.1. Partimos de un canal que transmite palabras de $\mathcal{P}_n$ de un punto emisor a uno receptor. Una vez que fijamos un código $\mathcal{C}$, supondremos que se emiten sólo palabras del código, aunque las que se reciban puedan o no estar en él. Si se emite una palabra $\mathbf{x} \in \mathcal{C}$ y se recibe una palabra $\mathbf{y} \in \mathcal{P}_n$, a la distancia $d(\mathbf{x}, \mathbf{y})$ se le llama el *número de errores introducidos en la transmisión.*

2.4.7.2. Hay que tener en cuenta que el punto receptor conoce sólo la palabra $\mathbf{y}$ (¡jamás la $\mathbf{x}$!) y el código $\mathcal{C}$. Por tanto, sólo puede actuar en función de estos datos. Una de las posibles actuaciones es decidir si $\mathbf{y} \in \mathcal{C}$ ó $\mathbf{y} \notin \mathcal{C}$. Esta actuación puede no arreglar nada, porque la transmisión ha podido introducir un número de errores suficiente para que $\mathbf{y} \in \mathcal{C}$ también. En este caso, el receptor sólo puede dar por buena la palabra recibida, aunque no sea la emitida. Esta situación es altamente indeseable.

2.4.7.3. Para un canal fijo, se puede determinar estadísticamente, mediante pruebas repetidas, cuál es el máximo número t de errores que se introducen en la transmisión de palabras de una cierta longitud n. Éste es un dato de entrada de la teoría de códigos, porque, conocido t, se trata de construir un código que no caiga en la situación de 2.4.7.2.

2.4.7.4. Fijado t, un código $\mathcal{C}$ que no cae en la situación de 2.4.7.2 es justamente uno tal que ninguna esfera de centro una palabra $\mathbf{a} \in \mathcal{C}$ y radio t contiene a otra

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

palabra de $\mathcal{C}$ distinta de $\mathbf{a}$. Un código de este tipo se llama un *código detector de t errores*. El punto receptor sólo tiene que determinar la pertenencia a $\mathcal{C}$ para saber si se han producido errores en la transmisión

Proposición 2.4.8.– *El código $\mathcal{C}$ es un código detector de t errores si y sólo si $d(\mathcal{C}) > t$.*

Demostración: Si fuese $d(\mathcal{C}) <= t$, habría al menos una bola de radio t y centro una palabra $\mathbf{a} \in \mathcal{C}$ que contendría a otra palabra del código $\mathbf{b} \neq \mathbf{a}$. Si $d(\mathcal{C}) > t$, es evidente que ninguna bola de centro una palabra de $\mathcal{C}$ contiene a otra distinta. □

Nota 2.4.9.– La formulación precisa de la frase "corregir t errores" se puede hacer ahora fácilmente. No olvidemos jamás que el número máximo t de errores introducidos en la transmisión es un dato de entrada. ¿Qué significa corregir t errores? Pues que, emitida la palabra $\mathbf{x} \in \mathcal{C}$, y recibida la palabra $\mathbf{y}$ (con t errores a lo máximo, porque éste es un dato a priori), el punto emisor pueda reconstruir $\mathbf{x}$ a partir de $\mathbf{y}$. Esto ocurre si y sólo si las esferas de centros las palabras de $\mathcal{C}$ y radio t son disjuntas. El extremo receptor sólo tiene que tener una lista de las palabras de cada esfera de radio t. Recibida $\mathbf{y}$ se busca, en la lista, en qué esfera está, y se determina $\mathbf{x}$ por ser el centro de la esfera. El siguiente teorema 2.4.10 nos da una condición necesaria y suficiente para que un código pueda corregir t errores.

Teorema 2.4.10.– *Sea $\mathcal{C} \subset \mathcal{P}_n$ un código y $t \in \mathbb{Z}_+$. Las condiciones siguientes son equivalentes:*

1. *$\mathcal{C}$ corrige t errores, es decir, las esferas de centros las palabras de $\mathcal{C}$ y radio t son disjuntas.*
2. *$d(\mathcal{C}) \geq 2t + 1$.*

Demostración: Si existiesen $\mathbf{a}, \mathbf{b} \in \mathcal{C}$, distintas, tales que las esferas de centros ambas y radio t no fuesen disjuntas, y si $\mathbf{x} \in \mathcal{P}_n$ fuese tal que $d(\mathbf{x}, \mathbf{a}) \leq t$, $d(\mathbf{x}, \mathbf{b}) \leq t$, sería

$$d(\mathbf{a}, \mathbf{b}) \leq d(\mathbf{a}, \mathbf{x}) + d(\mathbf{x}, \mathbf{b}) \leq t + t = 2t\,,$$

luego $d(\mathcal{C}) \leq 2t$, lo que no ocurre.

Recíprocamente, supongamos que $d(\mathcal{C}) \leq 2t$ y sean $\mathbf{a}, \mathbf{b} \in \mathcal{C}$ tales que $0 < d(\mathbf{a}, \mathbf{b}) = d(\mathcal{C})$. Consideremos dos casos:

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Caso 1: $d(\mathcal{C}) = 2t$. Sea $\mathbf{c}$ la palabra que coincide con $\mathbf{a}$ y $\mathbf{b}$ donde ellas coinciden y que tiene t elementos de $\mathbf{a}$ y t elementos de $\mathbf{b}$ en cualesquiera lugares en los que difieren. Así $\mathbf{c}$ pertenece a las dos esferas: las de centros $\mathbf{a}$ y $\mathbf{b}$ y radio t.
Caso 2: $d(\mathcal{C}) < 2t$. Sea $\mathbf{c}$ la palabra que coincide con $\mathbf{a}$ y $\mathbf{b}$ donde ellas coinciden y, donde no, tiene un número de elementos de $\mathbf{a}$ igual a la parte entera de $d(\mathcal{C})/2$ y un número de elementos de $\mathbf{b}$ para rellenar lo restante. De nuevo, $\mathbf{c}$ pertenece a las dos esferas: las de centros $\mathbf{a}$ y $\mathbf{b}$ y radio t. □

Nota 2.4.11.– También se puede realizar una tarea mixta: detectar y corregir. Esto viene impuesto por el hecho de que corregir errores es muy costoso en términos computacionales. Puede que nos venga bien una táctica de, dado el máximo número de errores t del canal, si la palabra tiene un número de errores pequeño, corregirla, y si tiene más (¡pero siempre menos o igual que t!), marcarla como palabra con errores. Hay que reflexionar sobre lo que significa un código que detecte y corrija al mismo tiempo, para entenderlo, porque no es un concepto fácil.

El punto de partida es el mismo de siempre: el número máximo t de errores que introduce el canal. Como dijimos antes, dependiendo del tipo de información, nos puede bastar con hacer algo como lo siguiente:

1. fijar un número $t_c < t$,
2. si la palabra recibida contiene un número de errores menor o igual que t_c, hallar la emitida.
3. si la palabra recibida contiene un número de errores mayor que t_c (¡ siempre menor o igual que t), marcarla como palabra con errores.

A estas operaciones se les llama corregir t_c errores y detectar $t_d = t - t_c$ a la vez. Es la terminología clásica, que no es muy buena por ser confusa. Por eso hemos hecho hincapié en su explicación.

Evidentemente un código $\mathcal{C}$ corrige t_c errores y a la vez detecta t_d errores si y sólo si las esferas de centros las palabras de $\mathcal{C}$ y radios t_c son disjuntas y ninguna esfera de centro una palabra de $\mathcal{C}$ y radio t contiene a otra palabra de $\mathcal{C}$ distinta. La táctica para el receptor pasa por tener la lista L_c de las esferas de centro las palabras de $\mathcal{C}$ y radio t_c. Recibida una palabra $\mathbf{y}$, si está en una de las esferas de la lista L_c se corrige al centro de la esfera. Si no, se la marca como palabra con t errores a lo máximo.

Teorema 2.4.12.– *Sea $\mathcal{C} \subset \mathcal{P}_n$ un código; las condiciones siguientes son equivalentes:*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

1. *$\mathcal{C}$ corrige t_c errores y detecta t_d errores.*

2. *$d(\mathcal{C}) \geq 2t_c + t_d + 1$.*

Demostración: Si $d(\mathcal{C}) \geq 2t_c + t_d + 1$ entonces $d(\mathcal{C}) \geq 2t_c + 1$, luego $\mathcal{C}$ corrige t_c errores por el teorema 2.4.10. Por otra parte,

$$d(\mathcal{C}) \geq 2t_c + t_d + 1 > t_c + t_d + 1 = t + 1\,,$$

luego detecta t errores por la proposición 2.4.8.

Supongamos ahora que $d(\mathcal{C}) \leq 2t_c + t_d$. Si fuese $d(\mathcal{C}) \leq 2t_c$, entonces $\mathcal{C}$ no corregiría t_c errores por el teorema 2.4.10, y así nuestra demostración habría terminado. Supongamos, pues, que $2t_c < d(\mathcal{C}) \leq 2t_c + t_d$. Sean $\mathbf{a}, \mathbf{b} \in \mathcal{C}$ tales que $2t_c < d(\mathbf{a}, \mathbf{b}) \leq 2t_c + t_d$. Sea $\mathbf{c}$ una palabra que coincide con $\mathbf{a}$ y $\mathbf{b}$ donde ellas coinciden, coincide con $\mathbf{a}$ en t_c lugares más y con $\mathbf{b}$ en los restantes. El número de lugares en que $\mathbf{a}$ y $\mathbf{b}$ coinciden es $n - d(\mathbf{a}, \mathbf{b})$ y

$$n - 2t_c > n - d(\mathbf{a}, \mathbf{b}) \geq n - (2t_c + t_d)\,.$$

Por tanto, el número de lugares en que coinciden $\mathbf{a}$ y $\mathbf{c}$ es

$$n - d(\mathbf{a}, \mathbf{b}) + t_c \geq n - (t_c + t_d)\,.$$

Así,

$$d(\mathbf{a}, \mathbf{c}) = n - [n - d(\mathbf{a}, \mathbf{b}) + t_c] \leq n - [n - (t_c + t_d)] = t_c + t_d = t\,.$$

El número de lugares en que coinciden $\mathbf{b}$ y $\mathbf{c}$ es

$$[n - d(\mathbf{a}, \mathbf{b})] + [d(\mathbf{a}, \mathbf{b}) - t_c] = n - t_c\,,$$

luego la distancia de $d(\mathbf{b}, \mathbf{c}) = t_c \leq t$. Así, $\mathbf{c}$ está en las bolas de centros $\mathbf{a}$ y $\mathbf{b}$ y radio t, con lo que $\mathcal{C}$ no puede detectar t errores. □

Ejemplo 2.4.13.– Volvamos al ejemplo de los números de lotería con repetición, como vimos en la sección 2.3. Vamos a responder a la pregunta de qué ganamos repitiendo los números transmitidos. En 2.3.2.4 vimos que la matriz generadora del código de los números con repetición es

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

y que el peso del código es 2. Esto significa que la repetición puede detectar un error, pero no puede corregir ninguno. Por ejemplo, supongamos que llega al receptor la palabra $[1, 2, 3, 1, 5, 3]$. Es evidente que hay un error en la transmisión porque las tres últimas componentes no son iguales a las tres primeras. En cambio, no podemos decir qué palabra se emitió porque puede ser, bien $[1, 2, 3, 1, 2, 3]$, bien $[1, 5, 3, 1, 5, 3]$.

De la misma manera, el repetir dos veces tiene como matriz generadora

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

y el código tiene peso 3. Así pueden detectar dos errores y corregir uno. Por ejemplo, supongamos que recibimos la palabra $[1, 2, 3, 1, 4, 3, 1, 5, 3]$; está claro que hay dos errores, pero no podemos corregirlos porque la palabra emitida puede ser, bien $[1, 2, 3, 1, 2, 3, 1, 2, 3]$, $[1, 4, 3, 1, 4, 3, 1, 4, 3]$, $[1, 5, 3, 1, 5, 3, 1, 5, 3]$. En cambio, sí se puede corregir un error porque, recibida la palabra $[1, 2, 3, 1, 2, 3, 1, 5, 3]$, sólo puede provenir de $[1, 2, 3, 1, 2, 3, 1, 2, 3]$.

Hay que hacer algunas advertencias importantes. Una de ellas es que la determinación a priori del número máximo de errores del canal es esencial. Si recibimos la palabra $[1, 2, 3, 1, 4, 3, 1, 5, 3]$ y admitimos que el canal pueda cometer cualquier número de errores, ¿por qué no pensar que la emitida pudo ser $[0, 0, 0, 0, 0, 0, 0, 0, 0]$? O si admitimos sólo cuatro errores y recibimos $[1, 2, 3, 1, 2, 3, 1, 5, 3]$, ¿por qué no pensar que la emitida fue $[0, 2, 3, 0, 2, 3, 0, 2, 3]$? El problema es al contrario: si queremos corregir cuatro errores, tenemos que diseñar un código que lo haga. Si no empeñamos en los códigos de repetición, tendríamos que ir a nueve copias de las palabras, o sea a k^{27}

Otra advertencia es que cuando decimos que un código no corrige dos errores, por ejemplo, significa que no los corrige siempre, aunque los pueda corregir para palabras particulares. Por ejemplo, supongamos que recibimos la palabra $[1, 2, 3, 1, 2, 3, 0, 0, 3]$ en el código de tres copias, y que el número de errores del canal es 2. Esa palabra sólo puede provenir de $[1, 2, 3, 1, 2, 3, 1, 2, 3]$. En efecto, debemos efectuar dos cambios en la palabra recibida para obtener una del código. Si efectuamos un cambio en una de las dos primeras ternas, tenemos que efectuarlo en el mismo lugar de la segunda y de esta forma no logramos una palabra del código. Por ejemplo, por este procedimiento podríamos lograr $[0, 2, 3, 0, 2, 3, 0, 0, 3]$, que no está en el código. Así es que los dos cambios a efectuar deben ir a la tercera terna, lo que deduce unívocamente la palabra emitida.

Terminamos esta sección abstracta con una cuenta sencilla. Los ejemplos con jugo vendrán más adelante.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Teorema 2.4.14.– *Consideremos un alfabeto $\mathcal{A}$ con q símbolos y el conjunto $\mathcal{P}_n$ de palabras de longitud n. Sea $\mathbf{a} \in \mathcal{P}_n$ fija; entonces la esfera de centro $\mathbf{a}$ y radio $t \geq 0$ contiene*

$$N(q,n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

elementos. Si $\mathcal{C} \subset \mathcal{P}_n$ es un código y $d = d(\mathcal{C}) = 2t+1$, entonces

$$\operatorname{card}(\mathcal{C}) \leq \frac{q^n}{N(q,n,t)}\,.$$

Si se alcanza la igualdad, el código se llama perfecto

Demostración: Las palabras que distan i de $\mathbf{a}$ se obtienen de $\mathbf{a}$ cambiando su símbolo en i posiciones. Las formas de seleccionar i posiciones son $\binom{n}{i}$. En cada una de las posiciones en que se cambia el símbolo hay $q-1$ posibilidades de introducir símbolos (todos menos el que $\mathbf{a}$ tiene en esa posición). Por tanto, para cada selección de i posiciones, hay $\binom{n}{i}(q-1)^i$ posibilidades de palabras. De ahí sale claramente la expresión para $N(q,n,t)$.

Sea ahora $\mathcal{C}$ un código en las condiciones del enunciado; por el teorema 2.4.10 las esferas de centros las palabras del código y radio t son disjuntas. Por tanto, la unión de esas esferas tiene $\operatorname{card}(\mathcal{C})N(q,n,t)$ palabras, que deber ser menor o igual que el número total de palabras, q^n. De ahí la desigualdad.

Como comentario final, nótese que en un código $\mathcal{C}$ como antes es perfecto si y sólo si se pueden corregir t errores de cada palabra. □

Naturalmente, los códigos perfectos aparecen como el ideal. El problema es que no hay muchos.

Vamos ahora a detener el estudio de la teoría de códigos para tratar de aritmética. Antes de nada, recordamos unas breves nociones de combinatoria.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 3

Combinatoria

3.1. El binomio de Newton

Definición 3.1.1.– *Sea $m \in \mathbb{Z}_0$; se define el factorial de m en forma recurrente así:*

1. $0! = 1$
2. *Si $m > 0$ es $m! = m[(m-1)!]$*

Lema 3.1.2.– *Sea $m > 0$ un entero; entonces $m! = m(m-1)(m-2)\cdots 3 \cdot 2 \cdot 1$.*

Demostración: En efecto, la fórmula se verifica para $m = 1$ porque, según la definición 3.1.1, se tiene $1! = 1 \cdot (0!) = 1 \cdot 1 = 1$. Supongamos la fórmula cierta para m; entonces, por la definición 3.1.1 es

$$(m+1)! = (m+1)[m!] = (m+1)m(m-1)\cdots 3 \cdot 2 \cdot 1$$

□

Definición 3.1.3.– *Sean $m, n \in \mathbb{Z}_0$; se define el número combinatorio $\binom{m}{n}$ en la forma siguiente:*

$$\binom{m}{n} = \begin{cases} \dfrac{m!}{n!(m-n)!} & si\ m \geq n \geq 0 \\ 0 & si\ m < n \end{cases}$$

UNIVERSIDAD DE SEVILLA

Notas 3.1.4.– Los números combinatorios tienen unas propiedades fascinantes desde el punto de vista aritmético, que los hacen parecer casi mágicos. Veamos unas cuantas.

3.1.4.1. Se verifica que

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}.$$

Esto se puede demostrar directamente desde la definición:

$$\begin{aligned}\binom{m-1}{n-1} + \binom{m-1}{n} &= \frac{(m-1)(m-2)\cdots(m-n+1)}{(n-1)!} + \\ &\quad \frac{(m-1)(m-2)\cdots(m-n)}{n!} \\ &= \frac{(m-1)(m-2)\cdots(m-n+1)[n+(m-n)]}{n!} \\ &= \frac{m(m-1)(m-2)\cdots(m-n+1)}{n!} = \binom{m}{n}\end{aligned}$$

3.1.4.2. La propiedad anterior permite formar el *triángulo de Tartaglia*. Observemos la tabla siguiente:

$$\begin{array}{ccccccccccc}
 & & & & \binom{1}{1} & & \binom{1}{1} & & & & \\
 & & \binom{2}{0} & & & \binom{2}{1} & & \binom{2}{2} & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & & \binom{3}{2} & & \binom{3}{3} & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & & \binom{4}{3} & & \binom{4}{4} & \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots &
\end{array}$$

o con números:

$$\begin{array}{ccccccccccc}
 & & & & 1 & & 1 & & & & \\
 & & 1 & & & 2 & & 1 & & & \\
 & 1 & & & 3 & & & 3 & & 1 & \\
1 & & & 4 & & & 6 & & 4 & & 1 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots &
\end{array}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

El hecho de que

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}.$$

significa que la regla de formación de cada fila del triángulo es la siguiente: se comienza y termina por 1; cada número es suma de los dos que tiene arriba (el de la izquierda y el de la derecha). Este triángulo de Tartaglia es, en cierto modo, una forma recurrente de calcular números combinatorios, usando sólo la suma de enteros. Como todo lo recurrente, es costoso en tiempo y en memoria; sin embargo, es fácil en operaciones.

3.1.4.3. La fórmula

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}.$$

tiene una aplicación muy buena a la suma de números combinatorios con parte inferior igual. Apliquémosla sucesivamente a numeradores decrecientes, suponiendo $m > n$:

$$\begin{aligned}
\binom{m}{n} &= \binom{m-1}{n-1} + \binom{m-1}{n} \\
\binom{m-1}{n} &= \binom{m-2}{n-1} + \binom{m-2}{n} \\
\vdots &= \vdots \\
\binom{n+1}{n} &= \binom{n}{n-1} + \binom{n}{n} \\
\binom{n}{n} &= \binom{n-1}{n-1}
\end{aligned}$$

Sumando miembro a miembro y cancelando los términos iguales se tiene:

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-2}{n-1} + \cdots \binom{n}{n-1} + \binom{n-1}{n-1}$$

Esta fórmula será enormemente útil más adelante al calcular dimensiones de espacios vectoriales de polinomios homogéneos.

Teorema 3.1.5.– *Sean a, b números reales o complejos, variables o expresiones y sea $m > 0$ un entero. Entonces se verifica:*

$$(a+b)^m = \binom{m}{0}a^m + \binom{m}{1}a^{m-1}b + \cdots \binom{m}{m-1}ab^{m-1} + \binom{m}{m}b^m$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$$= \sum_{i=0}^{m} \binom{m}{i} a^{m-i} b^i$$

Demostración: La podemos hacer por recurrencia sobre m. El caso $m = 1$ es trivial porque

$$a + b = \binom{1}{0} a + \binom{1}{1} b\,.$$

Supongamos que el teorema se verifica para $m \geq 1$, es decir que

$$(a+b)^m = \sum_{i=0}^{m} \binom{m}{i} a^{m-i} b^i\,.$$

Entonces

$$\begin{aligned}
(a+b)^{m+1} &= (a+b)^m \cdot (a+b) = (a+b)^m \cdot a + (a+b)^m \cdot b \\
&= a \sum_{i=0}^{m} \binom{m}{i} a^{m-i} b^i + b \sum_{i=0}^{m} \binom{m}{i} a^{m-i} b^i \\
&= \sum_{i=0}^{m} \binom{m}{i} a^{m+1-i} b^i + \sum_{i=0}^{m} \binom{m}{i} a^{m-i} b^{i+1} \\
&= a^{m+1} + \sum_{i=1}^{m} \left(\binom{m}{i} + \binom{m}{i-1} \right) a^{m+1-i} b^i + b^{m+1} \\
&= a^{m+1} + \sum_{i=1}^{m} \binom{m+1}{i} a^{m+1-i} b^i + b^{m+1} \\
&= \sum_{i=0}^{m+1} \binom{m+1}{i} a^{m+1-i} b^i
\end{aligned}$$

Esto prueba el teorema. □

3.2. Cominatoria sin repetición

El problema de la combinatoria básica se plantea así. Se parte de un conjunto finito ordenado de símbolos, que se llama un *alfabeto*, llamando *letras* a estos símbolos. Como la representación tipográfica de los símbolos no juega papel alguno en los razonamientos, representaremos usualmente a un alfabeto de m letras por $\mathcal{A}_m = [1, 2, 3, \ldots, m]$, es decir, los números desde 1 hasta m ordenados en su orden

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

natural, lo que se expresa poniéndolos entre corchetes y suponiendo que el orden va de izquierda a derecha. Con este alfabeto se forman todas las palabras de longitud fija n, con $0 < n \leq m$, sujetas a ciertas reglas que se especifican. Se trata de, para cada regla, formar todas las palabras, contarlas, ponerlas en el orden en que aparecerían en un diccionario (*orden lexicográfico*) y establecer las funciones que, a cada palabra asigna su número de orden, y a cada número asigna la palabra cuyo orden en la lista es ese número.

La combinatoria sin repetición versa sobre las palabras que se pueden formar sin repetir letras. Para la combinatoria sin repetición, hay tres tipos clásicos de palabras: permutaciones, variaciones y combinaciones.

Definición 3.2.1.– *Se llaman permutaciones del alfabeto $\mathcal{A}_m$ a todas las palabras que se pueden formar con las m letras.*

Por ejemplo, si $\mathcal{A} = [c, b, a]$, las permutaciones, ordenadas por orden lexicográfico, son

$$[[c, b, a], [c, a, b], [b, c, a], [b, a, c], [a, c, b], [a, b, c]] .$$

Proposición 3.2.2.– *El número de permutaciones del alfabeto $\mathcal{A}_m$ es $m!$.*

Demostración: Para la primera posición de una palabra tenemos m posibles elecciones de una letra, es decir, podemos elegir cualquiera. Elegida la primera, tenemos $m-1$ posibles elecciones para la segunda (todas las letras menos la primera), luego hay $m(m-1)$ posibilidades de elección de la primera y la segunda letras. Elegidos éstas, tenemos $m-2$ posibilidades de elección de la tercera y $m(m-1)(m-2)$ posibilidades de elección de las tres primeras. Procediendo así sucesivamente se ve ya que habrá $m!$ maneras de colocar las letras, luego $m!$ palabras. □

Notas 3.2.3.– Sea $\mathcal{A} = \mathcal{A}_m$ un alfabeto con m letras, y supongamos formado el conjunto $P_{\mathcal{A}}$ de las permutaciones de $\mathcal{A}$, ordenadas por orden lexicográfico. En estas notas daremos la función que, a cada permutación $p \in P_{\mathcal{A}}$, asigna el número de orden en el que aparece en la lista $P_{\mathcal{A}}$. En el ejemplo de más arriba, la permutación $[b, a, c]$ tiene el número de orden 4.

3.2.3.1. Sea $f_{\mathcal{A}}: \mathcal{A} \to \mathbb{Z}_>$ la función que a cada elemento $a \in \mathcal{A}$ hace corresponder el número de permutaciones de la lista ordenada que hay antes de la primera que empieza por a. Evidentemente, si a ocupa el lugar k en $\mathcal{A}$, entonces $f_{\mathcal{A}}(a) = (k-1)(m-1)!$. Por tanto, si $[a_1, a_2, \ldots, a_m] \in P_{\mathcal{A}}$, su número de orden en la lista de

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

todas las permutaciones es

$$f_{\mathcal{A}}(a_1) + f_{\mathcal{A}\setminus[a_1]}(a_2) + \cdots + f_{\mathcal{A}\setminus[a_1,\ldots,a_{m-1}]}(a_m) + 1$$

3.2.3.2. Por ejemplo, si $\mathcal{A} = [c, b, a]$, las permutaciones, ordenadas por orden lexicográfico, son

$$[[c, b, a], [c, a, b], [b, c, a], [b, a, c], [a, c, b], [a, b, c]]\,.$$

El número de orden que ocupa $[a, c, b]$ es

$$f_{[c,b,a]}(a) + f_{[c,b]}(c) + f_{[b]}(b) + 1 = 2 \cdot 2! + 0 \cdot 1! + 0 \cdot 0! + 1 = 5\,.$$

3.2.3.3. Otro ejemplo de más tamaño es el alfabeto $\mathcal{A} = [1, 2, 3, 4, 5, 6, 7, 8]$; la lista $P_{\mathcal{A}}$ de las permutaciones de $\mathcal{A}$ tiene $8! = 40320$. El número de orden de $[6, 8, 1, 7, 3, 5, 4, 2]$ en $P_{\mathcal{A}}$ es

$$\begin{aligned} & f_{[1,2,3,4,5,6,7,8]}(6) + f_{[1,2,3,4,5,7,8]}(8) + f_{[1,2,3,4,5,7]}(1) + f_{[2,3,4,5,7]}(7) \\ & + f_{[2,3,4,5]}(3) + f_{[2,4,5]}(5) + f_{[2,4]}(4) + f_{[2]}(2) + 1 \\ = \;& 5 \cdot 7! + 6 \cdot 6! + 0 \cdot 5! + 4 \cdot 4! + 1 \cdot 3! + 2 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! + 1 \\ = \;& 29628 \end{aligned}$$

3.2.3.4. Recíprocamente, la función $g_{\mathcal{A}}{:}\{1, \ldots, n!\} \to \mathcal{A}$ que, a cada entero n, $1 \leq n \leq m!$ asigna el elemento con el que empieza la permutación que ocupa el lugar n viene dada por: $g_{\mathcal{A}}(n)$ es el elemento que ocupa el lugar $q_1 + 1$ en $\mathcal{A}$, donde q_1 es el cociente de dividir $n - 1$ entre $(m - 1)!$. Si r_1 es el resto de esta división, la permutación que ocupa el lugar n en $P_{\mathcal{A}}$ es

$$[a_{q_1+1}, a_{q_2+1}, \ldots, a_{q_n+1}]$$

donde, para todo $i \geq 2$, q_i es el resto de dividir r_{i-1} entre $(m - i)!$, y a_{q_i+1} es el elemento que ocupa el lugar $q_i + 1$ en $\mathcal{A}$, habiéndole quitado todos los elementos anteriores.

3.2.3.5. En el ejemplo de 3.2.3.3, la permutación que ocupa el lugar 11111 es:

$$\begin{aligned} 11110 &= 2 \cdot 7! + 1030 \longrightarrow 3 \\ 1030 &= 1 \cdot 6! + 310 \longrightarrow 2 \\ 310 &= 2 \cdot 5! + 70 \longrightarrow 5 \end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$$\begin{aligned} 70 &= 2\cdot 4! + 22 \longrightarrow 6 \\ 22 &= 3\cdot 3! + 4 \longrightarrow 8 \\ 4 &= 2\cdot 2! + 0 \longrightarrow 7 \\ 0 &= 0\cdot 1! + 0 \longrightarrow 1 \\ 0 &= 0\cdot 0! + 0 \longrightarrow 4\,, \end{aligned}$$

luego la permutación que ocupa el lugar 11111 es $[3,2,5,6,8,7,1,4]$.

Definición 3.2.4.– *Se llaman variaciones sobre el alfabeto $\mathcal{A}_m$ con n letras (o variaciones de m elementos tomados de n en n) a todas las palabras que se pueden formar con n letras, $1 \leq n \leq m$.*

Por ejemplo, si $\mathcal{A} = [c,b,a]$, las variaciones con dos letras, ordenadas por orden lexicográfico, son

$$[[c,b],[c,a],[b,c],[b,a],[a,c],[a,b]]\,.$$

Proposición 3.2.5.– *El número de variaciones del alfabeto $\mathcal{A}_m$ con n letras es $m(m-1)\cdots(m-n-1)$. Se le designa por $v_{m,n}$ porque sólo depende de m y n pero no de $\mathcal{A}_m$.*

La demostración es trivialmente análoga a la de la proposición 3.2.2

Notas 3.2.6.– Sea $\mathcal{A} = \mathcal{A}_m$ un alfabeto con m letras, y supongamos formado el conjunto $V_{\mathcal{A},n}$ de las variaciones de $\mathcal{A}$ con n letras, ordenadas por orden lexicográfico. En estas notas daremos la función que, a cada variación $v \in V_{\mathcal{A},n}$, asigna el número de orden en el que aparece en la lista $V_{\mathcal{A},n}$. En el ejemplo de más arriba, la permutación $[b,a]$ tiene el número de orden 4.

3.2.6.1. Sea $f_{\mathcal{A},n}\colon \mathcal{A} \to \mathbb{Z}_>$ la función que a cada elemento $a \in \mathcal{A}$ hace corresponder el número de variaciones de la lista ordenada que hay antes de la primera que empieza por a. Evidentemente, si a ocupa el lugar k en $\mathcal{A}$, entonces $f_{\mathcal{A}}(a) = (k-1)v_{m,n}/m$. Por tanto, si $[a_1,a_2,\ldots,a_n] \in V_{\mathcal{A}}$, su número de orden en la lista de todas las variaciones es

$$f_{\mathcal{A},n}(a_1) + f_{\mathcal{A}\setminus[a_1],n-1}(a_2) + \cdots + f_{\mathcal{A}\setminus[a_1,\ldots,a_{n-1}],1}(a_n) + 1$$

3.2.6.2. Por ejemplo, si $\mathcal{A} = [c,b,a]$, las variaciones con dos letras, ordenadas por orden lexicográfico, son

$$[[c,b],[c,a],[b,c],[b,a],[a,c],[a,b]]\,.$$

UNIVERSIDAD DE SEVILLA

El número de orden que ocupa $[a, c]$ es

$$f_{[c,b,a],2}(a) + f_{[c,b],1}(c) = 2 \cdot 6/3 + 0 \cdot 2/2 + 1 = 5\,.$$

3.2.6.3. Otro ejemplo de más tamaño es el alfabeto $\mathcal{A} = [1, 2, 3, 4, 5, 6, 7, 8]$; la lista $V_{\mathcal{A},n}$ de las variaciones de $\mathcal{A}$ con 4 letras tiene $8 \cdot 7 \cdot 6 \cdot 6 = 1680$ elementos. El número de orden de $[7, 6, 5, 4]$ en $V_{\mathcal{A},4}$ es

$$\begin{aligned} & f_{[1,2,3,4,5,6,7,8],4}(7) + f_{[1,2,3,4,5,6,8],3}(6) + f_{[1,2,3,4,5,8],2}(5) + f_{[1,2,3,4,8],1}(4) \\ = \;& 6 \cdot 7 \cdot 6 \cdot 5 + 5 \cdot 6 \cdot 5 + 4 \cdot 5 + 3 \cdot 1 + 1 = 1434 \end{aligned}$$

3.2.6.4. Recíprocamente, la función $g_{\mathcal{A},n}{:}\{1, \ldots, v_{m,n}\} \to \mathcal{A}$ que, a cada entero x, $1 \leq x \leq v_{m,n}$ asigna el elemento con el que empieza la permutación que ocupa el lugar x viene dada por: $g_{\mathcal{A}}(x)$ es el elemento que ocupa el lugar $q_1 + 1$ en $\mathcal{A}$, donde q_1 es el cociente de dividir $x - 1$ entre $v_{m,n}/m$. Si r_1 es el resto de esta división, la variación que ocupa el lugar x en $V_{\mathcal{A}}$ es

$$[a_{q_1+1}, a_{q_2+1}, \ldots, a_{q_n+1}]$$

donde, para todo $i \geq 2$, q_i es el resto de dividir r_{i-1} entre $v_{m-i,n-i}/(m-i)$, y a_{q_i+1} es el elemento que ocupa el lugar $q_i + 1$ en $\mathcal{A}$, habiéndole quitado todos los elementos anteriores.

3.2.6.5. En el ejemplo de 3.2.6.3, $v_{8,4} = 1680$, $v_{7,3} = 210$, $v_{6,2} = 30$, $v_{5,1} = 5$ y la variación que ocupa el lugar 1111 es:

$$\begin{aligned} 1110 &= 5 \cdot 1680/8 + 60 \longrightarrow 6 \\ 60 &= 2 \cdot 210/7 + 0 \longrightarrow 3 \\ 0 &= 0 \cdot 30/6 + 0 \longrightarrow 1 \\ 0 &= 0 \cdot 5/5 + 0 \longrightarrow 2\,, \end{aligned}$$

luego la variación que ocupa el lugar 1111 es $[6, 3, 1, 2]$.

Definición 3.2.7.– *Se llaman combinaciones sobre el alfabeto $\mathcal{A}_m$ con n letras a todas las palabras que se pueden formar con n letras, $1 \leq n \leq m$ puestas en orden lexicográfico.*

Por ejemplo, si $\mathcal{A} = [c, b, a]$, las combinaciones con dos letras, ordenadas por orden lexicográfico, son

$$[[c, b], [c, a], [b, a]]\,.$$

UNIVERSIDAD DE SEVILLA

Proposición 3.2.8.– *El número de combinaciones del alfabeto $\mathcal{A}_m$ con n letras es $\binom{m}{n}$. Se le designa por $c_{m,n}$ porque sólo depende de m y n pero no de $\mathcal{A}_m$.*

Demostración: El número de variaciones de $\mathcal{A}_m$ tomado con n letras es $v_{m,n} = m(m-1)\cdots(m-n+1)$. Elegidas todas las variaciones que constan de las mismas letras, sólo una de ellas las tiene en orden lexicográfico, evidentemente. Las otras se obtienen permutando las letras de ésta de todas las formas posibles. Así,

$$c_{m,n} = \frac{v_{m,n}}{n!} = \frac{m(m-1)\cdots(m-n+1)}{n!} = \frac{m!}{(m-n)!} = \binom{m}{n}.$$

□

Notas 3.2.9.– Sea $\mathcal{A} = \mathcal{A}_m$ un alfabeto con m letras, y supongamos formado el conjunto $C_{\mathcal{A},n}$ de las combinaciones de $\mathcal{A}$ con n letras, ordenadas por orden lexicográfico. En estas notas daremos la función que, a cada combinación $c \in C_{\mathcal{A},n}$, asigna el número de orden en el que aparece en la lista $C_{\mathcal{A},n}$. En el ejemplo de más arriba, la combinación $[b, a]$ tiene el número de orden 3.

3.2.9.1. Sea $f_{\mathcal{A},n}\colon \mathcal{A} \to \mathbb{Z}_>$ la función que a cada elemento $a \in \mathcal{A}$ hace corresponder el número de combinaciones de la lista ordenada que hay antes de la primera que empieza por a. Evidentemente, si a ocupa el lugar k en $\mathcal{A}$, entonces, si $k = 1$ es $f_{\mathcal{A},n}(a) = 0$ y, si $k > 1$,

$$f_{\mathcal{A},n}(a) = \sum_{i=1}^{k-1} \binom{m-i}{n-1}$$

Por tanto, si $[a_1, a_2, \ldots, a_n] \in C_{\mathcal{A}}$, su número de orden en la lista de todas las combinaciones es

$$f_{A'_0,n}(a_1) + f_{A'_1,n-1}(a_2) + \cdots + f_{A'_{n-1},1}(a_n) + 1$$

donde $A'_0 = \mathcal{A}$ y cada A'_i, $1 \le i \le n-1$ se forma quitando de A'_{i-1} el elemento a_i y todos los que le anteceden.

3.2.9.2. Por ejemplo, sea el alfabeto $\mathcal{A} = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]$; la lista $C_{\mathcal{A},6}$ de las combinaciones de $\mathcal{A}$ con 6 letras tiene $\binom{12}{6} = 924$ elementos. El número de orden de $[3, 6, 7, 9, 11, 12]$ en $C_{\mathcal{A},6}$ se calcula así:

$$f_{[1,2,3,4,5,6,7,8,9,10,11,12],6}(3) \;=\; \binom{11}{5} + \binom{10}{5} = 462 + 252 = 714$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$$\begin{aligned} f_{[4,5,6,7,8,9,10,11,12],5}(6) &= \binom{8}{4} + \binom{7}{4} = 70 + 35 = 105 \\ f_{[7,8,9,10,11,12],4}(7) &= 0 \\ f_{[8,9,10,11,12],3}(9) &= \binom{4}{2} = 6 \\ f_{[10,11,12],2}(11) &= \binom{2}{1} = 2 \\ f_{[12],1}(12) &= 0 \end{aligned}$$

siendo el número $714 + 105 + 0 + 6 + 2 + 0 + 1 = 828$.

3.2.9.3. Recíprocamente, la función $g_{\mathcal{A},n}{:}\{1, \ldots, c_{m,n}\} \to \mathcal{A}$ que, a cada entero x, $1 \leq x \leq c_{m,n}$ asigna el elemento con el que empieza la permutación que ocupa el lugar x se calcula simplemente por bactracking, teniendo en cuenta que, $g_{\mathcal{A},n}(c_{m,n})$ es el elemento que ocupa el lugar $m - n + 1$ en $\mathcal{A}$. Después, recurrentemente, a la manera de 3.2.9.1 se calcula la combinación que ocupa el lugar dado.

3.2.9.4. Continuamos con el ejemplo de 3.2.9.2. Queremos calcular qué combinación ocupa el lugar 666. Para hallar el elemento con el que empieza hacemos lo siguiente:

$$\begin{aligned} f_{[1,2,3,4,5,6,7,8,9,10,11,12],6}(1) &= 0 \\ f_{[1,2,3,4,5,6,7,8,9,10,11,12],6}(2) &= \binom{11}{5} = 462 \\ f_{[1,2,3,4,5,6,7,8,9,10,11,12],6}(3) &= \binom{11}{5} + \binom{10}{5} = 462 + 252 = 714\,, \end{aligned}$$

de donde deducimos que la combinación ha de empezar por 2. Ahora, dentro de las combinaciones de $[3, 4, 5, 6, 7, 8, 9, 10, 11, 12]$ tomadas de 5 en 5 tenemos que hallar el elemento con el que empieza la que tiene número de orden $666 - 462 = 204$. Para ello hacemos lo siguiente:

$$\begin{aligned} f_{[3,4,5,6,7,8,9,10,11,12],5}(3) &= 0 \\ f_{[3,4,5,6,7,8,9,10,11,12],5}(4) &= \binom{9}{4} = 126 \\ f_{[3,4,5,6,7,8,9,10,11,12],5}(5) &= \binom{9}{4} + \binom{8}{4} = 126 + 70 = 196 \end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$$f_{[3,4,5,6,7,8,9,10,11,12],5}(6) = \binom{9}{4} + \binom{8}{4} + \binom{7}{4} = 126 + 70 + 35 = 231\,,$$

de donde deducimos que la combinación ha de continuar por 5. Ahora, dentro de las combinaciones de $[6, 7, 8, 9, 10, 11, 12]$ tomadas de 4 en 4 tenemos que hallar el elemento con el que empieza la que tiene número de orden $204 - 196 = 8$. Para ello hacemos lo siguiente:

$$\begin{aligned} f_{[6,7,8,9,10,11,12],4}(6) &= 0 \\ f_{[6,7,8,9,10,11,12],4}(7) &= \binom{6}{3} = 20\,, \end{aligned}$$

de donde deducimos que la combinación ha de continuar por 6. Ahora, dentro de las combinaciones de $[7, 8, 9, 10, 11, 12]$ tomadas de 3 en 3 tenemos que hallar el elemento con el que empieza la que tiene número de orden 8. Para ello hacemos lo siguiente:

$$\begin{aligned} f_{[7,8,9,10,11,12],3}(7) &= 0 \\ f_{[7,8,9,10,11,12],3}(8) &= \binom{5}{2} = 10\,, \end{aligned}$$

de donde deducimos que la combinación ha de continuar por 7. Ahora, dentro de las combinaciones de $[8, 9, 10, 11, 12]$ tomadas de 2 en 2 tenemos que hallar el elemento con el que empieza la que tiene número de orden 8. Para ello hacemos lo siguiente:

$$\begin{aligned} f_{[8,9,10,11,12],2}(8) &= 0 \\ f_{[8,9,10,11,12],2}(9) &= \binom{4}{1} = 4 \\ f_{[8,9,10,11,12],2}(10) &= \binom{4}{1} + \binom{3}{1} = 4 + 3 = 7 \\ f_{[8,9,10,11,12],2}(11) &= \binom{4}{1} + \binom{3}{1} + \binom{2}{1} = 4 + 3 + 2 = 9\,, \end{aligned}$$

de donde deducimos que la combinación ha de continuar por 10. Ahora, dentro de las combinaciones de $[11, 12]$ tomadas de 1 en 1 tenemos que hallar el elemento con el que empieza la que tiene número de orden $8 - 7 = 1$ que es, evidentemente, 11. Así, la combinación con número de orden 666 es $[2, 5, 6, 7, 10, 11]$.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 4

Enteros

4.1. Los principios básicos

En esta sección se recuerdan los principios básicos en que se apoya la aritmética de los números enteros, que son bien conocidos.

La notación mundialmente aceptada para el conjunto de los números enteros es $\mathbb{Z}$. Se designa por $\mathbb{Z}_0$ al conjunto de los enteros no negativos (por otro nombre los *números naturales*) y por $\mathbb{Z}_+$ al de los enteros positivos.

Del conjunto de los números enteros tenemos en cuenta las operaciones aritméticas de adición y multiplicación, junto con las siguientes propiedades fundamentales:

1. El orden total natural y sus relaciones con las operaciones aritméticas, que son:

   a) $a \leq b$ y $c \leq d$ implican que $a + c \leq b + d$.

   b) $a \leq b$ y $c > 0$ implican que $ac \leq bc$. Además, $a \leq b$ y $c < 0$ implican que $ac \geq bc$.

2. El hecho de que el orden total natural sea un *buen orden*. Esto quiere decir lo siguiente:

   Principio de la buena ordenación: Todo subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente posee un mínimo.

   También admite una variante, que es equivalente a la anterior[1]:

[1] multiplíquese todo el conjunto por -1

PRINCIPIO DE LA BUENA ORDENACIÓN: Todo subconjunto no vacío de $\mathbb{Z}$ acotado superiormente posee un máximo.

3. El principio de inducción o recurrencia, que usaremos en cada una de las dos formas siguientes:

   PRINCIPIO DE RECURRENCIA ASCENDENTE: Sea $S \subset \mathbb{Z}$ un subconjunto no vacío y sea $s_0 \in S$ un elemento fijo. Supongamos que S verifica la propiedad siguiente: Para todo $s \in S$, $s \geq s_0$, es $s+1 \in S$. Entonces S contiene a todos los enteros mayores o iguales que s_0.

   Multiplicando por -1 se obtiene la segunda variante:

   PRINCIPIO DE RECURRENCIA DESCENDENTE: Sea $S \subset \mathbb{Z}$ un subconjunto no vacío y sea $s_0 \in S$ un elemento fijo. Supongamos que S verifica la propiedad siguiente: Para todo $s \in S$, $s \leq s_0$, es $s-1 \in S$. Entonces S contiene a todos los enteros menores o iguales que s_0.

Vamos a dar ahora dos aplicaciones esenciales: una del principio de la buena ordenación y otra del de recurrencia. La del principio de la buena ordenación va a ser la división euclídea. Para ello recordemos que el valor absoluto $|n|$ de un $n \in \mathbb{Z}$ se define así:

$$\begin{cases} |0| = 0 \\ |n| = n\,,\ \forall n > 0 \\ |n| = -n\,,\ \forall n < 0 \end{cases} .$$

Teorema 4.1.1.– (DIVISIÓN EUCLÍDEA) *Dados dos enteros $a, b \in \mathbb{Z}$, $b \neq 0$, existen $q, r \in \mathbb{Z}$, unívocamente determinados por el par (a, b) tales que $a = bq + r$ y $0 \leq r < |b|$.*

Demostración: Vamos a demostrar primero la existencia y después lo haremos con la unicidad. Para probar la existencia podemos suponer que $a \neq 0$ (o sea que $|a| \geq 1$) porque, si $a = 0$, entonces $a = 0 = 0 \cdot |b| + 0$ y así $q = r = 0$ satisfacen las condiciones del enunciado.

Como $b \neq 0$, es $|b| \geq 1$, luego el conjunto

$$I = \{x \in \mathbb{Z} \mid x|b| \leq |a|\}$$

está acotado superiormente por $|a|$. En efecto, para todo $x \in I$ es $x = x \cdot 1 \leq x|b| \leq |a|$. Aplicando a I el principio de la buena ordenación, deducimos que tiene un

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

máximo q_1. Poniendo $r_1 = |a| - q_1|b|$ vemos que $0 \leq r_1$ porque $q_1 \in I$. Supongamos, por un momentro, que $r_1 = 0$; entonces $|a| = q_1|b|$, de donde $a = (\pm q_1)b$ y el resultado estaría probado tomando $q = \pm q_1$ (según el caso) y $r = 0$. Así pues, de ahora en adelante suponemos que $r_1 > 0$.

Por otra parte, si fuese $r_1 \geq |b|$, podríamos escribir $r_1 = |b| + r'$ con $r' \geq 0$; así $|b| + r' = |a| - q_1|b|$, de donde $0 \leq r' = |a| - (q_1 + 1)|b|$ y así $(q_1 + 1)|b| \leq |a|$, luego $(q_1+1) \in I$, lo que contradice la hipótesis de ser q_1 el máximo de I. De aquí se deduce que $0 < r_1 < |b|$. También se deduce de este razonamiento que $(q_1 + 1)|b| > |a|$ y

$$(q_1 + 1)|b| - |a| = q_1|b| - |a| + |b| = |b| - r_1 \, .$$

Poniendo $q_2 = q_1 + 1$ y $r_2 = |b| - r_1$ tenemos que $r_2 > 0$ porque $r_1 < |b|$ y $r_2 < |b|$ porque $r_1 > 0$. Además, $|a| = q_2|b| - r_2$.

Para terminar la demostración de la existencia de q y r tenemos que considerar dos casos:

1. Si $a > 0$, tomamos la relación $a = |a| = q_1|b| + r_1$, luego $a = (\pm q_1)b + r_1$ y, poniendo $q = \pm q_1$ (según el caso) y $r = r_1$, se tiene el enunciado.

2. Si $a < 0$ tomamos la relación $a = -|a| = (-q_2)|b| - r_2$, luego $a = (\mp q_2)b + r_2$ y, poniendo $q = \mp q_2$ (según el caso) y $r = r_2$, se tiene el enunciado.

Esto prueba la parte de la existencia.

La demostración de la unicidad es mucho más corta. Supongamos que $a = qb + r = q'b + r'$ y, digamos, $r \geq r'$; entonces $r - r' = (q' - q)b$, luego $0 \leq r - r' = |q' - q||b|$. Como $r - r' \leq r < |b|$, la igualdad anterior sólo puede darse si $0 = r - r' = q' - q$. Esto prueba la unicidad y el teorema. □

Definición 4.1.2.– *Los números a y b del teorema 4.1.1 se llaman, respectivamente, el dividendo y divisor de la división euclídea. Los números q y r se llaman, respectivamente, el cociente y el resto. Cuando $a \neq 0 \neq b$ y el resto es cero se dirá que b divide a a y se escribirá $b|a$. En este caso, se dirá también que a es divisible por b o que b es un divisor de a. A los divisores de 1 se les llama unidades.*

Ejemplo 4.1.3.– Sean $a = 1436$, $b = 345$. Las cuatro posibles divisiones euclídeas dan como cociente y resto:

1. La división de a por b da $q = 4$, $r = 56$, es decir

$$1436 = 4 \cdot 345 + 56 \, .$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

2. La división de $-a$ por b da $q = -5$, $r = 289$, es decir

$$-1436 = (-5) \cdot 345 + 289\,.$$

3. La división de a por $-b$ da $q = -4$, $r = 56$, es decir

$$1436 = (-4) \cdot (-345) + 56\,.$$

4. La división de $-a$ por $-b$ da $q = 5$, $r = 289$, es decir

$$-1436 = 5 \cdot (-345) + 289\,.$$

Finalizamos esta sección con unas observaciones sencillas sobre el principio de recurrencia.

Nota 4.1.4.– Normalmente utilizaremos el principio de recurrencia ascendente, combinándolo con la definición de un conjunto de números por una propiedad. En este caso se procederá así: sea P una propiedad relativa a números enteros y supongamos que

1. El entero s_0 satisface P.
2. Si $s \geq s_0$ verifica P, entonces $s + 1$ verifica P

Bajo estas condiciones, todos los números mayores o iguales que s_0 verifican P. En efecto, esto se reduce al principio de recurrencia ascendente, definiendo S como el conjunto de los enteros que satisfacen la propiedad P.

Un ejemplo servirá de aclaración. Vamos a probar que, para todo $n \geq 0$, es

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\,.$$

La demostración por inducción, según lo anterior, requiere los pasos siguientes:

1. Hay que ver que la propiedad de suma indicada más arriba se verifica para $n = 0$. En efecto,

$$\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}\,.$$

2. Hay que ver que, si $n \geq 1$ verifica la propiedad de suma indicada más arriba, también la verifica $n+1$. En efecto, supongamos que

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Entonces tenemos que

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \left(\sum_{i=0}^{n} i\right) + (n+1) = \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n^2+n}{2} + (n+1) = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

Esto prueba que la propiedad de la suma se verifica para todo $n \geq 1$.

4.2. El máximo común divisor

Desarrollamos el concepto y el algoritmo más básicos de la teoría clásica de los números enteros. Las nociones de partida las hemos ya dado en la definición 4.1.2.

Notas 4.2.1.– Damos unas cuantas propiedades elementales de la divisibilidad.

4.2.1.1. Si $a \in \mathbb{Z}$ divide a una unidad, es una unidad. En efecto, sea u una unidad tal que $a|u$; entonces $u = a'a$ y existe u' tal que $1 = u'u$. Por tanto, $1 = (u'a')a$ y así a es una unidad.

4.2.1.2. Las únicas unidades de $\mathbb{Z}$ son 1 y -1. En efecto, tanto 1 como -1 son unidades porque $1 \cdot 1 = 1$ y $(-1)(-1) = 1$. Sean $a, b \in \mathbb{Z}$ tales que $ab = 1$; entonces $a \neq 0 \neq b$. Ahora bien, o a, b son ambos positivos o ambos negativos. Si son negativos, se pone $(-a)(-b) = 1$, con lo que se puede suponer que ambos son positivos. En este caso, si fuese a ó b mayor que 1 (por ejemplo a), sería $a > 1$ y $b > 0$ (luego $b \geq 1$) sería $ab > 1 \cdot b = b \geq 1$, luego $ab > 1$, lo que no puede ser. Así, $a = b = 1$, luego desde el principio $a = \pm 1$, $b = \pm 1$.

4.2.1.3. Las unidades son los únicos elementos que dividen a todos los enteros no nulos. En efecto, para todo $a \in \mathbb{Z}$, $a \neq 0$, es $a = 1 \cdot a$ y $a = (-1)(-a)$. Recíprocamente, si un entero divide a todos los enteros no nulos, divide a 1 luego es una unidad.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

4.2.1.4. Por convenio, y para no introducir demasiada asimetría en los enunciados, diremos que cualquier número no nulo divide a cero y que cero no divide a ningún número.

4.2.1.5. La relación de divisibilidad verifica las propiedades siguientes:

1. Propiedad reflexiva: $a|a$. En efecto, $a = 1 \cdot a$.
2. Propiedad antisimétrica: $a|b$ y $b|a$ implican que $a = \pm b$. En efecto, existen c, c' tales que $b = ac$ y $a = bc'$. Así $a = acc'$, luego $a - acc' = a(1 - cc') = 0$. Como $a \neq 0$ por definición de divisibilidad, es $1 - cc' = 0$ luego $cc' = 1$, de donde $c' = \pm 1$ y así $a = \pm b$.
3. Propiedad transitiva: Si $a|b$ y $b|c$ entonces $a|c$. En efecto, existen d, d' tales que $b = ad$ y $c = bd'$, luego $c = add'$ lo que implica que $a|c$.

Por consiguiente, si nos restringimos a enteros positivos, la divisibilidad es una relación de orden parcial porque la propiedad antisimétrica se enuncia así: $a|b$ y $b|a \Longrightarrow a = b$.

4.2.1.6. La divisibilidad es compatible con las operaciones aritméticas. En concreto:

1. Si $a|b$ y $a|c$ entonces $a|(b \pm c)$. En efecto, existen $d, d' \in \mathbb{Z}$ tales que $b = ad$ y $c = ad'$. Así
$$b \pm c = ad \pm ad' = a(d \pm d')\,,$$
luego $a|(b \pm c)$.
2. Si $a|b$ entonces $a|bc$, $\forall c \in \mathbb{Z}$. En efecto, existe $d \in \mathbb{Z}$ tal que $b = ad$. Así $bc = adc$, luego $a|bc$.

Definición 4.2.2.– *Dados dos enteros a, b no ambos nulos, se llama un máximo común divisor de a y b a todo entero $d \neq 0$ que verifique:*

1. *$d|a$ y $d|b$.*
2. *Si $d' \neq 0$ es tal que $d'|a$ y $d'|b$ entonces $d'|d$.*

Nótese que la propia definición determina unívocamente al máximo común divisor de a y b salvo signo. Haciendo el convenio de tomar siempre el positivo, podemos decir que el máximo común divisor es único, si existe, y se le denota por $d = \text{m.c.d}\,(a, b)$. También, si $d = \text{m.c.d}\,(a, b)$, es $d = \text{m.c.d}\,(\pm a, \pm b)$, luego, salvo aviso en contrario,

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

siempre hablaremos del máximo común divisor de dos enteros positivos, conviniendo en que $\text{m.c.d}\,(0,b)=b$. *Si* $d=1$ *se dice que* a *y* b *son primos entre sí.*

Naturalmente, lo primero que tenemos que hacer es demostrar que el máximo común divisor de dos números existe. Esto se hace mediante el algoritmo de Euclides, que se apoya en una una sencilla observación:

Nota 4.2.3.– Sean $a,b\in\mathbb{Z}$, $b\neq 0$ y sea $a=q\,b+r$ la división euclídea. Si existe $\text{m.c.d}\,(a,b)$ entonces existe $\text{m.c.d}\,(b,r)$ y $\text{m.c.d}\,(a,b)=\text{m.c.d}\,(b,r)$. Para demostrar esta afirmación basta ver que el conjunto de los enteros que dividen simultáneamente a a y b es el mismo que el de los que dividen simultáneamente a b y r. Pero eso es muy sencillo por 4.2.1.6. En efecto, si $c|a$ y $c|b$ entonces $c|q\,b$ y $c|(a-q\,b)=r$, luego $c|b$ y $c|r$. Recíprocamente, si $c|b$ y $c|r$ entonces $c|q\,b$ luego $c|(q\,b+r)=a$, de donde $c|a$ y $c|b$.

Notas 4.2.4.– El algoritmo de Euclides Sean $a,b\in\mathbb{Z}$, $b\neq 0$ fijos.

4.2.4.1. El algoritmo de Euclides: Creamos tres posiciones de memoria `A,B,R`.
Paso 1 Situación inicial: Inicialmente se coloca en `A` el número a, en `B` el número b y en `R` el resto de la división euclídea de a entre b.
Paso 2 Bucle: Mientras el contenido de `R` sea distinto de cero, se coloca el contenido de `B` en `A`, el `R` en `B` y `R` se rellena con el resto de la división de `A` entre `B`.

Nótese que el algoritmo anterior debe terminar necesariamente, es decir, que el bucle se ejecuta solamente un número finito de veces. En efecto, en cada paso del bucle se almacena en `R` el resto de una división, *que va a ser el divisor de la siguiente.* Así pues, los contenidos de `R` son siempre números positivos que decrecen. Esto sólo se puede dar un número finito de veces. Nótese también que, en cada paso del bucle, el máximo común divisor de `A` y `B` es igual a $\text{m.c.d}\,(a,b)$, si éste existe. El final es un contenido de `R` igual a cero, en cuyo caso el algoritmo devuelve el contenido de `B`.

Si $c\in\mathbb{Z}$ es el contenido de `A` y $d\in\mathbb{Z}$ es el contenido de `B`, entonces $d|c$, luego existe el máximo común divisor de c y d y es $\text{m.c.d}\,(c,d)=d$. Por tanto, $\text{m.c.d}\,(a,b)=d$, lo que prueba dos cosas:

1. Que existe el máximo común divisor de dos números cualesquiera, a,b, $b\neq 0$.
2. Que ese máximo común divisor se puede calcular mediante un número finito de divisiones.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

4.2.4.2. Calculemos, por ejemplo, m.c.d $(66612, 9114)$. Tenemos las sucesivas divisiones euclídeas siguientes, siguiendo las pautas del algoritmo:

A= 66612	B= 9114	R= 2814
A= 9114	B= 2814	R= 672
A= 2814	B= 672	R= 126
A= 672	B= 126	R= 42
A= 126	B= 42	R= 0

Aquí se detiene el algoritmo y produce como salida 42, que es el máximo común divisor de los números dados.

4.2.4.3. Nótese que la cadena de divisiones de 4.2.4.2 se puede escribir una manera ligeramente distinta. En esa cadena hemos omitido los cocientes; vamos a añadirlos dentro de una nueva variable Q:

A= 66612	B= 9114	Q= 7	R= 2814
A= 9114	B= 2814	Q= 3	R= 672
A= 2814	B= 672	Q= 4	R= 126
A= 672	B= 126	Q= 5	R= 42
A= 126	B= 42	Q= 3	R= 0

De la igualdad que establece la división euclídea se deduce que

$$\begin{aligned}
\frac{66612}{9114} &= 7+\frac{2814}{9114} = 7+\frac{1}{\frac{9114}{2814}} \\
&= 7+\frac{1}{3+\frac{672}{2814}} = 7+\frac{1}{3+\frac{1}{\frac{2814}{672}}} \\
&= 7+\frac{1}{3+\frac{1}{4+\frac{126}{672}}} = 7+\frac{1}{3+\frac{1}{4+\frac{1}{\frac{672}{126}}}} \\
&= 7+\frac{1}{3+\frac{1}{4+\frac{1}{5+\frac{42}{126}}}} = 7+\frac{1}{3+\frac{1}{4+\frac{1}{5+\frac{1}{\frac{126}{42}}}}}
\end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

$$= 7 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{3}}}}$$

Esta última expresión se llama una *fracción continua*.

Toda fracción continua se puede reducir a una fracción ordinaria, efectuando las operaciones indicadas, de abajo arriba. Por ejemplo, en el caso anterior, tenemos

$$\begin{aligned} 7 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{3}}}} &= 7 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{\cfrac{16}{3}}}} = 7 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{3}{16}}} \\ &= 7 + \cfrac{1}{3 + \cfrac{1}{\cfrac{67}{16}}} = 7 + \cfrac{1}{3 + \cfrac{16}{67}} \\ &= 7 + \cfrac{1}{\cfrac{217}{67}} = 7 + \frac{67}{217} \\ &= \frac{1586}{217}\,. \end{aligned}$$

Se obtiene así, la fracción inicial en su forma irreducible, es decir, sin divisores comunes entre el numerador y el denominador. Como el máximo común divisor del numerador y denominador de la fracción inicial era 42, vemos que

$$\frac{66612}{9114} = \frac{1586 \cdot 42}{217 \cdot 42}\,.$$

Otra posible interpretación de este hecho es que, dado el máximo común divisor y la lista ordenada de cocientes, se pueden reconstruir los números, bien por el procedimiento de la fracción continua, bien reconstruyendo de abajo arriba la lista de divisiones del algoritmo de Euclides.

4.2.4.4. Los hechos apuntados en 4.2.4.3 son completamente generales. Sean $a > b > 0$ dos números enteros y escribamos la cadena de divisiones que constituye el algoritmo de Euclides en la forma

$$a = q_1 b + r_1$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

$$\begin{aligned} b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ \vdots &= \vdots \\ r_n &= q_{n+2} r_{n+1} + r_{n+2} \\ r_{n+1} &= q_{n+3} r_{n+2}\,. \end{aligned}$$

Tenemos que

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \cfrac{1}{\cfrac{b}{r_1}}$$

y que

$$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1} = q_2 + \cfrac{1}{\cfrac{r_1}{r_2}}$$

luego

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cfrac{r_1}{r_2}}}\,.$$

Por construcción es evidente que, continuando la aplicación de este algoritmo, llegamos a que

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{r_{n+1}}{r_{n+2}}} = q_1 + \cfrac{1}{q_2 + \ddots + q_{n+2} + \cfrac{1}{\cfrac{r_{n+1}}{r_{n+2}}}}$$

luego a que

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \ddots + q_{n+2} + \cfrac{1}{q_{n+3}}}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Recíprocamente, supongamos que partimos de la fracción continua

$$q_1 + \cfrac{1}{q_2 + \ddots + q_{n+2} + \cfrac{1}{q_{n+3}}}$$

y la calculamos de abajo arriba, obtenemos lo que se obtendría del algoritmo de Euclides anterior haciendo $r_{n+2} = 1$. Como $r_{n+2} = \text{m.c.d}\,(a, b)$, lo que se obtiene es la reducción de a/b a su forma irreducible.

Nota 4.2.5.– Vamos a dar un algoritmo con números enteros que extiende el algoritmo de Euclides, del que sacaremos toda la teoría de la divisibilidad de los enteros. Como el algoritmo de Euclides, el nuevo algoritmo parte de dos enteros a, b , $b \neq 0$ y devuelve un vector $\mathbf{u} = (u_1, u_2, u_3)$ tal que $u_3 = \text{m.c.d}\,(a, b)$ y $u_1 a + u_2 b = u_3$.

El algoritmo consta de una serie de divisiones euclídeas y emplea los vectores auxiliares $\mathbf{u} = (u_1, u_2, u_3)$, $\mathbf{v} = (v_1, v_2, v_3)$ y $\mathbf{t} = (t_1, t_2, t_3)$. Es como sigue:

Paso 1: (Inicialización) Se define

$$(u_1, u_2, u_3) := (1, 0, a), \quad (v_1, v_2, v_3) := (0, 1, b)$$

Evidentemente se verifica, al inicio, que

$$u_1 a + u_2 b = u_3\,, \quad v_1 a + v_2 b = v_3\,.$$

Paso 2: bucle Mientras que $v_3 \neq 0$ hacer lo siguiente: hallar el cociente q de la división euclídea de u_3 entre v_3 y poner

$$\begin{aligned} (t_1, t_2, t_3) &:= (u_1, u_2, u_3) - q(v_1, v_2, v_3) \\ (u_1, u_2, u_3) &:= (v_1, v_2, v_3) \\ (v_1, v_2, v_3) &:= (t_1, t_2, t_3) \end{aligned}$$

Conforme se va recorriendo el bucle, la primera línea nos dice que en t_3 se van a almacenar los restos de las divisiones de u_3 entre v_3. La segunda línea dice simplemente que el vector $\mathbf{u}$ del paso siguiente va a ser el $\mathbf{v}$ actual. La tercera línea dice que el vector $\mathbf{v}$ del paso siguiente va a ser el $\mathbf{t}$ actual. Esto nos dice que los suvesivos u_3, v_3, q, t_3 van a ser, respectivamente, los dividiendos, divisores, cocientes

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

y restos del algoritmo de Euclides. Esto implica que el algoritmo es finito, o sea que termina. Al terminar, el algoritmo devuelve el vector $\mathbf{u}$, cuya tercera componente es $u_3 = \text{m.c.d}\,(a, b)$.

A lo largo de todos los pasos del bucle es

$$u_1 a + u_2 a = u_3\,, \quad v_1 a + v_2 a = v_3\,, \quad t_1 a + t_2 b = t_3\,.$$

En efecto, a la vista de que las dos primeras relaciones se verifican al comienzo, sólo hay que demostrar la tercera, al cabo de una pasada en el bucle porque la estructura del bucle lleva a que esas igualdades se propagan. Pero

$$(u_1 - q v_1)a + (u_2 - q v_2)b = (u_1 a + u_2 b) - q(v_1 a + v_2 b) = u_3 - q v_3\,,$$

con lo que queda establecida nuestra afirmación.

Veamos cómo funciona este algoritmo para calcular el máximo común divisor y la identidad de Bézout en el caso de $u = 66612$ y $v = 9114$.

u_1	u_2	u_3	v_1	v_2	v_3	t_1	t_2	t_3	q
1	0	66612	0	1	9114	1	−7	2814	7
0	1	9114	1	−7	2814	−3	22	672	3
1	−7	2814	−3	22	672	13	−95	126	4
−3	22	672	13	−95	126	−68	497	42	5
13	−95	126	−68	497	42	217	−1586	0	3
−68	497	42	217	−1586	0				

y $-68 * 66612 + 497 * 9114 = 42$.

Definición 4.2.6.– *El algoritmo de la nota 4.2.5 se llama el algoritmo de Euclides extendido. Si* $\mathbf{u} = (u_1, u_2, u_3)$ *es el vector de salida (recordando que* $u_3 = \text{m.c.d}\,(a, b)$*), la relación* $u_1 a + u_2 b = u_3$ *se llama una identidad de Bézout. Hay infinitas identidades de Bézout: para cada* $z \in \mathbb{Z}$*, es*

$$(u_1 - z\,b)a + (u_2 + z\,a)b = u_3$$

Teorema 4.2.7.– Existencia del mínimo común múltiplo. *Dados dos números* $a, b > 1$*, existe un único* $m > 0$ *que verifica:*

1. $a|m$ *y* $b|m$.
2. *Si* $m' > 0$ *es tal que* $a|m'$ *y* $b|m'$ *entonces* $m|m'$.

A este entero se le llama el mínimo común múltiplo de a y b y se le denota $m = \mathrm{m.c.m}\,(a, b)$.

Demostración: Es evidente que

$$m = \frac{a\,b}{\mathrm{m.c.d}\,(a, b)}\,.$$

□

4.3. Aplicación del máximo común divisor: divisibilidad

En esta sección dsarrollamos la teoría clásica de la divisibilidad de enteros.

Definición 4.3.1.– *Un entero p se llama primo si y sólo si no es cero ni una unidad y es divisible únicamente por $\pm p$ y ± 1. Nótese que, si p es primo, $-p$ lo es también. En general reservaremos el nombre de primo para los positivos.*

Notas 4.3.2.– En general, averiguar si un número es primo o no, es un problema abierto. Naturalmente, la dificultad estriba en los números grandes. Con medios modestos se puede hacer una tabla de números primos hasta un cierto límite mediante un procedimiento llamado la *criba de Eratóstenes*.

4.3.2.1. El principio de la criba de Eratóstenes es sencillo. Se escribe una lista de todos los enteros desde 1 hasta n. Con ella procedemos así:

1. Tachamos el 1 porque no es primo y vamos al siguiente número.
2. Si, en un estadio determinado, estamos sobre el número m no tachado, tachamos todos los número $2m$, $3m$, etc, que quepan en la lista.

Los números que quedan sin tachar son todos los primos que hay entre 1 y n.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

4.3.2.2. Por ejemplo, queremos hallar todos los primos entre 1 y 100. Para ello escribimos la lista

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

con el 1 tachado (marcado). Nos vamos al siguiente número no tachado que es el 2, y tachamos los números $2 \cdot 2$, $2 \cdot 3$, $2 \cdot 4$, ..., $2 \cdot 50 = 100$:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Ahora nos vamos al siguiente no tachado, que es el 3, y tachamos $3 \cdot 2$, $3 \cdot 3$, $3 \cdot 4$, etc. Naturalmente, si encontramos un número previamente tachado, no hacemos nada

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

porque ya lo está.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Ahora nos vamos al siguiente no tachado, que es el 5, y tachamos $5 \cdot 2$, $5 \cdot 3$, $5 \cdot 4$, etc. Naturalmente, si encontramos un número previamente tachado, no hacemos nada porque ya lo está.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Ahora nos vamos al siguiente no tachado, que es el 7, y tachamos $7 \cdot 2$, $7 \cdot 3$, $7 \cdot 4$, etc. Naturalmente, si encontramos un número previamente tachado, no hacemos nada

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

porque ya lo está.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Ahora nos vamos al siguiente no tachado, que es el 11, y tachamos $11 \cdot 2$, $11 \cdot 3$, $11 \cdot 4$, etc. Como todos están ya tachados, el cuadro no varía. ¿Por qué está todos tachados? Porque los números de la forma $11 \cdot m$ menores que 100 son

$$11 \cdot 2\,, 11 \cdot 3\,, 11 \cdot 4\,, 11 \cdot 5\,, 11 \cdot 6\,, 11 \cdot 7\,, 11 \cdot 8\,, 11 \cdot 9\,,$$

y todos ellos están ya tachados como múltiplos de 2, 3, 5 y 7. Lo mismo ocurre para los números no tachados mayores que 11, luego hemos terminado de construir la criba de Eratóstenes. Los números primos menores que 100 son los que quedan sin tachar en el último cuadro.

4.3.2.3. Normalmente los sistemas de cálculo simbólico tienen una lista muy grande de números primos almacenada en la memoria del sistema. Esto les permite definir, dentro de un cierto límite, la función "primo n-ésimo" y la función "primo siguiente", de manera obvia. Usando nuestro modesto cuadro, podemos ver, por ejemplo, que el primo decimotercero es 41 y que el primo siguiente a 75 es 79.

La aplicación central del máximo común divisor es el siguiente teorema 4.3.3, que nos permite demostrar la parte más difícil de la factorización: la unicidad.

Teorema 4.3.3.– Teorema de Euclides. *Sean a, b, c distintos de cero tales que $c|ab$ y $\text{m.c.d}\,(c, a) = 1$; entonces $c|b$. En particular, si p es primo, $p|ab$ y $p \not| a$, entonces $p|b$ (el signo $\not|$ significa "no divide").*

Demostración: Evidentemente, la segunda afirmación es consecuencia de la primera; demostremos ésta. Por la identidad de Bézout, existen $\alpha, \beta \in \mathbb{Z}$ tales que $1 = \alpha\, c + \beta\, a$. Así, $b = \alpha\, b\, c + \beta\, b\, a$. Como $c|ab$ y $c|bc$, lo anterior implica que $c|b$, que es lo que queríamos demostrar. □

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Teorema 4.3.4.– TEOREMA FUNDAMENTAL DE LA DIVISIBILIDAD*: Toda no unidad distinta de cero se descompone en producto finito de números primos. Esta descomposición es única salvo orden y producto por unidades.*

Demostración: Vamos primero a demostrar la existencia de la descomposición. Sea $n \neq 0$ $n \neq \pm 1$ un entero fijo, y vamos a demostrar que n se descompone en producto de primos. Podemos suponer que $n > 0$ porque, si lo demostramos en este caso y $n = p_1 \cdots p_r$, entonces $-n = (-1)p_1 \cdots p_r$, lo que lo demuestra para los negativos.

La existencia de la descomposición se prueba por recurrencia a partir de $n = 2$. El número $n = 2$ es primo. Supongamos que $n > 2$ y que todos los números menores que n se descomponen en producto finito de primos. Si n es primo hemos terminado: es producto de un primo (él mismo). Si no lo es, se descompone en producto $n = n_1 n_2$ de dos enteros positivos estrictamente menores que n. Al aplicar a n_1 y n_2 la hipótesis de recurrencia, vemos que n se descompone en producto finito de primos.

Para demostrar la unicidad (salvo orden y producto por unidades), basta considerar enteros positivos n por la misma razón que antes. Además, basta ver que no puede haber dos descomposiciones esencialmente distintas de un mismo número positivo en producto de primos positivos. Sean

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

dos descomposiciones de n en producto de primos positivos. Por el teorema de Euclides (teorema 4.3.3), el primo p_1 debe figurar entre los q_i, digamos $p_1 = q_1$. Cancelando tenemos

$$p_2 \cdots p_r = q_2 \cdots q_s$$

y continuando el razonamiento vemos que las dos descomposiciones son iguales (salvo orden, claro). □

Teorema 4.3.5.– (EUCLIDES) *El conjunto de los primos es infinito.*

Demostración: Supongamos que no, es decir que el conjunto de los primos fuese finito, y sean $p_1, \ldots, p_r$ todos los primos. Sea $n = p_1 \cdots p_r + 1$. Por la existencia de la factorización en producto de primos (teorema 4.3.4), n debe ser divisible por algún p_i, lo que implicaría que $p_i | 1$ y eso es imposible. □

Nota 4.3.6.– La factorización única de un entero positivo n la escribiremos usualmente en la forma

$$n = \prod_{p \text{ primo}} p^{\nu_n(p)}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

donde todos los $\nu_n(p)$ son cero salvo un número finito. Esta notación se puede extender a enteros $n < 0$ poniendo

$$n = (-1) \prod_{p \text{ primo}} p^{\nu_{-n}(p)} .$$

Sin embargo, la noción de número primo la reservaremos para los positivos, como hemos dicho antes.

Nota 4.3.7.– Una cosa es demostrar que existe la factorización y otra muy distinta calcularla. El cálculo de la factorización de un número es un problema muy difícil en general. En esta dificultad se basa la "seguridad" de los métodos de codificación de clave pública. La codificación depende de la factorización de un número. Aunque sea teóricamente posible el efectuarla, en la práctica puede requerir millones de años de computador el hacerla, si el número es muy grande y de un tipo especial. Por eso, estos sistemas de codificación se consideran "seguros".

Hay un método clásico, que funciona bien sólo en ciertos casos, que se llama también la *criba de Eratóstenes* porque depende esencialmente de la vista en 4.3.2. Suponemos construida una lista de todos los primos hasta un cierto número, bien a mano por la criba de Eratóstenes, bien almacenados en la memoria de un computador. Dado un entero positivo, se trata de ir probando primos que puedan dividirlo; si se encuentran, se divide y se comienza de nuevo. Si no se encuentra ninguno, se da como salida el número, lo que indicará que es primo. Escribimos ahora su seudocódigo, usando la función "primo siguiente", que toma un argumento `i` y devuelve el primer primo estrictamente mayor que `i`.

La entrada es un número $n > 1$. Se crean dos posiciones de memoria, `N` y `P`, almanenando en ellas al principio `N`$= n$ y `P`$= 2$. El algoritmo se describe en un único paso general:

Paso general: Si `P` divide a `N`, se escribe en `N` el cociente de `N` por `P` y se recomienza siempre que `N` sea mayor que 1. Si `P` no divide a `N`, se escribe en `P` primo siguiente al almacenado antes en `P` y se recomienza.

La criba de Eratóstenes para factorizar un número funciona bien cuando los divisores del número sean pequeños, aunque el número en sí pueda ser grande. Por ejemplo, para

$$n = 23572201153694123824389928575000 00$$

la criba nos daría en poco tiempo $n = 2^5 \cdot 3^4 \cdot 5^7 \cdot 11^{23} \cdot 13$. La criba de Eratóstenes colapsará completamente para números con todos sus factores primos muy grandes.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Por supuesto que hay otros métodos de factorización, que están diseñados para números con todos sus factores primos muy grandes. Sin embargo, antes o después, pueden colapsar. Éste es uno de los grandes retos que tiene hoy día la computación.

Notas 4.3.8.– Veamos unas cuantas propiedades del máximo común divisor y del mínimo común múltiplo, usando la factorización única.

4.3.8.1. Sea

$$d = \text{m.c.d}\,(a,b), \quad a' = \frac{a}{d}, \quad , b' = \frac{b}{d}\,.$$

Entonces a', b' son primos entre sí porque si no, existiría $d' \neq 1$ tal que $d'|a'$ y $d'|b'$. Entonces sería $d < dd'|a$, $dd'|b$, lo que no es posible.

4.3.8.2. Sean $a, b \in \mathbb{Z}_+$ y consideremos sus descomposiciones factoriales

$$a = \prod_{p \text{ primo}} p^{\nu_a(p)}\,, \quad b = \prod_{p \text{ primo}} p^{\nu_b(p)}\,.$$

Leyendo con atención la definición de máximo común divisor y de mínimo común múltiplo se ve que

$$\text{m.c.d}\,(a,b) = \prod_{p \text{ primo}} p^{\text{mín}(\nu_a(p),\nu_b(p))}\,, \quad \text{m.c.m}\,(a,b) = \prod_{p \text{ primo}} p^{\text{máx}(\nu_a(p),\nu_b(p))}\,.$$

4.3.8.3. De la expresión del máximo común divisor y del mínimo común múltiplo en función de la descomposición factorial se deducen las siguientes propiedades:

$$\begin{aligned}
\text{m.c.d}\,(a,b)c &= \text{m.c.d}\,(ac,bc)\\
\text{m.c.m}\,(a,b)c &= \text{m.c.m}\,(ac,bc)\\
\text{m.c.d}\,(\,\text{m.c.m}\,(a,b),\,\text{m.c.m}\,(a,c)) &= \text{m.c.m}\,(a,\,\text{m.c.d}\,(b,c))\\
\text{m.c.m}\,(\,\text{m.c.d}\,(a,b),\,\text{m.c.d}\,(a,c)) &= \text{m.c.d}\,(a,\,\text{m.c.m}\,(b,c))
\end{aligned}$$

4.4. Aplicación de la división euclídea: congruencias

La división euclídea nos conduce inmediatamente a la noción de congruencia de módulo dado.

Sea $m > 0$ un entero fijo, designemos por $\mathbb{Z}/\mathbb{Z}\,m$ al conjunto $\mathbb{Z}/\mathbb{Z}\,m = \{0, 1, \ldots, m-1\}$ y sea $C_m : \mathbb{Z} \to \mathbb{Z}/\mathbb{Z}\,m$ la función que, a cada entero n, hace corresponder el resto de su división euclídea por m. Al entero $C_m(n)$ se le llama la *congruencia*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

de n módulo m. Por ejemplo, si $m = 7$ y $n = -37$, es $-37 = (-6) \cdot t + 5$, luego $C_7(-37) = 5$ y 5 es la congruencia de -37 módulo m. Por tanto, al conjunto $\mathbb{Z}/\mathbb{Z}\,m$ lo llamamos el conjunto de las congruencias módulo m

Nota 4.4.1.– Para cada $r \in \mathbb{Z}/\mathbb{Z}\,m$, el conjunto $C_m^{-1}(r)$ es el de todos los enteros que, divididos por m, dan de resto r. Entonces

$$C_m^{-1}(r) = \{qm + r \mid q \in \mathbb{Z}\}\,,$$

luego, para todo $n_1\,, n_2 \in \mathbb{Z}$ tenemos

$$C_m(n_1) = C_m(n_2) \Longleftrightarrow m|(n_1 - n_2)\,.$$

En palabras: dos números dan el mismo resto al dividirlos por m si y sólo si m divide a la diferencia de ambos. En notación clásica, el hecho de que $C_m(n_1) = C_m(n_2)$ se expresa diciendo que n_1 y n_2 son *congruentes módulo* m y escribiendo $n_1 \equiv n_2 \pmod m$.

Notas 4.4.2.– Vamos a dotar al conjunto $\mathbb{Z}/\mathbb{Z}\,m$ de una estructura de anillo, utilizando la función C_m.

4.4.2.1. Se define la suma de dos elementos $r_1, r_2 \in \mathbb{Z}/\mathbb{Z}\,m$ como el resto de la división euclídea de $r_1 + r_2$ (como enteros) por m. Es decir, si, como enteros, $r_1 + r_2 = qm + r$, la suma de r_1 y r_2 como congruencias es $r_1 + r_2 = r$. Por ejemplo, en $\mathbb{Z}/\mathbb{Z}\,7$ es $6 + 5 = 4$ porque $11 = 1 \cdot 7 + 4$. Esta suma de congruencias verifica una propiedad esencial: si $n_1 \in C_m^{-1}(r_1)$ y $n_2 \in C_m^{-1}(r_2)$ son cualesquiera, entonces $C_m(n_1 + n_2) = r$. En efecto, si $n_1 = q_1 m + r_1$ y $n_2 = q_2 m + r_2$ es

$$n_1 + n_2 = (q_1 + q_2)m + (r_1 + r_2) = (q_1 + q_2 + q)m + r\,,$$

luego $C_m(n_1 + n_2) = r$. Esto se escribe poniendo que $C_m(n_1 + n_2) = C_m(n_1) + C_m(n_2)$, donde la suma en el primer miembro es de enteros y la del segundo, de congruencias.

4.4.2.2. Es fácil ver que, con la suma de congruencias, $\mathbb{Z}/\mathbb{Z}\,m$ es un grupo abeliano. En efecto, la propiedad conmutativa es muy clara, la congruencia 0 actúa como el cero del grupo y si $r \in \mathbb{Z}/\mathbb{Z}\,m$, el opuesto de r es

$$\begin{cases} 0 & \text{si} \quad r = 0 \\ m - r & \text{si} \quad r \neq 0\,. \end{cases}$$

La propiedad asociativa de la suma de congruencias es fácil de demostrar: si $r_1\,, r_2\,, r_3 \in \mathbb{Z}/\mathbb{Z}\,m$, y tomamos $n_i \in C_m^{-1}(r_i)$, $i = 1, 2, 3$, cualesquiera, entonces

$$(r_1 + r_2) + r_3 \;\; = \;\; (C_m(n_1) + C_m(n_2)) + C_m(n_3) = C_m(n_1 + n_2) + C_m(n_3)$$

$$\begin{aligned} &= C_m[(n_1+n_2)+n_3] = C_m[n_1+(n_2+n_3)] \\ &= C_m(n_1)+C_m(n_2+n_3) = C_m(n_1)+[C_m(n_2)+C_m(n_3)] \\ &= r_1+(r_2+r_3) \end{aligned}$$

4.4.2.3. Se define el producto de dos elementos $r_1, r_2 \in \mathbb{Z}/\mathbb{Z}\,m$ como el resto de la división euclídea de $r_1 r_2$ (como enteros) por m. Es decir, si, como enteros, $r_1 r_2 = qm + r$, el producto de r_1 y r_2 como congruencias es $r_1 r_2 = r$. Por ejemplo, en $\mathbb{Z}/\mathbb{Z}\,7$ es $6 \cdot 5 = 2$ porque $30 = 4 \cdot 7 + 2$. Este producto de congruencias verifica una propiedad esencial: si $n_1 \in C_m^{-1}(r_1)$ y $n_2 \in C_m^{-1}(r_2)$ son cualesquiera, entonces $C_m(n_1 n_2) = r$. En efecto, si $n_1 = q_1 m + r_1$ y $n_2 = q_2 m + r_2$ es

$$n_1 n_2 = (q_1 q_2 + q_1 r_2 + q_2 r_1)m + (r_1 r_2) = (q_1 q_2 + q_1 r_2 + q_2 r_1 + q)m + r\,,$$

luego $C_m(n_1 n_2) = r$. Esto se escribe poniendo que $C_m(n_1 n_2) = C_m(n_1) C_m(n_2)$, donde el producto en el primer miembro es de enteros y en el segundo, de congruencias.

4.4.2.4. Con estas dos operaciones, $\mathbb{Z}/\mathbb{Z}\,m$ es un anillo, en el que 1 es el elemento unidad si $m > 1$ (nótese que $\mathbb{Z}/\mathbb{Z}\,1 = \{0\}$).

4.4.2.5. Como ejemplos creamos una tabla de sumar y otra de multiplicar de las congruencias módulos 4 y 5.

Para $\mathbb{Z}/\mathbb{Z}\,4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Para $\mathbb{Z}/\mathbb{Z}\,5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

La explicación de estas tablas es que, como en el clásico juego de los barcos, dentro de cada cuadrado completo está la suma o el producto de las congruencias representadas por el correspondiente número de más a la izquierda en su línea horizontal y el de más arriba en su línea vertical.

4.4.2.6. Entre estos dos anillos de congruencias hay una diferencia esencial. Fijémonos en las tablas de multiplicar. En el caso de $\mathbb{Z}/\mathbb{Z}\,5$, para todo par de elementos $a\,, b \in \mathbb{Z}/\mathbb{Z}\,5$, $b \neq 0$, existe $c \in \mathbb{Z}/\mathbb{Z}\,5$ tal que $a = bc$. Esto lo expresaremos diciendo que todo $0 \neq b \in \mathbb{Z}/\mathbb{Z}\,5$ es tal que se puede dividir por él todo elemento de $\mathbb{Z}/\mathbb{Z}\,5$, y escribiremos que $a/b = c$. Para demostrar esto nos fijamos en la segunda, tercera, cuarta y quinta filas de la tabla de multiplicar. Tenemos:

1. La segunda fila nos dice que
$$\frac{0}{1} = 0 \quad , \quad \frac{1}{1} = 1 \quad , \quad \frac{2}{1} = 2 \quad , \quad \frac{3}{1} = 3 \quad , \quad \frac{4}{1} = 5\,.$$
2. La tercera fila nos dice que
$$\frac{0}{2} = 0 \quad , \quad \frac{1}{2} = 3 \quad , \quad \frac{2}{2} = 1 \quad , \quad \frac{3}{2} = 4 \quad , \quad \frac{4}{2} = 2\,.$$
3. La cuarta fila nos dice que
$$\frac{0}{3} = 0 \quad , \quad \frac{1}{3} = 2 \quad , \quad \frac{2}{3} = 4 \quad , \quad \frac{3}{3} = 1 \quad , \quad \frac{4}{3} = 3\,.$$
4. La quinta fila nos dice que
$$\frac{0}{4} = 0 \quad , \quad \frac{1}{4} = 4 \quad , \quad \frac{2}{4} = 3 \quad , \quad \frac{3}{4} = 2 \quad , \quad \frac{4}{4} = 1\,.$$

En cambio, la tabla de multiplicar de $\mathbb{Z}/\mathbb{Z}\,4$ nos dice que se puede dividir todo elemento de $\mathbb{Z}/\mathbb{Z}\,4$ por 1 y por 3, pero no por 2. Por 2 sólo se pueden dividir 0 y 2, dando $0/2 = 0$, $2/2 = 1$.

El apartado 4.4.2.6 nos plantea la siguiente cuestión: si $n_1\,, n_2 \in \mathbb{Z}/\mathbb{Z}\,m$ son distintos de cero, ¿cuándo existe el cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$? Esto lo resolvemos en las notas siguientes (4.4.3).

Notas 4.4.3.– Vamos a operar dentro del anillo de congruencias $\mathbb{Z}/\mathbb{Z}\,m$, con $m > 1$.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

4.4.3.1. Sea $n \in \mathbb{Z}$, $0 < n < m$, $d = \text{m.c.d}\,(n, m)$, $d = \alpha n + \beta m$ una identidad de Bézout, $m = m'd$, $n = n'd$, de tal manera que $\text{m.c.d}\,(m', n') = 1$. Entonces está claro que existe el cociente n/d en $\mathbb{Z}/\mathbb{Z}\,m$ y $n/d = n'$. También existe el cociente d/n en $\mathbb{Z}/\mathbb{Z}\,m$ porque, de la identidad de Bézout, se deduce que $d = C_m(\alpha)n$, luego $d/n = C_m(\alpha)$ en $\mathbb{Z}/\mathbb{Z}\,m$. Hay que tener un cuidado extremo con el manejo de los cocientes en un anillo de congruencias, porque tienen unas propiedades a las que no estamos acostumbrados por las enseñanzas elementales de Matemáticas:

1. Los cocientes *no son únicos*. Por ejemplo, si $m = 30$, $n = 12$, es $d = 6$, $6 = (-2) \cdot 12 + 1 \cdot 30$, $30 = 5 \cdot 6$, $12 = 2 \cdot 6$, luego

   a) En $\mathbb{Z}/\mathbb{Z}\,30$ es $12 = 2 \cdot 6$, $12 = 7 \cdot 6$, $12 = 12 \cdot 6$, $12 = 17 \cdot 6$, $12 = 22 \cdot 6$, $12 = 27 \cdot 6$, de donde $12/6$ es igual a cualquiera de las congruencias $2, 7, 12, 17, 22, 27$ al menos.

   b) En $\mathbb{Z}/\mathbb{Z}\,30$ es $6 = 3 \cdot 12$, $6 = 8 \cdot 12$, $6 = 13 \cdot 12$, $6 = 18 \cdot 12$, $6 = 23 \cdot 12$, $6 = 28 \cdot 12$, de donde $6/12$ es igual a cualquiera de las congruencias $3, 6, 13, 18, 23, 28$ al menos.

2. De que exista $12/6$ y $6/12$ no se puede deducir que, en $\mathbb{Z}/\mathbb{Z}\,30$, sea $(12/6)(6/12) = 1$; puede que sí y puede que no. Por ejemplo, si tomamos $12/6 = 2$ y $6/12 = 3$ es $2 \cdot 3 = 6 \neq 1$. En cambio, si tomamos $12/6 = 7$ y $6/12 = 13$, es $7 \cdot 13 = C_{30}(7 \cdot 13) = C_{30}(91) = 1$.

4.4.3.2. Sean ahora n_1, n_2 dos enteros, $0 < n_1, n_2 < m$, y vamos a ver cuándo existe un cociente de congruencias n_1/n_2. Sean $d_i = \text{m.c.d}\,(n_i, m)$, $i = 1, 2$, $n_i = n_i' d_i$ $m_i = m_i' d_i$, $1 = \text{m.c.d}\,(n_i', m_i')$, y $d_i = \alpha_i n_i + \beta_i m$ las identidades de Bézout. Si $d_2 | d_1$, es $d_1 = d' d_2$, luego $n_1 = n_1' d' d_2$ y, usando la correspondiente identidad de Bézout, tenemos

$$n_1 = n_1' d' (\alpha_2 n_2 + \beta_2 m) = n_1' d' \alpha_2 n_2 + n_1' d' \beta_2 m\,,$$

de donde $n_1 = C_m(n_1' d' \alpha_2) n_2$ y así existe un cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$.

Recíprocamente, supongamos que existe $n' \in \mathbb{Z}$, $0 < n' < m$ tal que $n_1 = n' n_2 + \gamma m$, es decir, que existe un cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$. Por la identidad de Bézout correspondiente tenemos:

$$\begin{aligned} d_1 &= \alpha_1 n_1 + \beta_1 m = \alpha_1 (n' n_2 + \gamma m) + \beta_1 m \\ &= \alpha_1 n' n_2 + (\alpha_1 \gamma + \beta_1) m = \alpha_1 n' n_2' d_2 + (\alpha_1 \gamma + \beta_1) m_2' d_2 \\ &= [\alpha_1 n' n_2' + (\alpha_1 \gamma + \beta_1) m_2'] d_2 \end{aligned}$$

luego $d_2|d_1$.

4.4.3.3. El resumen de 4.4.3.2 es el siguiente: Sean $n_1, n_2 \in \mathbb{Z}$, $0 < n_1, n_2 < m$; entonces existe un cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$ si y sólo si $\text{m.c.d}\,(n_2, m)$ divide a $\text{m.c.d}\,(n_1, m)$ en $\mathbb{Z}$.

4.4.3.4. Sigamos con las notaciones de 4.4.3.2 y supongamos que $d_2|d_1$, es decir, que existe el cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$. ¿Cuántos cocientes n_1/n_2 hay en $\mathbb{Z}/\mathbb{Z}\,m$?

Como existe el cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$, podemos escribir en $\mathbb{Z}$ que $n_1 = qn_2 + \alpha m$, $0 < q < m$. Por otra parte, si $k \in \mathbb{Z}$, entonces

$$(q + km_2')n_2 + \alpha m = (q + km_2')n_2'd_2 + \alpha m = qn_2 + (kn_2' + \alpha)m = n_1 + kn_2'm$$

de donde $n_1 = C_m(q + km_2')n_2$ y así $C_m(q + km_2') = q + C_m(km_2')$ es también un cociente n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$. Así pues, son cocientes n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$ todas las congruencias de la forma $q + k'm_2'$, de tal forma que $q + k'm_2' < m$. Para que se verifique esa condición, los valores posibles de k' son $k' = 0, 1, \ldots, d_2 - 1$ y ninguno más, porque $k' = d_2$ implica que $k'm_2' = 0$ en $\mathbb{Z}/\mathbb{Z}\,m$. Estas congruencias $\{0, m_2', \ldots, (d_2 - 1)m_2'\}$ son distintos porque, si hubiera dos iguales, digamos $im_2' = jm_2'$ con $i \geq j$, sería $(i-j)m_2' = hm = hd_2m_2'$, luego $(i-j) = hd_2$ y, como $i-j < d_2$, debe ser $i - j = 0$.

Recíprocamente, supongamos que hay dos cocientes n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$; entonces podemos escribir en $\mathbb{Z}$ que $n_1 = qn_2+km = q'n_2+k'm'$, luego $(q-q')n_2 = (k'-k)m$, de donde $(q - q')n_2' = (k' - k)m_2'$. Como $1 = \text{m.c.d}\,(n_2', m_2')$, debe ser $m_2'|(q - q')$ por el teorema de Euclides 4.3.3; así $q = q' + km_2'$.

4.4.3.5. El resumen de 4.4.3.3 es el siguiente: Si existe un cociente q de n_1/n_2 en $\mathbb{Z}/\mathbb{Z}\,m$, entonces hay exactamente d_2 cocientes distintos en $\mathbb{Z}/\mathbb{Z}\,m$, que son

$$q\,, q + m_2'\,, \ldots\,, q + (d_2 - 1)m_2'.$$

En el ejemplo de 4.4.3.3 vemos que un cociente $6/12$ en $\mathbb{Z}/\mathbb{Z}\,30$ es 3 y que $d_2 = 6$, $m_2' = 5$, luego hay seis cocientes, que son

$$3\,, 3 + 5 = 8\,, 3 + 2 \cdot 5 = 13\,, 3 + 3 \cdot 5 = 18\,, 3 + 4 \cdot 5 = 23\,, 3 + 5 \cdot 5 = 28\,.$$

Si hubiésemos partido de otro cociente, obtendríamos lo mismo pues, por ejemplo (teniendo en cuenta que operamos en $\mathbb{Z}/\mathbb{Z}\,30$), tomando 18 como cociente inicial, los cocientes serían

$$18\,, 18 + 5 = 23\,, 18 + 2 \cdot 5 = 28\,, 18 + 3 \cdot 5 = 3\,, 18 + 4 \cdot 5 = 8\,, 18 + 5 \cdot 5 = 13\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Notas 4.4.4.– Fijamos un entero $m > 1$ y el anillo de congruencias $\mathbb{Z}/\mathbb{Z}\,m$. Seguimos en la situación de las notas 4.4.3. La pregunta natural que surge es: ¿hay divisores "universales" en $\mathbb{Z}/\mathbb{Z}\,m$?. Es decir, ¿hay enteros n_2, $0 < n_2 < m$ tales que existe cualquier cociente n_1/n_2, para toda congruencia $n_1 \neq 0$?. Teniendo en cuenta las notas 4.4.3, la respuesta es que sí: $n_2 = 1$ porque 1 divide a cualquier enteros. Pero hay más.

4.4.4.1. Un n_2 que sea divisor universal debe dividir a 1, luego $\text{m.c.d}\,(n_2, m) = 1$. Recíprocamente, si $\text{m.c.d}\,(n_2, m) = 1$, entonces n_2 divide a cualquier congruencia. Estos elementos se llaman las *unidades* de $\mathbb{Z}/\mathbb{Z}\,m$. Por ejemplo, en $\mathbb{Z}/\mathbb{Z}\,16$ las unidades son

$$1\,,3\,,5\,,7\,,9\,,11\,,13\,,15\,,23\,,$$

es decir, todos los números impares entre 1 y 12.

4.4.4.2. Si n_2 es una unidad, para toda congruencia n_1, el cociente n_1/n_2 es único. En efecto, como $1 = \text{m.c.d}\,(n_2, m)$, por 4.4.3.5, el número de cocientes n_1/n_2 es 1. Nótese que, por 4.4.3.4, para que exista también el cociente n_2/n_1, debe ser n_1 una unidad. Si lo es, siempre $(n_1/n_2)(n_2/n_1) = 1$, expresiónn que tiene sentido porque los cocientes son únicos. En efecto, si $q = n_1/n_2$ y $q' = n_2/n_1$, podemos escribir en $\mathbb{Z}$ que $n_1 = qn_2 + km$ y $n_2 = q'n_1 + k'm$, luego

$$n_1 = q(q'n_1 + k'm) = (qq')n_1 + qk'm\,.$$

Como n_1 es una unidad, el cociente n_1/n_1 es único y, como $n_1 = 1 \cdot n_1 + 0 \cdot m$, es $n_1/n_1 = 1$ luego, de lo anterior, se deduce que $qq' = 1$, o sea que $(n_1/n_2)(n_2/n_1) = 1$.

4.4.4.3. La última pregunta que surge de manera natural es si hay módulos m tales que todas las congruencias no nulas de $\mathbb{Z}/\mathbb{Z}\,m$ sean unidades. La respuesta es que sí, y en el caso afirmativo, se dice que $\mathbb{Z}/\mathbb{Z}\,m$ es un cuerpo. La dmostración está en el siguiente teorema 4.4.5.

Teorema 4.4.5.– *$\mathbb{Z}/\mathbb{Z}\,m$ es un cuerpo si y sólo si m es primo.*

Demostración: Si m es primo, todo $n \in \mathbb{Z}$ tal que $0 < n < m$ es primo con m, es decir, $\text{m.c.d}\,(n, m) = 1$, porque m sólo tiene a 1 y a m como divisores positivos. Esto significa que, si m es primo, entonces $\mathbb{Z}/\mathbb{Z}\,m$ es un cuerpo. Recíprocamente, supongamos que $\mathbb{Z}/\mathbb{Z}\,m$ es un cuerpo y que m no es primo. Esto significa que $m = m_1m_2$ con $0 < m_1, m_2 < m$. Así, las congruencias m_1, m_2 son distintas de cero y su producto es cero, luego no pueden ser unidades. Esto contradice el hecho de que $\mathbb{Z}/\mathbb{Z}\,m$ sea un cuerpo, luego m es primo. □

UNIVERSIDAD DE SEVILLA

Definición 4.4.6.– *Los cuerpos de la forma* $\mathbb{Z}/\mathbb{Z}\,m$ *con* $m \in \mathbb{Z}_+$ *primo, se llaman cuerpos primos.*

Terminamos esta sección con un teorema muy importante sobre las congruencias: *el teorema chino del resto.*

Teorema 4.4.7.– (Teorema chino del resto). *Sean* $m_1, m_2, \ldots, m_r$, $r \geq 2$, *enteros mayores que* 1 *dos a dos primos entre sí, es decir,* $\text{m.c.d}\,(m_i, m_j) = 1$ *sin* $i \neq j$, *y sea* $m = m_1 m_2 \cdots m_r$. *Se considera la función*

$$\begin{array}{rcl} \chi\colon \mathbb{Z}/\mathbb{Z}\,m & \longrightarrow & \mathbb{Z}/\mathbb{Z}\,m_1 \times \mathbb{Z}/\mathbb{Z}\,m_2 \times \cdots \times \mathbb{Z}/\mathbb{Z}\,m_r \\ x & \longrightarrow & (C_{m_1}(x), C_{m_2}(x), \ldots, C_{m_r}(x))\,. \end{array}$$

Entonces χ *es una biyección compatible con la suma y el producto componente a componente, es decir:*

$$\begin{array}{rcl} \chi(x+y) & = & \chi(x) + \chi(y) \\ \chi(xy) & = & \chi(x)\chi(y)\,. \end{array}$$

En otras palabras χ *es un isomorfismo de anillos.*

Demostración: La compatibilidad con la suma y el producto son evidentes, puesto que ambas se definen en

$$\mathbb{Z}/\mathbb{Z}\,m_1 \times \mathbb{Z}/\mathbb{Z}\,m_2 \times \cdots \times \mathbb{Z}/\mathbb{Z}\,m_r$$

componente a componente. Probemos que χ es inyectiva. Si $\chi(x) = \chi(y)$, entonces $\chi(x-y) = (0, 0, \ldots, 0)$, luego $x - y$ es divisible por $m_1, m_2, \ldots, m_r$. Como éstos son primos entre sí tomados de dos en dos, $x - y$ debe ser divisible por el producto m. Así, $x = y$ por ser ambas congruencias módulo m.

Finalmente probamos que χ es sobre. Por la hipótesis de ser primos dos a dos los m_i, cada m_i es primo con el producto de los restantes, luego existen unas identidades de Bézout

$$\begin{array}{rcl} 1 & = & \alpha_1 m_1 + \beta_1 m_2 \cdots m_r \\ 1 & = & \alpha_2 m_2 + \beta_2 m_1 m_3 \cdots m_r \\ \vdots & & \vdots \\ 1 & = & \alpha_r m_r + \beta_r m_1 \cdots m_{r-1}\,. \end{array}$$

Sea

$$(x_1, x_2, \ldots, x_r) \in \mathbb{Z}/\mathbb{Z}\,m_1 \times \mathbb{Z}/\mathbb{Z}\,m_2 \times \cdots \times \mathbb{Z}/\mathbb{Z}\,m_r$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

y sea

$$x = C_m(x_1\beta_1 m_2 \cdots m_r + x_2\beta_2 m_1 m_3 \cdots m_r + \cdots + x_r\beta_r m_1 \cdots m_{r-1})\,;$$

para cada $i = 1, 2, \ldots, r$ es

$$\begin{aligned} C_{m_i}(x) &= C_{m_i}(x_1\beta_1 m_2 \cdots m_r + x_2\beta_2 m_1 m_3 \cdots m_r + \cdots + x_r\beta_r m_1 \cdots m_{r-1}) \\ &= C_{m_i}(x_i\beta_i m_1 \cdots m_{i-1} m_{i+1} \cdots m_r) = C_{m_i}(x_i - x_i\alpha_i m_i) = C_m(x_i) \\ &= x_i\,, \end{aligned}$$

lo que prueba el teorema. □

Corolario 4.4.8.– *Si $0 \neq x \in \mathbb{Z}/\mathbb{Z}\,m$, entonces $x \in (\mathbb{Z}/\mathbb{Z}\,m)^*$ si y sólo si $C_{m_i}(x) \in (\mathbb{Z}/\mathbb{Z}\,m_i)^*$, para todo $i = 1, 2, \ldots, r$. En palabras, el isomorfismo de anillos χ transforma unidades en unidades.*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 5

Unidades en anillos de congruencias

5.1. Grupos de unidades

En esta sección estudiamos el grupo de las unidades de un anillo de congruencias de $\mathbb{Z}$, o sea un anillo $\mathbb{Z}/\mathbb{Z}\,m$, donde $m \in \mathbb{Z}$, $m > 1$. Para aligerar la notación vamos a hacer un convenio. Una vez fijado un anillo de congruencias $\mathbb{Z}/\mathbb{Z}\,m$, entenderemos que operamos en él y escribiremos $x = y$ en lugar de $C_m(x) = y$. Por ejemplo, operando en $\mathbb{Z}/\mathbb{Z}\,5$ escribiremos $7 = 2$. No olvidaremos tampoco la notación clásica que, para expresar que $C_m(x) = y$, escribe $x \equiv y \pmod{m}$

Las unidades de $\mathbb{Z}/\mathbb{Z}\,m$ forman un grupo multiplicativo, finito por tanto, que se llama el *grupo de las unidades* de $\mathbb{Z}/\mathbb{Z}\,m$. En efecto, si $u, v \in \mathbb{Z}/\mathbb{Z}\,m$ son unidades, existen $u', v' \in \mathbb{Z}/\mathbb{Z}\,m$ tales que $u\,u' = 1$, $v\,v' = 1$. Así $(uv)(u'v') = (uu')(vv') = (uv')(u'v) = 1$. Esto prueba que, tanto uv como uv' como $u'v$ son unidades. Como 1 es una unidad, las unidades de $\mathbb{Z}/\mathbb{Z}\,m$ forman grupo, que se designa por $(\mathbb{Z}/\mathbb{Z}\,m)^*$.

Notas 5.1.1.– Debemos ahora pasar a un plano abstracto: el de un grupo multiplicativo, conmutativo, finito G. En G designamos por 1 el elemento unidad, y si $a \in G$, designamos por a^{-1} a su inverso, es decir, al único elemento de G tal que $aa^{-1} = 1$.

5.1.1.1. Sea $a \in G$; definimos las potencias a^n, $n \in \mathbb{Z}$ de la forma siguiente:

$$\begin{cases} a^0 = 1 & \\ a^n = a^{n-1}a & \text{si } n > 0 \\ a^n = (a^{n+1})a^{-1} & \text{si } n < 0 \end{cases}$$

UNIVERSIDAD DE SEVILLA

Con estas reglas, se verifican las propiedades usuales de la potenciación, a saber

$$a^m a^n = a^{m+n}\,, \quad (ab)^n = a^n b^n\,.$$

5.1.1.2. Sea $a \in G$ y consideremos las sucesivas potencias $a^0 = 1, a^1 = a, a^2, \ldots$; es evidente que no puede haber infinitas potencias distintas en ese conjunto porque todas ellas están en G y éste es finito. Sean $0 \leq r < s$ dos enteros tales que $a^r = a^s$; entonces $a^{s-r} = 1$, luego existen potencias de a de exponentes positivos que son iguales a 1. Sea $s > 0$ el mínimo entero positivo tal que $a^s = 1$; a este entero s se le llama el *orden* de a en G. Si $t \in \mathbb{Z}$ es un entero cualquiera y $t = cs + r$ es la división euclídea, $0 \leq r < s$, es $a^t = a^{cs}a^r = (a^s)^c a^r = a^r$. Así pues, el conjunto de todas las potencias de a de exponente entero arbitrario se reduce a

$$\{a^n \mid n \in \mathbb{Z}\} = \{1 = a^0, a = a^1, a^2, \ldots, a^{s-1}\}\,.$$

5.1.1.3. Sea $a \in G$ de orden s y sea $A = \{a^0 = 1, a^1 = a, \ldots, a^{s-1}\}$ el conjunto de las potencias de a distintas; es evidente que A es un grupo, subgrupo de G. Se le llama *un grupo cíclico*, o un *subgrupo cíclico* G. Se le suele designar por la notación $A = \langle a \rangle$.

5.1.1.4. Sea $\{1\} \neq A' \subset A$ un subgrupo de A y sea d el menor entero $0 < d \leq s - 1$ tal que $a^d \in A'$. Vamos a ver que $d|s$. Si $s = cd + r$ es la división euclídea, con $r = 0$ ó $0 < r < d$, es $1 = a^s = (a^d)^c a^r$, de donde $a^r = (a^d)^{-c} \in A'$. La minimalidad de d obliga a que $r = 0$, o sea que $d|s$. Vamos a demostrar ahora que A' es el conjunto de las potencias de a^d. Por condición de subgrupo,

$$(a^d)^i = a^{di} \in A'\,, \quad \forall i \in \mathbb{Z}\,.$$

Vamos a ver que, recíprocamente, un elemento de A que pertenece a A' es una potencia de a^d. En efecto, sea $i \in \mathbb{Z}$ tal que $a^i \in A'$ y sea $i = cd + r$ la división euclídea, con $r = 0$ ó $0 < r < d$. Entonces $a^i = (a^d)^c a^r$, luego $a^r = a^i (a^d)^{-c} \in A'$. La minimalidad de d obliga entonces a que $r = 0$, luego a que $i = cd$ y así $a^i = (a^d)^c$. Esto prueba nuestro aserto.

5.1.1.5. Sea $\langle a \rangle = \{a^0 = 1, a^1 = a, \ldots, a^{s-1}\}$ el subgrupo cíclico de G engendrado por a. Sea $n \in \mathbb{Z} \setminus \{0\}$; entonces $\langle a^n \rangle = \langle a^d \rangle$, donde $d = \text{m.c.d}\,(n, s)$. En efecto, sean $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha n + \beta s = d$; entonces:

1. $a^d = a^{\alpha n + \beta s} = (a^n)^\alpha + (a^s)^\beta = (a^n)^\alpha \in \langle a^n \rangle$, luego $\langle a^d \rangle \subset \langle a^n \rangle$ y

2. $a^n = (a^d)^{n/d} \in \langle a^d \rangle$, luego $\langle a^n \rangle \subset \langle a^d \rangle$,

de donde la igualdad. Más aún, es evidente que el orden de a^n es igual al orden de a^d, igual a s/d.

Ejemplo 5.1.2.– Vamos a escribir el grupo de las unidades $(\mathbb{Z}/\mathbb{Z}\,36)^*$ de $\mathbb{Z}/\mathbb{Z}\,36$. Repasando los números desde 1 hasta 36, y descartando los que no son pares ni divisibles por 3 porque $36 = 2^2 \cdot 3^2$, encontramos que

$$(\mathbb{Z}/\mathbb{Z}\,36)^* = \{1\,,5\,,7\,,11\,,13\,,17\,,19\,,23\,,25\,,29\,,31\,,35\},,.$$

Para cada unidad buscamos su orden, por simple rastreo calculando sus potencias. Por ejemplo,

$$5^2 = 25\,, 5^3 = 17\,, 5^4 = 13\,, 5^5 = 29\,, 5^6 = 1\,,$$

luego el orden de 5 en $(\mathbb{Z}/\mathbb{Z}\,36)^*$ es 6 y

$$A = \langle 5 \rangle = \{5^0 = 1\,,\, 5^1 = 5\,,\, 5^2 = 25\,,\, 5^3 = 17\,,\, 5^4 = 13\,,\, 5^5 = 29\}\,.$$

Así construimos una tabla de órdenes:

Unidad	1	5	7	11	13	17	19	23	25	29	31	35
Orden	1	6	6	6	3	2	2	6	3	6	6	2

Tomamos ahora el subgrupo de A engendrado por la congruencia 5^{22}. Como m.c.d $(()22, 6) = 2$, es $\langle 5^{22} \rangle = \langle 5^2 \rangle$, que debe tener 3 elementos: $\langle 5^2 \rangle = \{(5^2)^0 = 1, (5^2)^1 = 25, (5^2)^2 = 13\}$.

Como observación final diremos que la tabla de órdenes nos suministra una información interesante. El orden de cada elemento de $(\mathbb{Z}/\mathbb{Z}\,36)^*$ es un divisor del número de elementos de $(\mathbb{Z}/\mathbb{Z}\,36)^*$, que es 12. Este hecho es general, como veremos en un momento.

Aplicando las notas 5.1.1 al caso de $(\mathbb{Z}/\mathbb{Z}\,m)^*$, tenemos el siguiente

Teorema 5.1.3.– *Sea el anillo de congruencias $\mathbb{Z}/\mathbb{Z}\,m$ y $(\mathbb{Z}/\mathbb{Z}\,m)^*$ el conjunto de sus unidades. Se verifica:*

1. *$(\mathbb{Z}/\mathbb{Z}\,m)^*$ es un grupo multiplicativo.*
2. *Para cada $a \in (\mathbb{Z}/\mathbb{Z}\,m)^*$, existe un entero positivo s' tal que $a^{s'} = 1$. Al mínimo s de todos ellos se le llama el orden de a en $(\mathbb{Z}/\mathbb{Z}\,m)^*$.*

UNIVERSIDAD DE SEVILLA

3. Se verifica que

$$\langle a\rangle = \{a^i \mid i \in \mathbb{Z}\} = \{1 = a^0, a = a^1, \ldots, a^{s-1}\}$$

es un subgrupo de $(\mathbb{Z}/\mathbb{Z}\,m)^*$*, que se llama el grupo cíclico engendrado por* a*.*

4. Todo subgrupo $A' \subset \langle a\rangle$ *es un grupo cíclico engendrado por una potencia de* a*. Más aún,* $\langle a^n\rangle = \langle a^d\rangle$*, donde* $d = \text{m.c.d}\,(n, s)$*.*

Notas 5.1.4.– Sea G un grupo multiplicativo, abeliano y $a \in G$ un elemento de orden s.

5.1.4.1. Sea $A = \langle a\rangle = \{a^0 = 1, a^1 = a, \ldots, a^{s-1}\}$ el conjunto de las potencias de a distintas; para cada $b \in G$ se pondrá

$$bA = \{b, ba, \ldots, ba^{s-1}\}\,.$$

Comprobemos que, si $b, c \in G$ y $bA \cap cA \neq \emptyset$ entonces $bA = cA$. Por simetría, basta ver que $bA \subset cA$. Sean i, j tales que $0 \leq i, j < s$ y $ba^i = ca^j$; entonces, para todo $n \in \mathbb{Z}$ es $ba^n = (ba^i)a^{n-i} = ca^{n-i+j} \in cA$, luego $bA \subset cA$. A todos los paquetes bA de s elementos, $b \in (\mathbb{Z}/\mathbb{Z}\,m)^*$, se les llama *clases*.

5.1.4.2. Es evidente que los elementos de G quedan clasificados en clases disjuntas. Como cada una de ellas tiene s elementos, el número total de elementos de G es un múltiplo de s. O sea, el orden de un elemento de G divide al número de elementos de G.

5.1.4.3. Lo dicho en 5.1.4.1 para $A = \langle a\rangle$ se puede decir para cualquier subgrupo A de G, resultando que el número de elementos de un subgrupo de G divide siempre al número de elementos de G.

Los resultados obtenidos en las notas 5.1.4 se resumen en el siguiente enunciado preciso:

Teorema 5.1.5.– *Para todo* $a \in (\mathbb{Z}/\mathbb{Z}\,m)^*$*, el orden de* a *divide al número de elementos de* $(\mathbb{Z}/\mathbb{Z}\,m)^*$*.*

Ejemplo 5.1.6.– En un cuerpo $\mathbb{Z}/\mathbb{Z}\,p$, $p \in \mathbb{Z}_+$ primo, todas las congruencias distintas de cero son unidades. Al grupo de unidades $(\mathbb{Z}/\mathbb{Z}\,p)^*$ se le llama el *grupo multiplicativo del cuerpo.* $\mathbb{Z}/\mathbb{Z}\,p$. Consideremos el cuerpo $k = \mathbb{Z}/\mathbb{Z}\,19$ y la congruencia $4 \in (\mathbb{Z}/\mathbb{Z}\,19)^*$. Como los divisores de 18, que el número de elementos de

UNIVERSIDAD DE SEVILLA

$(\mathbb{Z}/\mathbb{Z}\,19)^* = \mathbb{Z}/\mathbb{Z}\,19 \setminus \{0\}$, son

$$\{1\,,2\,,3\,,6\,,9\,,18\,,\}\,,$$

para calcular el orden de 4 no hace falta calcular todas sus potencias, sino solamente aquéllas de exponente uno de esos divisores. Así

$$4^{16} = 8\,, 4^3 = 7\,, 4^6 = 11\,, 4^2 = 1\,,$$

luego el orden de 4 es 9. Haciendo esto con cada elmento de $(\mathbb{Z}/\mathbb{Z}\,19)^*$ tenemos la tabla

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2

donde arriba están las unidades y abajo los órdenes. En ella vemos que, al haber elementos de orden 18 (por ejemplo, el 10), el propio $(\mathbb{Z}/\mathbb{Z}\,19)^*$ es el grupo cíclico engendrado por cada uno de ellos; por ejemplo, $(\mathbb{Z}/\mathbb{Z}\,19)^* = \langle 10 \rangle$.

5.2. Grupos de unidades de un cuerpo finito

Recordemos que un grupo multiplicativo G se llama *cíclico* si existe un elemento $a \in G$ tal que

$$G = \{a^i \mid i \in \mathbb{Z}\}\,.$$

Si G es finito y tiene n elementos, entonces el orden de cualquier generador $a \in G$ debe ser n. Nuestro objetivo en esta sección va a ser el demostrar que el grupo multiplicativo de cualquier cuerpo finito es cíclico. Para ello necesitamos un lema previo, que damos a continuación.

Lema 5.2.1.– *Sea G un grupo finito, multiplicativo y abeliano. Sean $a, b \in G$ de órdenes respectivos r, s primos entre sí. Entonces el orden de ab es rs*

Demostración: Desde luego, $(ab)^{rs} = (a^r)^s(b^s)^r = 1$. Sea t el orden de ab; lo anterior indica que $t|rs$. Por otra parte, $a^t b^t = 1$, luego $a^t = b^{-t}$, de donde $a^{st} = 1$. Así, $r|st$, luego $r|t$. De la misma manera se demuestra que $s|t$, luego $rs|t$ y así $t = rs$.

□

UNIVERSIDAD DE SEVILLA

Corolario 5.2.2.– *Sean G, H grupos cíclicos multiplicativos con m y n elementos respectivamente. Considerando la estructura de grupo sobre $G \times H$ que opera elemento a elemento, se verifica que $G \times H$ es cíclico si y sólo si* $\text{m.c.d}\,(m,n) = 1$.

Demostración: Supongamos que $\text{m.c.d}\,(m,n) = 1$ y sean $a \in G$, $b \in H$ generadores, es decir, elementos de órdenes respectivos m y n. Entonces $(a,1) \in G \times H$ es un elemento de orden m y $(1,b) \in G \times H$ es un elemento de orden n. Por el lema 5.2.1, $(a,b) = (a,1)\cdot(1,b)$ tiene orden mn, que es el número de elementos de $G \times H$, luego éste es cíclico.

Supongamos que $\text{m.c.d}\,(m,n) = d > 1$, $m = m'd$, $n = n'd$, $\text{m.c.d}\,(m',n') = 1$; entonces $u = m'n'd < mn$. Si $(a_1,b_1) \in G \times H$, entonces

$$(a_1,b_1)^{m'n'd} = (a_1^{m'n'd}, b_1^{m'n'd}) = [(a_1^m)^{b'}, (b_1^n)^{a'}] = (1,1)\,,$$

luego ningún elemento de $G \times H$ tiene orden mn, luego $G \times H$ no es cíclico. □

Teorema 5.2.3.– *El grupo multiplicativo K^* de un cuerpo finito K es cíclico, es decir, existe $a \in K^*$ tal que $K^* = \langle a \rangle$, el conjunto de las potencias de a.*

Demostración: Sea $a \in K^*$ un elemento de orden máximo u en K^*. Supongamos que el orden de cualquier elemento $b \in K^*$ es un divisor de u. Sea $b \in K^*$ un elemento de orden $v|u$ y sea $u = v'v$. Entonces la ecuación $X^u - 1 = 0$ tiene, a lo más, u raíces en K^*. Como, las potencias a^i, $0 \le i \le u-1$ son distintas y todas ellas verifican que $(a^i)^u = 1$, esas potencias son todas las raíces de $X^u - 1 = 0$ y pertenecen a K^*. Como $b^v = 1$, es $(b^v)^{v'} = b^u = 1$, luego b debe ser una potencia de a. Así $b \in \langle a \rangle$ y $K^* = \langle a \rangle$.

Supongamos que existe un elemento $b \in K^*$ cuyo orden v no es divisor de u. Sea $d = \text{m.c.d}\,(u,v)$, $u = u'd$, $v = v'd$, con $\text{m.c.d}\,(u',v') = 1$. Como v no divide a u es $v' > 1$. Como a^d tiene orden u' y b^d tiene orden v', por el lema 5.2.1, el elemento $a^d b^d = (ab)^d$ tiene orden $u'v'$. Así, ab tiene orden $du'v' = uv' > u$, lo que no es posible por hipótesis. Esto prueba el teorema. □

Definición 5.2.4.– *Sea K un cuerpo finito con n elementos, K^* su grupo multiplicativo. Cada generador de K^* se llama una raíz primitiva de 1 en K. Si $a \in K^*$ es una raíz primitiva, entonces el conjunto de las raíces primitivas es*

$$\{a^i \mid 1 \le i \le n-1 \ \text{m.c.d}\,(i,n-1) = 1\}\,.$$

por 5.1.1.5.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Nota 5.2.5.– No es fácil dar un procedimiento para encontrar una raíz primitiva de $(\mathbb{Z}/\mathbb{Z}\,p)^*$, $p \in \mathbb{Z}_+$, primo, salvo el rastreo. Por ejemplo, tomando $p = 17$, tenemos que los divisores de 16 son $1, 2, 4, 8, 16$. Si comenzamos por 2 tenemos:

$$2^2 = 4\,,\, 2^4 = 16\,,\, 2^8 = 16^2 = 256 = 15 \cdot 17 + 1 = 1\,,$$

luego el orden de 2 en $\mathbb{Z}/\mathbb{Z}\,17$ es 8 y así 2 no es una raíz primitiva. Si tomamos 3 tenemos

$$3^2 = 9\,,\, 3^4 = 13\,,\, 3^8 = 16\,,$$

luego debe ser $3^{16} = 1$ y así 3 es una raíz primitiva de $(\mathbb{Z}/\mathbb{Z}\,17)^*$. El conjunto de todas las raíces primitivas es el de las potencias 3^i, donde $1 \leq i \leq 16$ es primo con 16, es decir que i es impar. Así, el conjunto de las raíces primitivas de $(\mathbb{Z}/\mathbb{Z}\,17)^*$ es

$$3^1 = 3\,,\, 3^3 = 10\,,\, 3^5 = 5\,,\, 3^7 = 11\,,\, 3^9 = 14\,,\, 3^{11} = 7\,,\, 3^{13} = 12\,,\, 3^{15} = 6\,.$$

Queda pendiente una cuestión importante: si $m > 1$ es un entero, ¿cuántas unidades hay en $(\mathbb{Z}/\mathbb{Z}\,m)^*$?. Es decir, ¿cuántos elementos tiene $(\mathbb{Z}/\mathbb{Z}\,m)^*$? La respuesta viene dada por el cálculo explícito de la función de Euler, que se se basa en el teorema chino del resto, más concretamente, en su corolario 4.4.8.

5.3. La función de Euler

Sabemos que las unidades de $\mathbb{Z}/\mathbb{Z}\,m$ son las congruencias de aquéllos números menores que m y primos con m.

Definición 5.3.1.– *La función φ de Euler es la función $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$ definida por $\varphi(1) = 1$ y, si $m > 1$, entonces $\varphi(m)$ es el número de elementos de en $(\mathbb{Z}/\mathbb{Z}\,m)^*$, o sea, el número de números positivos menores que m y primos con m.*

Notas 5.3.2.– Es relativamente sencillo calcular $\varphi(m)$ para cualquier entero $m > 1$.

5.3.2.1. Sea $m = p_1^{u_1} \cdots p_t^{u_t}$ la descomposición factorial de m; como los números $p_i^{u_i}$ son primos entre sí tomados dos a dos, el corolario 4.4.8 nos dice que

$$\varphi(m) = \varphi(p_1^{u_1}) \cdots p_t^{u_t}\,,$$

con lo que el cálculo de $\varphi(m)$ se reduce al caso de calcular φ sobre los números que sean potencias de primos.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

5.3.2.2. Sea $p \in \mathbb{Z}_+$ un número primo, $u \in \mathbb{Z}_+$; entonces

$$\varphi(p^u) = p^u - p^{u-1} = p^u \left(1 - \frac{1}{p}\right) .$$

En efecto, hay $p^u - 1$ números positivos menores que p^u, de los cuales los no primos con p^u son los divisibles por p, o sea

$$\{1, p, 2p, \ldots, (p^{u-1} - 1)p\} ,$$

que son en total $p^{u-1} - 1$. Así, los primos con p^u totalizan

$$\varphi(p^u) = (p^u - 1) - (p^{u-1} - 1) = p^u - p^{u-1} = p^{u-1}(p - 1) .$$

5.3.2.3. De 5.3.2.1 y 5.3.2.2 se deduce que, si $m = p_1^{u_1} \cdots p_t^{u_t}$ es la descomposición factorial, entonces

$$\varphi(m) = p_1^{u_1} \left(1 - \frac{1}{p_1}\right) \cdots p_t^{u_t} \left(1 - \frac{1}{p_t}\right) = m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right) .$$

Ésta no es una buena fórmula, porque hace depender el cálculo de $\varphi(m)$ de la descomposición factorial de m. Sin embargo, muy posteriormente a Euler se logró demostrar que la complejidad algorítmica de calcular $\varphi(m)$ es equivalente a la de la descomposición factorial. Ésta es la base del algoritmo de codificación de clave pública que describiremos más adelante.

5.3.2.4. Por ejemplo, si $m = 36 = 2^2 3^2$, el número de elementos de $(\mathbb{Z}/\mathbb{Z}\,36)^*$ es

$$\varphi(m) = 36 \left(1 - \frac{1}{2}\right) (1 - \frac{1}{3}) = 12 ,$$

como ya vimos en el ejemplo 5.1.2.

Una propiedad esencial de la función φ de Euler viene recogida en el siguiente

Teorema 5.3.3.– *Sea $m \in \mathbb{Z}_+$ y sean d_i, $i = 1, \ldots, r$ los divisores de m. Entonces*

$$\varphi(m) = \sum_{i=1}^{r} \varphi(d_i) .$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Demostración: Comencemos suponiendo que $m = p^n$ es una potencia de primo; los divisores de m son $\{1, p, \ldots, p^{n-1}, p^n\}$ luego, por **??.??** tenemos que

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(p) &= p-1 \\ \varphi(p^2) &= p(p-1) \\ \vdots &\quad \vdots \\ \varphi(p^n) &= p^{n-1}(p-1)\,. \end{aligned}$$

Sumando miembro a miembro estas igualdades tenemos que

$$\sum_{i=0}^{n} \varphi(p^i) = 1 + (p-1)(1 + p + \cdots + p^{n-1})\,.$$

Ahora bien, el paréntesis de la derecha en esta expresión es la suma de los términos de una progresión geométrica de razón p, luego

$$\sum_{i=0}^{n} \varphi(p^i) = 1 + (p-1)\frac{p^n - 1}{p-1} = 1 + p^n - 1 = p^n = m\,,$$

lo que demuestra el teorema en este caso.

En general, sea $m = p_1^{n_1} \cdots p_t^{n_t}$, $t > 1$, la descomposición factorial de m. Por el caso anterior tenemos

$$\begin{aligned} \varphi(p_1^{n_1}) &= \varphi(1) + \varphi(p_1) + \cdots + \varphi(p_1^{n_1}) \\ \vdots &\quad \vdots \\ \varphi(p_t^{n_t}) &= \varphi(1) + \varphi(p_t) + \cdots + \varphi(p_t^{n_t}) \end{aligned}$$

Multiplicando miembro a miembro estas igualdades, y teniendo en cuenta el corolario 4.4.8, vemos que

1. $$\varphi(p_1^{n_1}) \cdots \varphi(p_t^{n_t}) = \varphi(p_1^{n_1} \cdots p_t^{n_t}) = \varphi(m)$$

2. En el miembro de la derecha tenemos todas las sumas posibles de términos de la forma $\varphi(p_1^{i_1}) \cdots \varphi(p_t^{i_t})$ con $0 \leq i_j \leq n_j$, $j = 1, \ldots, t$. Por la misma razón que antes
$$\varphi(p_1^{i_1}) \cdots \varphi(p_t^{i_t}) = \varphi(p_1^{i_1} \cdots p_t^{i_t})\,.$$
Además, es evidente que todos los productos $p_1^{i_1} \cdots p_t^{i_t}$ son distintos por la factorización única, son divisores de m y son todos los divisores de m, porque cualquier divisor de m es de esa forma. Esto prueba el teorema.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

□

5.4. Criptografía de clave pública

Hay una aplicación estelar de la función φ de Euler, que es el método de criptografía de clave pública llamado RSA, por las iniciales de sus autores Rivest, Shamir y Adleman, que explicamos brevemente.

Notas 5.4.1.–

5.4.1.1. Uno de los grandes problemas de la criptografía es el intercambio de claves entre dos personas que van a enviarse correspondencia cifrada. Este problema se resuelve con la criptografía de clave pública, de la que RSA es el ejemplo más interesante. En ella, cada individuo del grupo que va a corresponder crea dos claves: una privada que mantiene en secreto, y una pública que divulga a través de una guía. Veremos en unos momentos cómo con esto se puede montar un esquema de codificación y decodificación que no necesita del intercambio de claves. Además, se trata de producir un sistema que sea casi imposible de romper, basado en la dificultad de factorizar números muy grandes.

La clave de todo está en el grupo multiplicativo de las congruencias de enteros. Fijemos un entero positivo n, y consideremos el grupo multiplicativo $U_n = (\mathbb{Z}/\mathbb{Z}n)^*$ de las unidades en $\mathbb{Z}/\mathbb{Z}n$; el número de elementos de U_n es $\varphi(n)$. Recordemos que, si $a \in U_n$, su orden es el menor exponente positivo r tal que $a^r = 1$ y $r|\varphi(n)$.

5.4.1.2. Supongamos un individuo que quiere hacerse usuario del sistema RSA. Para ello, debe elegir dos primos muy grandes p_1, p_2, de una cierta manera que vamos a explicar, y calcular $n = p_1 p_2$. El número n es uno de los datos que se van a hacer públicos, aunque los números p_1, p_2 van a permanecer secretos. La seguridad del sistema depende de la dificultad en descomponer n en producto de sus dos factores primos. Si para hacerlo se requieren varios siglos de computador, el sistema puede considerarse seguro, aunque en teoría se sepa cómo romperlo. No vale, para estos fines, cualquier par de primos, porque hay sistemas abreviados de factorización de un número. Se trata de producir primos que obliguen a que el único sistema aplicable de factorización sea el genérico. Para ello basta con elegir primos p tales que $(p-1)/2$ sea también primo. A éstos se les va a llamar *primos seguros*. Por ejemplo, $p = 10007$ es primo y $q = (p-1)/2 = 5003$ también, luego p es un primo seguro.

Construído n, el usuario calcula $\varphi(n) = (p_1 - 1)(p_2 - 1)$. Se elige ahora un entero c entre 0 y $\varphi(n)$ que sea primo con $\varphi(n)$. Esto se puede hacer al azar porque la

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

probabilidad de que no lo sea es ínfima, si los números son grandes. Este número c se hace público, junto con n, y sirve para codificar mensajes, como ahora vamos a ver. Después, el usuario construye la congruencia inversa de c módulo $\varphi(n)$, es decir un número d, usado para decodificar, comprendido entre 0 y $\varphi(n)$ tal que $cd = 1$ como congruencias módulo $\varphi(n)$. En resumen, lo que el usuario hace público es n, c y guarda para sí el resto de los datos.

5.4.1.3. Ahora viene una parte del sistema que nada tiene que ver con las Matemáticas. Se trata de convertir un mensaje de texto en un número, y recíprocamente, porque el cifrado de mensajes opera sobre números, no sobre textos. Convertir un texto en un número es fácil. Para ello se pueden usar, por ejemplo, los códigos ASCII de los caracteres. Para un operador que codifica, es absolutamente necesario que el número así obtenido sea primo con n, es decir represente una congruencia de U_n. Para ello basta con que este número sea más pequeño que p_1 y p_2, lo que se puede lograr descomponiendo el texto en trozos, si preciso fuera, y operando con una lista de los trozos. Por simplicidad, supondremos que el mensaje consta de un solo número m, comprendido entre 0 y el más pequeño de p_1, p_2. Así $m \in U_n$. Este es el sistema con el que operamos en el programa con que ilustraremos esta técnica.

5.4.1.4. Vamos a explicar cómo funciona la codificación y decodificación de mensajes, usando un poco de Matemáticas. Si un operador determinado tiene un mensaje m (numérico), el mensaje codificado es el entero $u = m^c (\mathrm{mod}\ n)$. Si ahora se calcula la congruencia $u^d (\mathrm{mod}\ n)$ se observa lo siguiente. Como $cd = 1$ como congruencias módulo $\varphi(n)$ es $cd = k\varphi(n) + 1$, luego $u^d = m^{cd} = m \cdot m^{k\varphi(n)}$. Como $m \in U_n$ y el orden de m en U_n es un divisor del número de elementos de U, que es $\varphi(n)$, como congruencias,

$$u^d = m^{cd} = m^{k\varphi(n)+1} = m^{k\varphi(n)} m = (m^{\varphi(n)+1})^k m = m\,.$$

Así pues, el mensaje decodificado es $u^d (\mathrm{mod}\ n)$. Si alguien extraño quiere averiguar qué dice el mensaje codificado u tiene que calcular d a partir de c y n. Esto es inmediato en teoría: se calcula la descomposición factorial $n = p_1 p_2$, con ella el entero $\varphi(n) = (p_1 - 1)(p_2 - 1)$, y luego el inverso multiplicativo d de c en U_n. En la práctica, esto puede ser imposible para p_1, p_2 muy grandes, del orden de 200 cifras cada uno. ¿No se puede calcular $\varphi(n)$ sin la factorización? Según y como, pues hay un teorema que afirma que *la dificultad de calcular $\varphi(n)$ es equivalente a la de calcular la factorización de n.*

5.4.1.5. Vamos a ver el esquema de utilización. Supongamos que hay dos usuarios, que se llaman Juan y Pedro. Cada uno por su cuenta, en secreto, produce sus núme-

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

ros $p_1, p_2, n, \varphi(n), c, d$. Entre ambos construyen un archivo público, que contiene el n y el c de Juan, y el n y el c de Pedro. Designémoslos, respectivamente, con las letras n_j, c_j, n_p, c_p. Supongamos que Juan quiere enviar un mensaje (numérico) m a Pedro, sin que nadie se entere de su contenido. Juan codifica m con la clave pública de Pedro, i.e. construye $m^{c_p} (\text{mod } n_p)$. Es evidente que este mensaje sólo puede ser descodificado con la clave privada de Pedro, que sólo él posee.

5.4.1.6. Hay otro aspecto igualmente interesante del sistema RSA, que es la firma electrónica. Supongamos que Pedro es banquero y Juan es su cliente. Juan envía a Pedro un mensaje por correo electrónico, en lenguaje ordinario, diciéndole que transfiera, con cargo a su cuenta corriente, un millón de euros al comité ecológico local. ¿Cómo sabe Pedro que el mensaje viene de Juan? Para ello Juan usa la firma electrónica. Esta es una pequeña frase, añadida al mensaje ordinario, convenida de antemano (por ejemplo el nombre completo de Juan), *y codificada con la clave privada de Juan*, es decir con n_j y d_j. Como este mensaje sólo puede ser descodificado con la clave pública de Juan, Pedro sabe que viene de él.

Ejemplo 5.4.2.– Vamos a dar un ejemplo con dos primos muy pequeños; por tanto, el sistema será fácilmente descifrable. Los usuarios son Juan y Pedro y las elecciones y cálculos secretos son:

1. Para Juan:

$$\begin{aligned} p_1 &= 113117105106111120527 \\ p_2 &= 11311710510611218039 \\ n_J &= 12795479467587001566175351676603105586553 \\ \varphi(n) &= 12795479467587001565949117466390883247988 \\ c_J &= 1001 \\ d_J &= 86155376235301089465032019703770782309 13 \end{aligned}$$

2. Para Pedro:

$$\begin{aligned} p_1 &= 113117105106211118819 \\ p_2 &= 113117105116111117019 \\ n_P &= 12795479468729472707454100635911822080561 \\ \varphi(n) &= 12795479468729472707227866425689499844724 \\ c_P &= 10001 \\ d_P &= 77481675495076179097062252848690741985 45 \end{aligned}$$

UNIVERSIDAD DE SEVILLA

La lista pública es

1. Para Juan:

$$\begin{aligned} n_J &= 127954794675870015661753516766031055865 53 \\ c_J &= 1001 \end{aligned}$$

2. Para Pedro

$$\begin{aligned} n_P &= 127954794687294727074541006359118220805 61 \\ c_P &= 10001 \end{aligned}$$

Vamos ahora a enviar mensajes sencillos. Empleamos un alfabeto de letras minúsculas sin acentos. Supongamos que Juan quiere enviar a Pedro el mensaje "quijote" sin que nadie se entere. La tabla de códigos ASCII de los caracteres es

Carácter	q	u	i	j	o	t	e
Código ASCII	113	117	105	106	111	116	101

y formamos el mensaje simplemente uniendo los códigos ASCII en su orden, luego es

$$m = 113117105106111116101\,.$$

Éste es el mensaje que Juan quiere enviar a Pedro sin que se entere nadie. Entonces Juan lo codifica con la clave pública de Pedro, es decir, calcula

$$m_r = m^{c_P} \bmod n_P = 119975014670414436890698891505684878927 39$$

y se lo envía a Pedro. Al recibirlo Pedro, lo descodifica con su clave privada, es decir, calcula

$$m_r^{d_P} \bmod n_P = 113117105106111116101\,,$$

que es igual a m. Ahora Pedro descompone el número en grupos de tres cifras y reconstruye los caracteres con la tabla anterior.

Veamos un ejemplo de firma electrónica. Juan envía a Pedro en claro la orden de trasnferencia que dijimos. Para firmarla convierte, por ejemplo, su nombre en un número mediante la tabla ASCII:

Carácter	j	u	a	n
Código ASCII	106	117	097	110

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

y construye el mensaje $m = 106117097110$. Entonces Juan codifica m con su clave privada, es decir, calcula

$$m_r = m^{d_J} \bmod n_J = 11785065971032435339728605950510167499482$$

y lo envía a Pedro. Éste lo decodifica con la clave pública de Juan, es decir, calcula

$$m' = m_r^{c_J} \bmod n_J = 106117097110\,.$$

Este número lo descompone en grupos de tres cifras y, con la tabla de códigos ASCII lee en claro el nombre de Juan, luego sólo ha podido ser él quien envió la orden de transferencia.

5.5. Grupos cíclicos de unidades

Esta sección tiene un fuerte contenido teórico. En ella se responde a la pregunta siguiente: dado un entero $m > 1$, ¿cuándo el grupo $U_m = (\mathbb{Z}/\mathbb{Z}\,m)^*$ de las unidades de $\mathbb{Z}/\mathbb{Z}\,m$ es cíclico?

Notas 5.5.1.– Comenzamos estudiando cuándo los grupos U_{2^n}, $n \geq 1$, son cíclicos.

5.5.1.1. Desde luego

$$(\mathbb{Z}/\mathbb{Z}\,2)^* = \{1\} \quad \text{y} \quad (\mathbb{Z}/\mathbb{Z}\,4)^* = \{1, 3\}$$

son cíclicos engendrados, respectivamente, por 1 y 3. Vamos a ver que son los dos únicos grupos cíclicos que hay entre los U_{2^n}, $n \geq 1$. Nótese que U_{2^n} está contituido por todas las congruencias de todos los números impares entre 1 y $2^n - 1$.

5.5.1.2. Todo número impar q se puede escribir en la forma $q = 2h + 1$, $h \in \mathbb{Z}_0$. Si $h = 2k$ es par, entonces $q = 4k + 1$. Si $h = 2k' + 1$ es impar, entonces

$$q = 2h + 1 = 2(2k' + 1) + 1 = 4k' + 3 = 4(k' + 1) - 1 = 4k - 1\,, k = k' + 1\,.$$

Concluimos de aquí que todo número impar q se puede escribir en la forma $q = 4k \pm 1$.

5.5.1.3. Sea $q = 4k \pm 1$ un número impar; vamos a probar que, para todo $u \in \mathbb{Z}_+$, existe $k_u \in \mathbb{Z}_+$ tal que $q^{2^u} = 2^{u+2}k_u + 1$. Esto lo hacemos por recurrencia sobre u. Si $u = 1$ tenemos que

$$q^2 = (4k \pm 1)^2 = 16k^2 \pm 8k + 1 = 2^3(2k^2 + k) + 1$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

con lo que se verifica el aserto poniendo $k_1 = 2k^2 + k$. Supongamos el aserto válido para u y probémoslo para $u+1$. Tenemos que

$$\begin{aligned} q^{2^{u+1}} &= (q^{2^u})^2 = (2^{u+2}k_u + 1)^2 \\ &= 2^{2u+4}k_u^2 + 2^{u+3}k_u + 1 = 2^{u+3}(2^{u+1}k_u^2 + k_u) + 1 \\ &= 2^{u+3}k_{u+1} + 1\,, \end{aligned}$$

donde hemos puesto $k_{u+1} = 2^{u+1}k_u^2 + k_u$.

5.5.1.4. Sea, pues $m > 2$ un entero y consideremos el grupo U_{2^m}, que tiene $\varphi(2^m) = 2^m(1-1/2) = 2^{m-1}$ elementos. Como todos los elementos de U_m son congruencias impares q, el apartado 5.5.1.3 nos dice que

$$q^{2^{m-2}} = 2^m k + 1\,,$$

o sea que, como congruencia, $q^{2^{m-2}} = 1$, lo que significa que el orden de q es, a lo más 2^{m-2}, luego nunca 2^{m-1}, que es lo que debería ser para que U_{2^m} fuese cíclico.

5.5.1.5. Por ejemplo, en $(\mathbb{Z}/\mathbb{Z}\,2^4)^* = (\mathbb{Z}/\mathbb{Z}\,16)^*$, una tabla con la primera fila los elementos de $(\mathbb{Z}/\mathbb{Z}\,16)^*$ y la segunda sus órdenes:

Elemento	1	3	5	7	9	11	13	15
Orden	1	4	4	2	2	4	4	2

Resumiendo las notas 5.5.1 tenemos la

Proposición 5.5.2.– *Sea $n \in \mathbb{Z}_+$; el grupo $(\mathbb{Z}/\mathbb{Z}\,2^n)^*$ es cíclico si y sólo si $n = 1, 2$.*

Se trata ahora de demostrar que, dado un primo impar $p > 0$, para todo $n \in \mathbb{Z}_+$, $U_{p^n} = (\mathbb{Z}/\mathbb{Z}\,p^n)^*$ es cíclico. Si $n = 1$ el resultado ya está probado en el teorema 5.2.3. Así es que, sin más, supondremos $n > 1$.

Proposición 5.5.3.– *Para todo entero $e \geq 1$ se verifica que*

$$(1+p)^{p^e} \equiv 1 + p^{e+1} \pmod{p^{e+2}}\,.$$

Demostración: En efecto, demostrémoslo por recurrencia sobre e. Si $e = 1$ tenemos

$$\begin{aligned} (1+p)^p &= 1 + \binom{p}{1}p + \binom{p}{2}p^2 + p^3T = 1 + p\cdot p + \frac{p-1}{2}\cdot p\cdot p^2 + p^3T \\ &= 1 + p^2 + \frac{p-1}{2}p^3 + p^3T \end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

y así

$$(1+p)^p \equiv 1+p^2 \pmod{p^3},$$

que prueba la fórmula para $e=1$. Supongamos, pues, $e \geq 1$ y la fórmula cierta para e; vamos a demostrarla para $e+1$. Tenemos que existe $k \in \mathbb{Z}_+$ tal que

$$(1+p)^{p^e} = 1+p^{e+1}+kp^{e+2},$$

luego existe un entero T tal que

$$\begin{aligned}(1+p)^{p^{e+1}} &= [(1+p)^{p^e}]^p = [1+p^{e+1}(1+kp)]^p \\ &= 1+p\cdot p^{e+1}(1+kp)+\frac{p-1}{2}p\cdot p^{2(e+1)}(1+kp)^2+p^{3e+3}\cdot T \\ &= 1+p^{e+2}+p^{2e+3}T'\end{aligned}$$

y, como $2e+3 > e+3$ queda claro que

$$(1+p)^{p^{e+1}} \equiv 1+p^{e+2} \pmod{p^{e+3}}.$$

Esto prueba la proposición. □

Corolario 5.5.4.– *Si p es un primo impar y $n>1$ un entero, $1+p \in (\mathbb{Z}/\mathbb{Z}\,p^n)^*$ y su orden es p^{n-1}.*

Demostración: En efecto, haciendo $e+2=n$, o sea $e=n-2$, en el enunciado de la proposición 5.5.3 tenemos que $(1+p)^{p^{n-2}} \equiv 1+p^{n-1} \pmod{p^n}$ luego $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Además $(1+p)^{p^{n-1}} \equiv 1+p^n \pmod{p^{n+1}}$ luego $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$, lo que prueba el corolario. □

Corolario 5.5.5.– *Si p es un primo impar y $n>1$ un entero, $U_{p^n} = (\mathbb{Z}/\mathbb{Z}\,p^n)^*$ es cíclico.*

Demostración: Sabemos que el número de elementos de $(\mathbb{Z}/\mathbb{Z}\,p^n)^*$ es $\varphi p^n = p^{n-1}(p-1)$. Si $a \in (\mathbb{Z}/\mathbb{Z}\,p)^*$ es una raíz primitiva, vamos a demostrar que $b = C_{p^n}(a^p(1+p))$ tiene orden $p^{n-1}(p-1)$. Sea s el orden de b en $(\mathbb{Z}/\mathbb{Z}\,p^n)^*$; como $b^s \equiv 1 \pmod{p^n}$ y $a^p(1+p) \equiv a^p \pmod{p}$ (luego $a^p(1+p) \equiv a \pmod{p}$) y a tiene orden $p-1$, vemos que $(p-1)|s$. Así, $s = p^e(p-1)$ con $e \leq n-1$ porque $s|p^{n-1}(p-1)$. Por otra parte,

$$[a^p(1+p)]^{p^{n-2}(p-1)} \equiv (1+p)^{p^{n-2}(p-1)} \pmod{p^n}$$

luego

$$[a^p(1+p)]^{p^{n-2}(p-1)} \not\equiv (1+p)^{p^{n-2}(p-1)} \pmod{p^n}$$

porque $(1+p)$ tiene orden p^{n-1} en $(\mathbb{Z}/\mathbb{Z}\,p^n)^*$ por el corolario 5.5.4. Esto implica que $s = p^{n-1}(p-1)$, y nuestra demostración. □

Corolario 5.5.6.– *Si p es un primo impar y $n \in \mathbb{Z}_+$, entonces los grupos U_{2p^n} son todos cíclicos. Si $m \in \mathbb{Z}_+$, $m > 1$ ningún grupo $U_{2^m p^n}$ es cíclico.*

Demostración: Por el corolario 4.4.8 al teorema chino del resto, siempre es $U_{2^m p^n}$ isomorfo a $U_{2^m} \times U_{p^n}$. El número de elementos de U_{2^m} es 2^{m-1} y el de $U_{p^n} esp^{n-1}(p-1)$. Como $p-1$ es par, la condición necesaria y suficiente para que $\text{m.c.d}\,(2^{m-1}, p^{n-1}(p-1)) = 1$ es que $m = 1$. Así, por el corolario 5.2.2, $U_{2^m p^n}$ es cíclico si y sólo si $m = 1$. Nótese que, si $m = 1$, entonces $U_2 = \{1\}$ y podemos escribir, por abuso de lenguaje

$$U_2 \times U_{2^n} = \{(1, a) \mid a \in U_{2^n}\} = U_{2^n}\,.$$

□

Corolario 5.5.7.– *Salvo los grupos U_2, U_4, U_{p^n}, U_{2p^n}, ninguno de los $U_m = (\mathbb{Z}/\mathbb{Z}\,m)^*$ son cíclicos.*

Demostración: Supongamos que en la descomposición factorial de m intervienen dos primos impares. Entonces se podrá escribir $m = p_1^{m_1} p_2^{m_2} q$, donde p_1 y p_2 son primos impares y q no es divisible por ninguno de ellos. Por el corolario 4.4.8 al teorema chino del resto, U_m es isomorfo a $U_{p_1^{m_1}} \times U_{p_2^{m_2} q}$. Por otra parte,

$$\begin{aligned} \varphi(p_1^{m_1}) &= p_1^{m_1-1}(p_1-1) \\ \varphi(p_2^{m_2} q) &= p_2^{m_2-1}(p_2-1)\varphi(q) \end{aligned}$$

y ambos son números pares. Por tanto, U_m no es cíclico por el corolario 5.2.2. Si en la descomposición factorial de m intervienen 2 y un primo impar, el resultado está tratado en el corolario 5.5.6. Si en la descompsición factorial de m sólo interviene un primo impar, el resultado está tratado en el corolario 5.5.5. Si $m = 2^n$, el resultado estñá tratado en la proposición 5.5.2. □

Terminamos esta sección dando un resultado que puede ser enormemente útil para buscar raíces primitivas de U_{2^n} que sean sencillas.

Teorema 5.5.8.– *Sea $p \in \mathbb{Z}_+$ un primo impar y $a \in \mathbb{Z}_+$, $1 < a < p$, una raíz primitiva de U_p. Entonces a es raíz primitiva de U_{p^n} para todo $n \in \mathbb{Z}_+$ si y sólo si $(a^{p-1} - 1)$ no es divisible por p^2.*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Demostración: Sea r el menor entero positivo tal que p^r divide a $a^{p-1}-1$, o sea, tal que $a^{p-1} = 1 + kp^r$, $k \in \mathbb{Z}_+$ no divisible por p. Desarrollando por el binomio de Newton $(1+p^r)^{p^{n-1}}$ para cualquier entero positivo n tenemos que

$$\begin{aligned} a^{p^{n-1}(p-1)} &= (1+kp^r)^{p^{n-1}} \\ &= 1 + \binom{p^{n-1}}{1} kp^r + \frac{p^{n-1}-1}{2} p^{n-1} k^2 p^{2r} + \cdots \\ &= 1 + (p^{r+n-1}) \left(k + \frac{p^{n-1}-1}{2} k^2 p^r + \cdots \right) \\ &= 1 + k_{n-1} p^{r+n-1} \end{aligned}$$

donde $k_{n-1} \in \mathbb{Z}_+$ no es divisible por p. Si $r = 1$, entonces a es raíz primitiva de U_{p^n} porque ninguna potencia $a^{p^s(p-1)}$ puede ser igual a 1 módulo p^n. Si $r > 1$, entonces $a^{p^{n-r}(p-1)} = 1 + k_{n-r}p^n$, luego a no puede ser raíz primitiva de U_{p^n}. □

Ejemplo 5.5.9.– Veamos un ejemplo relativo al teorema 5.5.8. Si $p = 29$, las raíces primitivas de U_{29} son

$$2\,,3\,,8\,,10\,,11\,,14\,,15\,,18\,,19\,,21\,,26\,,27$$

Los restos de dividir la potencia 28-ésima de cada raíz primitiva por 29^2 son, respectivamente,

$$29\,,435\,,87\,,377\,,667\,,0\,,783\,,58\,,464\,,406\,,725\,,464$$

luego todas las raíces primitivas, excepto 14, son raíces primtivas de 29^n para cualquier $n \in \mathbb{Z}_+$

Terminamos este capítulo de aritmética con un apéndice sobre otra función importante: la de Möbius.

5.6. La función de Möbius

Terminamos este capítulo dando otra función importantísima: la función μ de Möbius. Para definirla recordemos que un entero positivo n se llama *libre de cuadrados* si no es divisible por el cuadrado de ningún entero mayor que 1 o, equivalentemente, si en la descomposición factorial de n los exponentes de todos los primos que aparecen son 1. Por ejemplo, $15 = 3 \cdot 5$ es libre de cuadrados y $12 = 2^2 \cdot 3$ no lo es.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Definición 5.6.1.– *La función de Möbius es la función* $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ *definida así:*

1. $\mu(1) = 1$,
2. *Si* n *es libre de cuadrados,* $n = p_1 \cdots p_t$ *con los* p_i *distintos dos a dos, entonces* $\mu(n) = (-1)^t$,
3. $\mu(n) = 0$ *si* n *no es libre de cuadrados.*

Lo importante de la función de Möbius es calcular su suma cuando los argumentos recorren los divisores positivos de un número dado.

Proposición 5.6.2.– *Sea* $n > 0$ *un entero; entonces*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n > 1 \end{cases}$$

Demostración: Sea $n = p_1^{r_1} \cdots p_m^{r_m}$ la descomposición factorial. Sea

$$P(X_1, \ldots, X_m) = \prod_{i=1}^{m} (1 - X_i)\,;$$

si se sustituyen todas las X_i por 1 el polinomio se hace cero, pero los términos del desarrollo que son de la forma $(-1)^r X_{i_1} \cdots X_{i_r}$ se corresponden con los divisores de n que son libres de cuadrados. De ahí el resultado es ya trivial. □

La siguiente es también una fórmula clave en los cálculos con la función μ.

Proposición 5.6.3.– *(*Fórmula de inversión de Möbius*) Sea* $f : \mathbb{Z}_+ \to G$, *donde* G *es un grupo abeliano y sea* $g : \mathbb{Z}_+ \to G$ *definida por*

$$g(n) = \sum_{d|n} f(d)\,;$$

entonces

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \mu\left(\frac{n}{d}\right) g(d)\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Demostración:

$$\begin{aligned}\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right) &= \sum_{d|n}\mu(d)\sum_{e|(n/d)}f(e)\\ &= \sum_{e|n}\sum_{d|(n/e)}\mu(d)f(e)\\ &= \sum_{e|n}f(e)\sum_{d|(n/e)}\mu(d)\\ &= f(n)\end{aligned}$$

□

Más adelante tendremos ocasión de dar una aplicación importantísima de esta fórmula de inversión de Möbius.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 6

Polinomios

6.1. Álgebra polinómica

En esta sección consideraremos un cuerpo k cualquiera, el cuerpo de constantes, y el anillo $R = k[X]$ de los polinomios en la indeterminada X con coeficientes en k. Normalmente se escribirá un polinomio comenzando por su término de mayor grado (aquél que tiene máximo exponente de X) con coeficiente distinto de cero. A éste se le llamará el *término líder* y a su coeficiente, el *coeficiente líder*. Aparte del término de mayor grado se escribirán los de grado menor que él. Dicho en otras palabras, no se escribirá, en general, un polinomio con términos de grado mayor que el líder y coeficiente cero. Sin embargo, se hará algunas veces, por conveniencia, sobre todo en la suma de polinomios. Tampoco se escribirán, en general, los términos con coeficiente cero de un polinomio, salvo cuando se quieran tratar expresiones generales. Si $0 \neq f(X) \in k[X]$, la notación inglesa (muy extendida) `lcoeff` $(f(X))$ designará al coeficiente líder de $f(X)$. Se supondrá que el polinomio cero tiene grado -1 y no tiene coeficiente líder.

Se recuerda que las operaciones de adición y multiplicación en este anillo son las siguientes:

$$\begin{aligned} \sum_{i=0}^{r} a_i X^i + \sum_{i=0}^{r} b_i X^i &= \sum_{i=0}^{r} (a_i + b_i) X^i \\ \left(\sum_{i=0}^{r} a_i X^i\right) \cdot \left(\sum_{j=0}^{s} b_j X^j\right) &= \sum_{l=0}^{r+s} \sum_{i+j=l} (a_i b_j) X^l \end{aligned}$$

Notas 6.1.1.–

UNIVERSIDAD DE SEVILLA

6.1.1.1. Nótese que, si

$$f(X) = \sum_{i=0}^{r} a_i X^i\,, \quad g(X) = \sum_{j=0}^{s} b_j X^j\,,$$

donde $a_r \neq 0 \neq b_s$ son sus coeficientes líderes, entonces, $\operatorname{gr}(fg) = \operatorname{gr}(f) + \operatorname{gr}(g)$ y el coeficiente líder de fg es $a_r b_s$, el producto de los coeficientes líderes de $f(X)$ y de $g(X)$.

6.1.1.2. El hecho sencillo apuntado en 6.1.1.1 se traduce en varias consecuencias inmediatas:

1. Si $f(X) \neq 0 \neq g(X)$, entonces $f(X)g(X) \neq 0$.
2. Las unidades de un anillo son los elementos con inverso multiplicativo. Entonces las unidades de R son justamente las constantes distintas de cero porque un producto, en el que uno de los polinomios factores tenga grado positivo, tiene necesariamente grado positivo.

6.1.1.3. En cualquier caso, se tiene

$$\operatorname{gr}(f+g) \leq \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}\,.$$

Teorema 6.1.2.– División de polinomios. *Dados dos polinomios $f(X)$ y $g(X)$ en $k[X]$ con $g(X) \neq 0$, existen dos polinomios $q(X), r(X)$ unívocamente determinados por $f(X), g(X)$ tales que $f(X) = q(X)g(X) + r(X)$ y, o bien $r(X) = 0$, o bien $\operatorname{gr}(r(X)) < \operatorname{gr}(g(X))$. A $q(X)$ se le llama el cociente de la división y a $r(X)$ su resto.*

Demostración: Escribimos la demostración de la existencia en notación algorítmica:

Variables: F, G, Q :
Inicio: $F := f(X) : G := g(X) : Q := 0$:
`while` $\operatorname{gr}(G) \leq \operatorname{gr}(F)$ `do`
$F := F - (\texttt{lcoeff}\,(F)/\texttt{lcoeff}\,(G))*X^{\operatorname{gr}(F)-\operatorname{gr}(G)}G$:
$Q := Q + (\texttt{lcoeff}\,(F)/\texttt{lcoeff}\,(G))*X^{\operatorname{gr}(F)-\operatorname{gr}(G)}$:
`end do:`
Output: $q(X) = Q$, $r(X) = F$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Obsérvese que este algoritmo es finito porque el grado de F decrece en cada paso, eventualmente pudiéndose convertir en -1 al hacerse F cero.

En cuanto a la unicidad, pongamos

$$f(X) = q(X)g(X) + r(X) = q'(X)g(X) + r'(X)$$

con las condiciones anteriores. Entonces $(q(X) - q'(X))g(X) = r'(X) - r(X)$, de donde $r'(X) - r(X) = 0$ por cuestión de grado, luego $q(X) - q'(X) = 0$. □

Ejemplo 6.1.3.– Sea $k = \mathbb{Z}/\mathbb{Z}\,19$ y sean

$$\begin{aligned} f &= 7\,X^5 + 15\,X^4 + 4\,X^3 + 14\,X^2 + 4\,X + 2 \\ g &= 13\,X^3 + 4\,X^2 + 13\,X + 3\,. \end{aligned}$$

Como $7/13 = 2$ en $\mathbb{Z}/\mathbb{Z}\,19$, tenemos que

$$f - 2X^2 g = 7\,X^4 + 16\,X^3 + 8\,X^2 + 4\,X + 2\,.$$

Como $7/13 = 2$ en $\mathbb{Z}/\mathbb{Z}\,19$, tenemos que

$$f - 2X^2 g - 2Xg = 8\,X^3 + X^2 + 17\,X + 2\,.$$

Como $8/13 = 5$ en $\mathbb{Z}/\mathbb{Z}\,19$, tenemos que

$$f - 2X^2 g - 2Xg - 5g = 9\,X + 6\,.$$

Así pues,

$$f = (2\,X^2 + 2\,X + 5)g + (9\,X + 16)\,,$$

luego el cociente es $2\,X^2 + 2\,X + 5$ y el resto $9\,X + 16$.

Definición 6.1.4.– *Dados dos polinomios $f(X), g(X) \in k[X]$ con $g(X) \neq 0$, se dirá que $g(X)$ divide a $f(X)$ si existe $h(X) \in k[X]$ tal que $f(X) = h(X)g(X)$; en este caso se usará la notación $g(X)|f(X)$. A $g(X)$ se le llamará un divisor de $f(X)$ y a éste un múltiplo de $g(X)$. Dos elementos se llaman asociados si cada uno es divisor del otro. Las unidades son los divisores de 1. Si $f(X) \neq 0 \neq g(X)$, un máximo común divisor de $f(X)$ y $g(X)$ es un polinomio $g(X)$ que verifica:*

1. *$d(X)|f(X)$ y $d(X)|g(X)$,*
2. *si $d'(X) \in k[X]$ es tal que $d'(X)|f(X)$ y $d'(X)|g(X)$, entonces $d'(X)|d(X)$.*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Notas 6.1.5.– En estas notas vamos a ver algunas propiedades sencillas de la divisibilidad.

6.1.5.1. Dos polinomios $f(X) \neq 0 \neq g(X)$ son asociados si y sólo si uno de ellos es igual a una unidad por el otro. Como las unidades son las constantes distintas de cero (véase 6.1.1.2), los asociados de un polinomio son justamente sus múltiplos constantes distintos de cero.

6.1.5.2. Fijados $f(X) \neq 0 \neq g(X)$, si $d(X)$ es un máximo común divisor de ambos y $d'(X)$ es otro, entonces son asociados por definición. Esto quiere decir que el máximo común divisor de dos polinomios está unívocamente determinado salvo productos por constantes distintas de cero. Así se escribirá $\mathrm{m.c.d}\,(()f(X), g(X))$ para designar cualquier máximo común divisor de $f(X)$ y $g(X)$. Dos polinomios se llaman *primos entre sí* si sus únicos divisores comunes son las constantes distintas de cero. Así se puede decir que dos polinomios son primos entre sí si y sólo si su máximo común divisor es 1.

Nota 6.1.6.– La demostración de la existencia del máximo común divisor de dos polinomios se hace como en los enteros, mediante el algoritmo de Euclides. Naturalmente, el algoritmo de Euclides para polinomios es una copia exacta del algoritmo de Euclides para enteros, reemplazando la división de enteros por la polinómica. También se construye el algoritmo de Euclides extendido como en los enteros, sustituyendo la división entera por la polinómica.

Ejemplo 6.1.7.– Si $k = \mathbb{Z}/\mathbb{Z}\,7$ y

$$f(X) = 3\,X^5 + 4\,X^4 + 3\,X^3 + 3\,, \quad g(X) = 5\,X^4 + 3\,X^3 + 5\,X^2 + 3\,X$$

entonces el algorimo de Euclides para calcular el máximo común divisor es (en forma matricial)

$$\begin{bmatrix} \text{“}Dividendo\text{”} & \text{“}Cociente\text{”} & \text{“}Divisor\text{”} & \text{“}Resto\text{”} \\ 3\,X^5 + 4\,X^4 + 3\,X^3 + 3 & 2\,X + 1 & 5\,X^4 + 3\,X^3 + 5\,X^2 + 3\,X & 3 + 3\,X^2 + 4\,X^3 + 4\,X \\ 5\,X^4 + 3\,X^3 + 5\,X^2 + 3\,X & 3\,X + 2 & 3 + 3\,X^2 + 4\,X^3 + 4\,X & X^2 + 1 \\ 3 + 3\,X^2 + 4\,X^3 + 4\,X & 4\,X + 3 & X^2 + 1 & 0 \end{bmatrix}$$

con lo que $\mathrm{m.c.d}\,(f(X), g(X)) = X^2 + 1$. Por otra parte, y por analogía al caso de los números enteros, la fracción ordinaria $f(X)/g(X)$ se puede desarrollar como fracción continua, dando

$$\frac{f(X)}{g(X)} = (2\,X + 1) + \cfrac{1}{3\,X + 2 + \cfrac{1}{4\,X + 3}}\,.$$

Volviendo a reducir ésta a fracción ordinaria, se obtiene

$$\frac{3\,X^3+4\,X^2+3}{5\,X^2+3\,X}$$

que es igual a f/g habiendo dividido f y g por su máximo común divisor. Se puede hallar una identidad de Bézout construyendo el cuadro completo como en la nota 4.2.5, sustituyendo los números enteros por polinomios y la división euclídea por la polinómica. En nuestro caso

$$(4\,X+5)f(X)+(6\,X^2+3)g(X)=X^2+1\,,$$

que es el máximo común divisor de $f(X)$ y $g(X)$.

Definición 6.1.8.– *Un polinomio $0\neq f(X)\in k[X]$ de grado positivo (es decir, no constante) se llama irreducible si sólo es divisible por las unidades y por sus asociados.*

Teorema 6.1.9.– Teorema de Euclides: *Si $f(X)|(g(X)h(X))$ y $f(X)$, $g(X)$ son primos entres sí, es decir,* m.c.d $(()f(X),g(X))=1$*, entonces $f(X)|h(X)$. En particular, si $f(X)$ es irreducible, $f(X)|(g(X)h(X))$ y $f(X)$ no divide a $g(X)$, entonces $f(X)|h(X)$.*

Demostración: La segunda afirmación es consecuencia evidente de la primera; demostremos ésta. Existen $\alpha(X),\beta(X)\in k[X]$ que verifican $\alpha(X)f(X)+\beta(X)g(X)=1$. Así

$$h(X)=\alpha(X)f(X)h(X)+\beta(X)g(X)h(X)\,,$$

de donde resulta evidente que $f(X)|h(X)$. □

Teorema 6.1.10.– Factorialidad de $k[X]$*: Todo polinomio $f(X)$ de grado positivo se puede descomponer en producto de irreducibles. Dicha descomposición es única, salvo orden y producto por unidades.*

Demostración: La existencia de la descomposición se prueba por recurrencia sobre $n=\mathrm{gr}\,(f(X))$. Si $n=1$ entonces $f(X)$ es necesariamente irreducible, lo que implica ya la existencia de la descomposición. Supongamos, pues, que $n>1$ y la existencia demostrada para polinomios de grado menor que n. Si $f(X)$ es irreducible, ya hemos terminado porque está ya descompuesto. Si no lo es, se descompone en producto de dos factores $f(X)=g(X)h(X)$ de grados estrictamente menores que n. Para $g(X)$ y $h(X)$ existen sendas descomposiciones en producto de irreducibles, por hipótesis de recurrencia, luego existe la descomposición para $f(X)$.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

En cuanto a la unicidad, procedemos así: Sean

$$f(X) = f_1(X) \cdots f_r(X) = g_1(X) \cdots g_s(X)$$

dos descomposiciones en producto de irreducibles. De aquí se deduce que $f_1(X)|g_1(X) \cdots g_s(X)$ luego, por el teorema de Euclides 6.1.9, debe dividir a alguno de los $g_i(X)$. Supongamos que $f_1(X)|g_1(X)$; entonces $f_1(X)$ y $g_1(X)$ son asociados, luego existe una constante $0 \neq a \in k$ tal que $g_1(X) = af_1(X)$, de donde

$$f_2(X) \cdots f_r(X) = ag_2(X) \cdots g_s(X)\,.$$

Así tenemos dos descomposiciones factoriales iguales con un elemento menos. Procediendo así sucesivamente se ve la unicidad. □

6.2. Congruencias polinómicas

La división polinómica nos conduce inmediatamente a la noción de congruencia de módulo dado. Fijemos el cuerpo base k.

Sea $m(X) > 0$ un polinomio fijo, designemos por $k[X]/k[X]\,m(X)$ al conjunto de los restos de dividir todos los polinomios de $k[X]$ por $m(X)$ (es decir, al conjunto de todos los polinomios de $k[X]$ de grado estrictamente menor que el de $m(X)$) y sea $C_m : k[X] \to k[X]/k[X]\,m(X)$ la función que, a cada polinomio $f(X)$, hace corresponder el resto de su división por $m(X)$. Al polinomio $C_m(f)$ se le llama la *congruencia* de f módulo m. Por ejemplo, si $k = \mathbb{Z}/\mathbb{Z}\,2 = \{0, 1\}$, $m = X^2 + X + 1$ entonces

$$(\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2 + X + 1) = \{0, 1, X, X + 1\}$$

y, si $f(X) = X^7$, es $X^7 = (X^5 + X^4 + X^2 + X)(X^2 + X + 1) + X$, luego $C_m(X^7) = X$ y X es la congruencia de X^7 módulo $X^2 + X + 1$. Por tanto, al conjunto $k[X]/k[X]\,m(X)$ lo llamamos el conjunto de las congruencias módulo $m(X)$.

Nota 6.2.1.– Para cada $r(X) \in k[X]/k[X]\,m(X)$, el conjunto $C_m^{-1}(r)$ es el de todos los polinomios que, divididos por m, dan de resto r. Entonces

$$C_m^{-1}(r) = \{q(X)m(X) + r(X) \mid q \in k[X]\}\,,$$

luego, para todo $f_1\,, f_2 \in k[X]$ tenemos

$$C_m(f_1) = C_m(f_2) \Longleftrightarrow m|(f_1 - f_2)\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

En palabras: dos polinomios dan el mismo resto al dividirlos por m si y sólo si m divide a la diferencia de ambos. En notación clásica, el hecho de que $C_m(f_1) = C_m(f_2)$ se expresa diciendo que f_1 y f_2 son *congruentes módulo* m y escribiendo $f_1(X) \equiv f_2(X) \pmod{m(X)}$.

Notas 6.2.2.– Vamos a dotar al conjunto $k[X]/k[X]\,m(X)$ de una estructura de anillo, utilizando la función C_m.

6.2.2.1. Se define la suma de dos elementos $r_1, r_2 \in k[X]/k[X]\,m(X)$ como la suma ordinaria de polinomios. Nótese que, al tener r_1 y r_2 grado menor que el de $m(X)$, su suma también. Por ejemplo, en $(\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2+X+1)$, es $(X+1)+X=1$. Esta suma de congruencias verifica una propiedad esencial: si $f_1 \in C_m^{-1}(r_1)$ y $f_2 \in C_m^{-1}(r_2)$ son cualesquiera, entonces $C_m(f_1+f_2) = r_1+r_2$. En efecto, si $f_1(X) = q_1(X)m(X)+r_1(X)$ y $f_2(X) = q_2(X)m(X)+r_2(X)$ es

$$f_1(X)+f_2(X) = (q_1(X)+q_2(X))m + (r_1(X)+r_2(X))$$

y $r_1(X)+r_2(X)$ es el resto de esa división por ser de grado menor que el de $m(X)$. Esto se escribe poniendo que $C_m(f_1(X)+f_2(X)) = C_m(f_1(X)) + C_m(f_2(X))$.

6.2.2.2. Es inmediato ver que, con la suma de congruencias, $k[X]/k[X]\,m(X)$ es un grupo abeliano, porque la suma de congruencias es la misma que la polinómica.

6.2.2.3. Se define el producto de dos elementos $r_1, r_2 \in k[X]/k[X]\,m(X)$ como el resto de la división euclídea de $r_1(X)r_2(X)$ por $m(X)$. Es decir, si $r_1(X)r_2(X) = q(X)m(X)+r(X)$, el producto de $r_1(X)$ y $r_2(X)$ como congruencias es $r_1(X)r_2(X) = r(X)$. Por ejemplo, en $(\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2+X+1)$ el producto de las congruencias $(X+1)X = 1$. Este producto de congruencias verifica una propiedad esencial: si $f_1 \in C_m^{-1}(r_1)$ y $f_2 \in C_m^{-1}(r_2)$ son cualesquiera, entonces $C_m(f_1f_2) = r$. En efecto, si $f_1(X) = q_1(X)m(X)+r_1(X)$ y $f_2(X) = q_2(X)m(X)+r_2(X)$ es

$$\begin{aligned} f_1(X)f_2(X) &= (q_1(X)q_2(X)+q_1(X)r_2(X)+q_2(X)r_1(X))m(X) \\ &\quad +(r_1(X)r_2(X)) \\ &= (q_1(X)q_2(X)+q_1(X)r_2(x)+q_2(X)r_1(X)+q(X))m(X) \\ &\quad +r(X)\,, \end{aligned}$$

luego $C_m(f_1f_2) = r$. Esto se escribe poniendo que $C_m(f_1f_2) = C_m(f_1)C_m(f_2)$, donde el producto en el primer miembro es de polinomios y en el segundo, de congruencias.

6.2.2.4. Con estas dos operaciones, $k[X]/k[X]\,m(X)$ es un anillo, en el que 1 es el elemento unidad si $m(X)$ no es una constante distinta de cero (nótese que, si $\alpha \in k \setminus \{0\}$, entonces $k[X]/k[X]\,\alpha = \{0\}$).

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

6.2.2.5. Como ejemplos creamos una tabla de sumar y otra de multiplicar de los anillos de congruencias

$$(\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2+1) \quad \text{y} (\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2+X+1)\,.$$

La tabla de sumar es la misma en ambos casos:

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

En cambio, las de multiplicar son distintas. En el caso de $m(X) = X^2+1$ tenemos

$\times$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	1	$X+1$
$X+1$	0	$X+1$	$X+1$	0

y en el caso de $m(X) = X^2+X+1$

$\times$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

6.2.2.6. Entre estos dos anillos de congruencias hay una diferencia esencial. Fijémonos en las tablas de multiplicar. En el caso de $m(X) = X^2+X+1$, para todo par de elementos $a\,, b \in (\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2+X+1)$, $b \neq 0$, existe $c \in \mathbb{Z}/\mathbb{Z}\,5$ tal que $a = bc$. Esto lo expresaremos diciendo que todo $0 \neq b \in (\mathbb{Z}/\mathbb{Z}\,2)[X]/(\mathbb{Z}/\mathbb{Z}\,2)[X]\,(X^2+X+1)$ es tal que se puede dividir por él todo otro elemento, y escribiremos que $a/b = c$. Para demostrar esto nos fijamos en la tercera, cuarta y quinta filas de la tabla de multiplicar. Tenemos:

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

1. La tercera fila nos dice que

$$1 = \frac{1}{1} = \frac{X}{X} = \frac{X+1}{X+1}\,.$$

2. La cuarta fila nos dice que

$$X = \frac{X}{1} = \frac{X+1}{X} = \frac{1}{X+1}\,.$$

3. La quinta fila nos dice que

$$X+1 = \frac{X+1}{1} = \frac{1}{X} = \frac{X}{X+1}\,.$$

En cambio, la tabla de multiplicar para $m(X) = X^2+1$ nos dice que se puede dividir todo elemento por 1 y por X, pero no por $X+1$. Por $X+1$ sólo se puede dividir $X+1$, dando como cocientes 1 y X.

Ahora no vamos a hacer un estudio tan detallado de los cocientes como en el caso de las congruencias de enteros, por la simple razón de que se puede copiar éste con ligeras adaptaciones de lenguaje. Sólo nos van a interesar aquellos casos en que toda congruencia distinta de cero posea una inversa, o sea el caso en que $k[X]/k[X]\,m(X)$ sea un cuerpo.

Teorema 6.2.3.– *$k[X]/k[X]\,m(X)$ es un cuerpo si y sólo si $m(X)$ es un polinomio irreducible.*

Demostración: Si $m(X)$ es irreducible, todo $0 \neq r(X) \in k[X]/k[X]\,m(X)$ es de grado menor que el de $m(X)$, luego debe ser primo con $m(X)$, es decir, $\text{m.c.d}\,(f(X), m(X)) = 1$, porque $m(X)$ sólo tiene a las unidades y a sus asociados como divisores. Por la identidad de Bézout, existen $\alpha(X)\,, \beta(X) \in k[X]$ tales que $\alpha(X)r(X)+\beta(X)m(X) = 1$, luego $1 = C_m(\alpha)r(X)$, de donde $1/r(X) = \alpha(X)$. Esto significa que, si $m(X)$ es irreducible, entonces $k[X]/k[X]\,m(X)$ es un cuerpo. Recíprocamente, supongamos que $k[X]/k[X]\,m(X)$ es un cuerpo y que $m(X)$ es reducible. Esto significa que $m(X) = m_1(X)m_2(X)$ con $m_1(X), m_2(X)$ de grados estrictamente menores que el de $m(X)$. Así, las congruencias $m_1(X), m_2(X)$ son distintas de cero y su producto es cero, luego no pueden ser unidades. Esto contradice el hecho de que $k[X]/k[X]\,m(X)$ sea un cuerpo, luego $m(X)$ es irreducible. □

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Nota 6.2.4.– Es evidente que, si k es un cuerpo finito, entonces $k[X]/k[X]\,m(X)$ es un anillo finito porque el número de polinomios de un grado dado es finito, luego lo es el número de polinomios de grado menor que uno dado. Como se puede sustituir, evidentemente, $m(X)$ por un asociado (producto por constante no nula), supondremos siempre que el coeficiente de la máxima potencia de $m(X)$ es 1, es decir, que $m(X)$ será de la forma

$$m(X) = X^e + a_1X^{e-1} + \cdots + a_{e-1}X + a_e\,.$$

En el caso de las congruencias de polinomios, damos una notación especial: a la congruencia del polinomio X la llamaremos x (en lugar de X como hemos venido haciendo hasta ahora). Haciendo esto,

$$m(x) = x^e + a_1x^{e-1} + \cdots + a_{e-1}x + a_e = 0$$

en el sentido de operaciones con congruencias. Esto prueba que $k[X]/k[X]\,m(X) = k[x]$, donde x verifica la relación $m(x) = 0$.

Más aún, cualquier polinomio en la congruencia x (siempre dentro de $k[X]/k[X]\,m(X)$) se puede reducir a un polinomio en x de grado menor que e. En efecto, con el polinomio $f(x) \in k[x]$ podemos construir $f(X)$ cambiando la variable, dividir por $m(X)$ y tomar el resto $r(X)$. Así, como congruencias, $f(x) = r(x)$. Como caso particular de este hecho vemos que $k[x]$ es un k-espacio vectorial de dimensión n, en el que una base es $\mathcal{B} = \{1, x, x^2, \ldots, x^{e-1}\}$. En efecto, lo que acabamos de decir significa que todo elemento de $k[x]$ es combinación lineal de $\mathcal{B}$, con coeficientes en k. Como cualquier polinomio $f(X)$ que dé resto cero al dividirlo por $m(X)$ debe ser múltiplo de $m(X)$ (luego tener grado mayor o igual que e), está claro que $\mathcal{B}$ está formada por vectores linealmente independientes.

Lo anterior significa que, si el cuerpo k tiene q elementos, el anillo $k[x]$ tiene q^e elementos.

Teorema 6.2.5.– *Para todo cuerpo finito K, existe un primo $p \in \mathbb{Z}_+$, un polinomio irreducible $m(X) \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$ (con coeficiente de la máxima potencia igual a 1) y un elemento $x \in K$ tales que:*

1. *$m(x) = 0$ y, si $f(X) \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$ es tal que $f(x) = 0$, entonces $m(X)|f(X)$.*
2. *$K = (\mathbb{Z}/\mathbb{Z}\,p)[x]$.*
3. *El número de elementos de K es una potencia de p*

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Demostración: Designemos por $\epsilon \in K$ al elemento unidad y pongamos, para todo $n \in \mathbb{Z}$,

$$\begin{cases} n \cdot \epsilon = 0 & \text{si} \quad n = 0 \\ n \cdot \epsilon = (n-1) \cdot \epsilon + \epsilon & \text{si} \quad n > 0 \\ n \cdot \epsilon = (n+1) \cdot \epsilon - \epsilon & \text{si} \quad n < 0 \end{cases} ;$$

esto define el conjunto de los múltiplos enteros de ϵ. Se verifican las propiedades clásicas de los múltiplos enteros, como fácilmente se puede comprobar; en particular

$$(n_1 + n_2)\epsilon = n_1 \cdot \epsilon + n_2 \cdot \epsilon \,, \quad (n_1)(n_2 \cdot \epsilon) = (n_1 n_2)\epsilon \,.$$

Como K tiene un número finito de elementos, es obvio que no todos los múltiplos enteros de ϵ pueden ser distintos. Sean $n_1 > n_2$ enteros tales que $n_1 \cdot \epsilon = n_2 \cdot \epsilon$, luego $(n_1 - n_2)\epsilon$. Esto prueba que hay múltiplos positivos de ϵ que son cero. Sea p el menor entero positivo tal que $p \cdot \epsilon = 0$ y veamos que p es primo. Si no lo fuera, se descompondría en producto de dos números menores que él, $p = p_1 p_2$. Entonces sería $p_1\epsilon \neq 0$ $p_2\epsilon \neq 0$ por minimalidad de p y $(p_1\epsilon)(p_2\epsilon) = (p_1 p_2)(\epsilon\epsilon) = p\epsilon = 0$, lo que no es posible. Así p es primo y el conjunto de los mútiplos enteros de ϵ es

$$\mathbb{Z}\epsilon = \{0, \epsilon, 2\epsilon, \ldots, (p-1)\epsilon\}$$

por un uso evidente de la división euclídea. Las operaciones en $\mathbb{Z}\epsilon$ son, evidentemente, las de las congruencias módulo p, luego, como anillo $\mathbb{Z}\epsilon = (\mathbb{Z}/\mathbb{Z}\,p)\epsilon$, que es un cuerpo, subcuerpo de K. Podemos identificar $(\mathbb{Z}/\mathbb{Z}\,p)\epsilon$ con $\mathbb{Z}/\mathbb{Z}\,p$ y suponer que $\mathbb{Z}/\mathbb{Z}\,p \subset K$. Si hacemos esto, volvemos a llamar 1 al elemento unidad ϵ porque coincide con la congruencia 1. Al subcuerpo $\mathbb{Z}/\mathbb{Z}\,p$ de K se le llama *el cuerpo primo de* K porque es el más pequeño posible: todo otro subcuerpo de K lo contiene.

Por el teorema 5.2.3, K^* es cíclico; sea $x \in K^*$ una raíz primitiva, es decir, tal que $K^* = \langle x \rangle$. Como K es finito, es un $\mathbb{Z}/\mathbb{Z}\,p$-espacio vectorial de dimensión finita (con la adición en K y la multiplicación de un elemento de $\mathbb{Z}/\mathbb{Z}\,p$ por uno de K), luego las potencias $\{1 = x^0, x, x^2, \ldots\}$ no pueden ser todas linealmente independientes sobre $\mathbb{Z}/\mathbb{Z}\,p$. Sea e el entero mínimo tal que $\{1, x, \ldots, x^{e-1}\}$ sean linealmente independientes sobre $\mathbb{Z}/\mathbb{Z}\,p$ y $\{1, x, \ldots, x^{e-1}, x^e\}$ sean linealmente dependientes sobre $\mathbb{Z}/\mathbb{Z}\,p$. Entonces x^e es combinación lineal de las anteriores potencias, con coeficientes en $\mathbb{Z}/\mathbb{Z}\,p$, luego tenemos una relación

$$x^e + a_1 x^{e-1} + \cdots + a_{e-1}x + a_e = 0 \,, \quad a_i \in \mathbb{Z}/\mathbb{Z}\,p \,.$$

Sea $m(X) = X^e + a_1 X^{e-1} + \cdots + a_{e-1}X + a_e \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$ y veamos que $m(X)$ es irreducible. En efecto, si no lo fuese, sería producto de dos polinomios de grado inferior

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

a él, $m(X) = m_1(X)m_2(X)$, luego $0 = m(x) = m_1(x)m_2(x)$, de donde $m_1(x) = 0$ ó $m_2(x) = 0$. Esto no puede ser porque tanto m_1 como m_2 tienen grado menor que e, lo que implicaría que un subconjunto de $\{1, x, \ldots, x^{e-1}\}$ estaría formado por vectores linealmente independientes sobre *cpp*, lo que no ocurre. Así pues, como x es raíz primitiva de K^*, debe ser $K = (\mathbb{Z}/\mathbb{Z}\,p)[x]$, donde x satisface la relación irreducible $m(x) = 0$.

Finalmente, para todo polinomio $f(X) \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$, la división permite escribir $f(X) = q(X)m(X)+r(X)$ donde el grado de $r(X)$ es menor que e (ó $r(X) = 0$). Así, si $f(x) = 0$ se tiene que $r(x) = 0$, lo que implica que $r(X) = 0$ por la independencia lineal de $\{1, x, \ldots, x^{e-1}\}$. Por otra parte, al ser este conjunto una base de K como $\mathbb{Z}/\mathbb{Z}\,p$-espacio vectorial, es $K \simeq (\mathbb{Z}/\mathbb{Z}\,p)^e$ como espacio vectorial, lo que implica que el número de elementos de K es p^e. Esto prueba el teorema. □

Definición 6.2.6.– *Al número primo p cuya existencia viene garantizada por el teorema 6.2.5 se le llama la característica del cuerpo K.*

Obsérvese que los teoremas 6.2.3 y 6.2.5 se resumen en el

Teorema 6.2.7.– *Un cuerpo K es finito si y sólo si se puede escribir en la forma $K = (\mathbb{Z}/\mathbb{Z}\,p)[X]/(\mathbb{Z}/\mathbb{Z}\,p)[X]\,m(X)$ donde $m(X) \in (\mathbb{Z}/\mathbb{Z}\,p)[X]$ es irreducible.*

Terminamos esta sección enunciando *el teorema chino del resto* para congruencias de polinomios. Omitimos la demostración porque es análoga a la del caso de los enteros.

Teorema 6.2.8.– (Teorema chino del resto). *Sean $m_1(X), m_2(X), \ldots, m_r(X)$, $r \geq 2$, polinomios de $K[X]$ (K es un cuerpo arbitario) dos a dos primos entre sí, es decir,* $\text{m.c.d}\,(m_i(X), m_j(X)) = 1$ *si $i \neq j$, y sea $m(X) = m_1(X)m_2(X)\cdots m_r(X)$. Se considera la función*

$$\begin{aligned}&\chi\colon K[X]/K[X]\,m(X) \longrightarrow\\ &K[X]/K[X]\,m_1(X) \times K[X]/K[X]\,m_2(X) \times \cdots \times K[X]/K[X]\,m_r(X)\\ &\alpha \longrightarrow\\ &(C_{m_1}(\alpha), C_{m_2}(\alpha), \ldots, C_{m_r}(\alpha))\,.\end{aligned}$$

Entonces χ es una biyección compatible con la suma y el producto componente a componente, es decir:

$$\begin{aligned}\chi(\alpha+\beta) &= \chi(\alpha)+\chi(\beta)\\ \chi(\alpha\beta) &= \chi(\alpha)\chi(\beta)\,.\end{aligned}$$

En otras palabras χ es un isomorfismo de anillos.

Una vez que hemos profundizado algo en los estudios de aritmética, volvemos al tema de los códigos.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 7

Códigos lineales

En este capítulo vamos a estudiar el fundamento del manejo de los códigos lineales.

7.1. Matriz estándar de un código

En esta sección se hace un uso extensivo de la noción de forma de Gauss-Jordan (o reducida por filas) de una matriz.

Recuérdese que, fijado un cuerpo K y una matriz A de dimensiones $s \times n$ sobre K, existe una matriz invertible P de dimensiones $s \times s$ tal que $A' = PA$ es la (única) forma de Gauss-Jordan de A. Se recuerda que la forma de Gauss-Jordan de una matriz es una matriz de las mismas dimensiones que tiene dos tipos de columnas:

1. Las columnas pivote: son las compuestas por un uno en la primera posición y ceros fuera, un uno en la segunda posición y ceros fuera, etc. Estas columnas están puestas de izquierda a derecha por este orden.

2. Las columnas no pivote. Cuando hay columnas no pivote entre dos pivote consecutivas, digamos entre la que tiene un 1 en la posición i y la que tiene un 1 en la posición $i+1$, las columnas no pivote tienen ceros debajo de la posición i.

UNIVERSIDAD DE SEVILLA

Un ejemplo de forma de Gauss-Jordan de una matriz sería

$$\begin{pmatrix} 1 & -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 1 & 3 & -3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

donde las columnas pivote son la primera, tercera, sexta y séptima.

Definición 7.1.1.– *Sea K un cuerpo y $\mathcal{C} \subset K^n$ un código lineal. Una permutación de las coordenadas en K^n, que se traduce en una permutación entre las letras de las palabras de $\mathcal{C}$ produce un nuevo código $\mathcal{C}' \subset K^n$, que se llama equivalente al primero.*

La idea de la equivalencia es casi trivial. Para escribir la información da lo mismo contar con un conjunto definido de palabras, que con otro que resulte del primero permutando las letras de una cierta forma determinada.

Proposición 7.1.2.– *Sea K un cuerpo finito, $\mathcal{C} \subset K^n$ un código lineal de dimensión s. Entonces $\mathcal{C}$ es equivalente a un código con matriz generadora de la forma*

$$N = \left(\begin{array}{c|c} I_{s\times s} & N_1 \end{array} \right)$$

donde $I_{s\times s}$ es la matriz unidad de las dimensiones que indica el subíndice y N_1 es un bloque $s \times (n-s)$. Una matriz de este tipo (que no es única ni mucho menos) se llama una matriz estándar. El enunciado se podría resumir diciendo que todo código lineal es equivalente a uno con matriz generadora estándar.

Demostración: La demostración que damos es constructiva. Conociendo la forma de Gauss-Jordan es terriblemente sencilla, pero hay que prestar atención a su desarrollo porque nos será muy útil en lo sucesivo. Sea M una matriz generadora de $\mathcal{C}$; existe una matriz invertible P tal que $PM = M'$ está en la forma de Gauss-Jordan. La matriz M' es también una matriz generadora de $\mathcal{C}$ porque la premultiplicación por una matriz invertible significa cambiar de base en el espacio de los vectores fila, es decir, en $\mathcal{C}$. Nótese que M' tiene s columnas pivote porque M es de rango máximo, s, que es el número de filas.

Si las columnas pivote fuesen las s primeras, ya tendríamos un bloque de matriz unidad al principio y nuestra demostración estaría concluida. Si no lo son, se pueden poner al principio mediante una permutación de columnas de la matriz. Esta permutación se realiza mediante trasposiciones, es decir, intercambiando entre sí dos columnas. Este intercambiar entre sí dos columnas distintas, digamos la i-ésima y la

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

j-ésima se realiza por postmultiplicación por una *matriz de trasposición* T_{ij}. Se obtiene la matriz T_{ij} tomando una matriz unidad $n \times n$ poniendo ceros en las posiciones (i,i) y (j,j) y unos en las posiciones (i,j) y (j,i). Es inmediato darse cuenta de que, para cualquier matriz A con n columnas, la postmultiplicación AT_{ij} intercambia las columnas i-ésima y j-ésima entre sí. Esto prueba nuestro resultado. Por supuesto, las matrices de trasposición son invertibles porque $T_{ij}^2 = I_{n\times n}$. Nótese, finalmente, que multiplicar a izquierda por una matriz de trasposición de dimensiones adecuadas significa intercambiar filas. □

Ejemplo 7.1.3.– Veamos primero cómo actúan las matrices de trasposición. La matriz que intercambia las filas (o columnas) segunda y tercera en dimensión 4 es

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Su acción sobre columnas se efectúa por posmultiplicacción. Así

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix} T = \begin{pmatrix} a_{11} & a_{13} & a_{12} & a_{14} \\ a_{21} & a_{23} & a_{22} & a_{24} \end{pmatrix}.$$

Su acción sobre filas se efectúa por premultiplicacción. Así

$$T \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \end{pmatrix}.$$

Ejemplo 7.1.4.– Elegimos ahora un cuerpo base, por ejemplo

$$K = (\mathbb{Z}/\mathbb{Z}\,3)[x]/(\mathbb{Z}/\mathbb{Z}\,3)[x]\,(x^3 + 2\,x^2 + 1)$$

de $27 = 3^3$ elementos y tomamos la matriz

$$A = \begin{pmatrix} 2\,x^2 + 2\,x & 0 & x^2 + 1 & 2\,x^2 + x + 1 \\ x^2 + 1 & 1 & 1 & 2\,x^2 + x \\ 2x + 1 & x & x^2 & 2\,x^2 + 2\,x + 1 \end{pmatrix}.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

La forma de Gauss-Jordan de A es

$$B = \begin{pmatrix} 1 & 0 & 0 & x^2+x \\ 0 & 1 & 0 & x^2+2 \\ 0 & 0 & 1 & x^2+x \end{pmatrix}$$

y la matriz de paso es

$$P = \begin{pmatrix} x^2+2 & 2\,x^2+x & x+2 \\ 2\,x^2+2 & x^2+2 & x^2+x \\ x & x+2 & 2\,x^2+x+2 \end{pmatrix}$$

de tal manera que $PA = B$. Por la forma de Gauss-Jordan reconocemos que el rango de A es 3, luego A es la matriz generadora de un código de dimensión 3 en K^4. Es claro que B es ya una forma estándar del código, luego no hay que permutar columnas para obtenerla, es decir, el factor multiplicador a derecha es la matriz identidad 4×4.

Nota 7.1.5.– La forma estándar de un código ayuda a calcular la matriz de control de una matriz M generadora del código. Sea fijada una tal matriz generadora M.

Si M está ya en forma estándar, se tiene que

$$M = \left(\begin{array}{c|c} I_{s\times s} & M_1 \end{array} \right).$$

De aquí se ve inmediatamente que

$$M \begin{pmatrix} -M_1 \\ \hline I_{(n-s)\times(n-s)} \end{pmatrix} = 0\,,$$

luego la segunda matriz (que designamos por M_c) es una matriz de control de M.

Supongamos que M no está en la forma estándar y sean $Iz \in \mathcal{M}_{s\times s}(K)$, $De \in \mathcal{M}_{n\times n}(k)$ tales que $M' = (Iz)M(De)$ es la forma estándar. Sea M'_c la matriz construida como antes; se tiene que

$$0 = M'M'_c = (Iz)M(De)M'_c$$

luego, como Iz es invertible, es $M(De)M'_c = 0$ y así $M_c = (De)M'_c$ es una matriz cuyas columnas son los coeficientes de un sistema cuyo conjunto de soluciones es $\mathcal{C}$. Así M_c es una matriz de *control* de M.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

7.2. Pesos

Recordemos (cf. definición 2.4.1) que, en un código lineal $\mathcal{C}$, el peso $w(\mathbf{a})$ de una palabra $\mathbf{a} \in \mathcal{C}$ es el número de componentes distintas de cero.

Definición 7.2.1.– *Sea $\mathcal{C} \subset K^n$ un código lineal. Se llama polinomio de pesos del código al polinomio*

$$P(Y) = \sum_{\mathbf{a} \in \mathcal{C}} Y^{w(\mathbf{a})} = \sum_{i=0}^{n} \operatorname{card}(W_i) Y^i ,$$

donde

$$W_i = \{\mathbf{a} \in \mathcal{C} \mid w(\mathbf{a}) = i\} .$$

Nota 7.2.2.– El polinomio de pesos de un código se puede calcular por barrido, escribiendo todas las palabras del código y calculando el peso de cada una. Este es un proceso largo, y puede que imposible por su longitud. En un computador personal de grandes prestaciones, el polinomio de pesos del ejemplo 7.1.4 tarda varios minutos en salir. En efecto, al tener el cuerpo base 27 elementos y ser el código de dimensión 3, el número de elementos del código es $27^3 = 19683$. Contando, aproximadamente con 12 pasadas por segundo (¡en un PC excelente!), esto hace varios minutos.

Nótese que, para construir todas las palabras de un código, se parte de una matriz generadora M, que (supongamos) es de dimensiones $s \times n$. Las palabras en que está escrita la información son los elementos de K^s. Se codifican considerándolas como una matriz por una fila y multiplicándolas por M a la derecha. Si K tiene q elementos, hay que dar q^s pasadas de programa.

En general no es fácil de calcular el polinomio de pesos. De él se deduce, evidentemente, el peso del código. A veces es más fácil de calcular directamente el peso del código. Por ejemplo, el código del ejemplo 7.1.4 tiene peso 2. En efecto, de la observación de la matriz estándar se deduce que cualquier combinación lineal de sus filas tiene, en las tres primeras posiciones, tantos elementos distintos de cero como coeficientes distintos de cero tiene la combinación lineal. Así pues, el peso del código es 2.

Ejemplo 7.2.3.– El polinomio de pesos del código $\mathcal{C}$ de matriz generadora la del ejemplo 7.1.4 tiene como polinomio de pesos

$$P(Y) = 16926\, Y^4 + 2600\, Y^3 + 156\, Y^2 + 1$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Vemos cómo la suma de los coeficientes nos da 19683, que es el número de palabras del código.

Ejemplo 7.2.4.– Si $K = \mathbb{Z}/\mathbb{Z}\,5$, el polinomio de pesos del código de matriz generadora

$$\begin{pmatrix} 4 & 4 & 4 & 4 & 1 & 0 \\ 3 & 1 & 4 & 2 & 0 & 1 \end{pmatrix}$$

es $1 + 24\,Y^5$.

El teorema central de los pesos de los códigos lineales es el que determina el peso de un código en función de los menores de la matriz de control. Es el siguiente:

Teorema 7.2.5.– *Sea $\mathcal{C} \subset K^n$ un código lineal de dimensión s. Sean M una matriz generadora M_c una matriz de control de M; entonces M tiene dimensiones $s \times n$ y M_c tiene $n \times (n-s)$. Si todas los conjuntos de $d-1$ filas de M_c son linealmente independientes, y hay algún conjunto de d filas de M_c linealmente dependientes, entonces $d = d(\mathcal{C}) = w(\mathcal{C})$.*

Demostración: Recordemos que la distancia mínima de un código es igual a su peso. Si $\mathbf{x} \in \mathcal{C}$ es una palabra de peso w, como $\mathbf{x}M_c = 0$, esto se traduce en una combinación lineal no trivial de w filas de M_c, luego en M_c existen w filas linealmente dependientes. Así, el d del enunciado es tal que $d \leq w(\mathcal{C})$.

Si existiese un conjunto de $w(\mathcal{C}) - 1$ filas de M_c que fuesen linealmente dependientes, existiría un vector $\mathbf{x} \in K^n$ con $w(\mathcal{C}) - 1$ componentes distintas de cero tal que $\mathbf{x}M_c = 0$. Esta relación implicaría que $\mathbf{x} \in \mathcal{C}$, luego en $\mathcal{C}$ habría una palabra de peso $w(\mathcal{C}) - 1$, lo que no es posible. Esto implica que $d = w(\mathcal{C})$. □

Nota 7.2.6.– El teorema 7.2.5 tiene una consecuencia sencilla pero interesante. Si $\dim(\mathcal{C}) = s$ entonces $w(\mathcal{C}) \leq n-s+1$. Esta desigualdad se llama la *cota de Singleton*. Si se alcanza la igualdad, el código se llama de *máxima distancia separable*, o código *MDS* por sus iniciales en inglés.

7.3. Corrección de errores y descodificación

Sea $\mathcal{C} \subset K^n$ un código lineal de dimensión s, con distancia mínima $d \geq 2t+1$, $t > 0$. Así, $\mathcal{C}$ corrige t errores. Supongamos, también, como datos de entrada, una matriz A generadora del código y una matriz de control A_c. Supongamos una palabra de información $\mathbf{a} \in K^s$. Se trata de realizar los pasos siguientes:

UNIVERSIDAD DE SEVILLA

1. Codificarla, es decir, computar $\mathbf{x} = \mathbf{a}A$.
2. Supuesta $\mathbf{x}$ transmitida a través de un canal que introduce, como mucho, t errores, y recibida $\mathbf{y} \in K^n$, deducir $\mathbf{x}$ a partir de $\mathbf{y}$ en el punto recpetor.
3. Descodificar $\mathbf{x}$, es decir, hallar $\mathbf{a}$.

Nota 7.3.1.– El problema de codificar y descodificar es de álgebra lineal pura. Codificar es multiplicar matrices. Por ejemplo, sea $K = \mathbb{Z}/\mathbb{Z}5$ $\mathcal{C} \subset K^6$ con matriz generadora

$$A = \begin{pmatrix} 4 & 4 & 4 & 4 & 1 & 0 \\ 3 & 1 & 4 & 2 & 0 & 1 \end{pmatrix}$$

Si $\mathbf{a} = (2, 3)$ es una palabra de información, la codificación consiste en multiplicar

$$(2, 3)A = (2, 1, 0, 4, 2, 3)$$

Descodificar una palabra $\mathbf{x} \in \mathcal{C}$ es resolver el sistema $\mathbf{a}A = \mathbf{x}$, en el que la incógnita es $\mathbf{a}$. El método estándar es el de la forma de Gauss-Jordan. Trasponiendo queda el sistema $A^t\mathbf{a}^t = \mathbf{x}^t$. Si $A' = PA^t$ es la forma de Gauss-Jordan de A^t, donde P es una matriz cuadrada no singular, el sistema es equivalente a $A'\mathbf{a}^t = P\mathbf{x}^t$ en el que ya se lee la solución. En el ejemplo anterior hay que resolver el sistema

$$A^t \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = (2, 1, 0, 4, 2, 3)^t .$$

La forma de Gauss-Jordan de A^t y la correspondiente matriz de paso son, respectivamente,

$$A' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad P = \begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 2 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Como $P(2, 1, 0, 4, 2, 3)^t = (2, 3, 0, 0, 0, 0)^t$, tenemos que $a_1 = 2$, $a_2 = 3$.

Nos queda pendiente el tema de la corrección de errorres en la transmisión. Vamos a exponer el método más elemental, que es el de construir las esferas de centros las

UNIVERSIDAD DE SEVILLA

palabras de $\mathcal{C}$. En general, supondremos que $\mathcal{C} \subset K^n$ corrige t errores, y tiene una matriz generadora A. Supondremos asimismo emitida una palabra $\mathbf{x} \in \mathcal{C}$ a través de un canal, y recibida la palabra $\mathbf{y} \in K^n$. Sabiendo que en la transmisión se han introducido t errores a lo máximo, el problema es averiguar $\mathbf{x}$ conociendo $\mathbf{y}$.

Definición 7.3.2.– *Una palabra $\mathbf{e} \in K^n$ de peso $t' \leq t$ se llamará un error se peso t'. Una palabra $\mathbf{y} \in K^n$ se dice que procede de una palabra de $\mathcal{C}$ con t' errores ($t' \leq t$) si existe una palabra $\mathbf{x} \in \mathcal{C}$ tal que $d(\mathbf{x}, \mathbf{y}) = t'$*

Lema 7.3.3.– *Una palabra $\mathbf{y} \in K^n$ procede de una palabra de $\mathcal{C}$ con t' errores, $t' \leq t$ si y sólo si $\mathbf{y} = \mathbf{x} + \mathbf{e}$, donde $\mathbf{x} \in \mathcal{C}$ y $\mathbf{e}$ es un error de peso t'.*

Demostración: Supongamos que $\mathbf{y}$ procede de $\mathbf{x} \in \mathcal{C}$ con t' errores; entonces $d(\mathbf{x}, \mathbf{y}) = t'$, luego $\mathbf{y} - \mathbf{x}$ es una palabra de peso t'. Recíprocamente, si $\mathbf{y} = \mathbf{x} + \mathbf{e}$, con $\mathbf{x} \in \mathcal{C}$ y $\mathbf{e}$ un error de peso t', entonces es claro que la distancia de $\mathbf{x}$ a $\mathbf{y}$ es t'. □

En principio, está claro un procedimiento directo de corrección de errores. Se hace una lista de todas las esferas de centros las palabras de $\mathcal{C}$ y radio t. Transmitida una palabra del código, la recibida tiene que estar en la lista. Basta mirar el centro de la esfera en que esté para identificar la transmitida.

Ejemplo 7.3.4.– Vamos a operar con un código binario, es decir, sobre $\mathbb{Z}/\mathbb{Z}\,2$, con matriz generadora

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Como las palabras de información tienen 4 componentes y hay sólo dos escalares (0 y 1), hay $2^4 = 16$ palabras de información, que son

$$\begin{array}{c} (0,0,0,0)\,,(1,0,0,0)\,,(0,2,0,0)\,,(1,1,0,0) \\ (0,0,1,0)\,,(1,0,1,0)\,,(0,1,1,0)\,,(1,1,1,0) \\ (0,0,0,1)\,,(1,0,0,1)\,,(0,2,0,1)\,,(1,1,0,1) \\ (0,0,1,1)\,,(1,0,1,1)\,,(0,1,1,1)\,,(1,1,1,1) \end{array}$$

UNIVERSIDAD DE SEVILLA

en el código. Codificándolas obtenemos las 16 palabras del código, que son, respectivamente,

$$(0,0,0,0,0,0,0),(1,1,1,0,0,0,0),(1,0,0,1,1,0,0),(0,1,1,1,1,0,0)$$
$$(0,1,0,1,0,1,0),(1,0,1,1,0,1,0),(1,1,0,0,1,1,0),(0,0,1,0,1,1,0)$$
$$(1,1,0,1,0,0,1),(0,0,1,1,0,0,1),(0,1,0,0,1,0,1),(1,0,1,0,1,0,1)$$
$$(1,0,0,0,0,1,1),(0,1,1,0,0,1,1),(0,0,0,1,1,1,1),(1,1,1,1,1,1,1)$$

Ahora podemos escribir el polinomio de pesos simplemente contando, y resulta ser $1+7Y^3+7Y^4+Y^7$. Así el código tiene peso 3 y corrige un error. Evidentemente sólo hay 7 errores de peso 1, que son

$$(1,0,0,0,0,0,0),(0,1,0,0,0,0,0),(0,0,1,0,0,0,0),(0,0,0,1,0,0,0)$$
$$(0,0,0,0,1,0,0),(0,0,0,0,0,1,0),(0,0,0,0,0,0,1)\,.$$

Por tanto, hay 16 esferas de centros cada una de las palabras del código; cada esfera tiene 8 palabras, el centro y el centro más cada uno de los errores de peso 1. Hacemos una lista de esferas, poniendo como primera palabra el centro:
Esfera 1:

$$(0,0,0,0,0,0,0),(1,0,0,0,0,0,0),(0,1,0,0,0,0,0),(0,0,1,0,0,0,0)$$
$$(0,0,0,1,0,0,0),(0,0,0,0,1,0,0),(0,0,0,0,0,1,0),(0,0,0,0,0,0,1).$$

Esfera 2:

$$(1,1,1,0,0,0,0),(0,1,1,0,0,0,0),(1,0,1,0,0,0,0),(1,1,0,0,0,0,0)$$
$$(1,1,1,1,0,0,0),(1,1,1,0,1,0,0),(1,1,1,0,0,1,0),(1,1,1,0,0,0,1)$$

Esfera 3:

$$(1,0,0,1,1,0,0),(0,0,0,1,1,0,0),(1,1,0,1,1,0,0),(1,0,1,1,1,0,0)$$
$$(1,0,0,0,1,0,0),(1,0,0,1,0,0,0),(1,0,0,1,1,1,0),(1,0,0,1,1,0,1).$$

Esfera 4:

$$(0,1,1,1,1,0,0),(1,1,1,1,1,0,0),(0,0,1,1,1,0,0),(0,1,0,1,1,0,0)$$
$$(0,1,1,0,1,0,0),(0,1,1,1,0,0,0),(0,1,1,1,1,1,0),(0,1,1,1,1,0,1).$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Esfera 5:

$$(0,1,0,1,0,1,0),(1,1,0,1,0,1,0),(0,0,0,1,0,1,0),(0,1,1,1,0,1,0)$$
$$(0,1,0,0,0,1,0),(0,1,0,1,1,1,0),(0,1,0,1,0,0,0),(0,1,0,1,0,1,1).$$

Esfera 6:

$$(1,0,1,1,0,1,0),(0,0,1,1,0,1,0),(1,1,1,1,0,1,0),(1,0,0,1,0,1,0)$$
$$(1,0,1,0,0,1,0),(1,0,1,1,1,1,0),(1,0,1,1,0,0,0),(1,0,1,1,0,1,1)$$

Esfera 7:

$$(1,1,0,0,1,1,0)(0,1,0,0,1,1,0)(1,0,0,0,1,1,0)(1,1,1,0,1,1,0)$$
$$(1,1,0,1,1,1,0)(1,1,0,0,0,1,0)(1,1,0,0,1,0,0)(1,1,0,0,1,1,1)$$

Esfera 8:

$$(0,0,1,0,1,1,0),(1,0,1,0,1,1,0),(0,1,1,0,1,1,0),(0,0,0,0,1,1,0)$$
$$(0,0,1,1,1,1,0),(0,0,1,0,0,1,0),(0,0,1,0,1,0,0),(0,0,1,0,1,1,1).$$

Esfera 9:

$$(1,1,0,1,0,0,1),(0,1,0,1,0,0,1),(1,0,0,1,0,0,1),(1,1,1,1,0,0,1)$$
$$(1,1,0,0,0,0,1),(1,1,0,1,1,0,1),(1,1,0,1,0,1,1),(1,1,0,1,0,0,0).$$

Esfera 10:

$$(0,0,1,1,0,0,1),(1,0,1,1,0,0,1),(0,1,1,1,0,0,1),(0,0,0,1,0,0,1)$$
$$(0,0,1,0,0,0,1),(0,0,1,1,1,0,1),(0,0,1,1,0,1,1),(0,0,1,1,0,0,0)$$

Esfera 11:

$$(0,1,0,0,1,0,1),(1,1,0,0,1,0,1),(0,0,0,0,1,0,1),(0,1,1,0,1,0,1)$$
$$(0,1,0,1,1,0,1),(0,1,0,0,0,0,1),(0,1,0,0,1,1,1),(0,1,0,0,1,0,0).$$

Esfera 12:

$$(1,0,1,0,1,0,1),(0,0,1,0,1,0,1),(1,1,1,0,1,0,1),(1,0,0,0,1,0,1)$$
$$(1,0,1,1,1,0,1),(1,0,1,0,0,0,1),(1,0,1,0,1,1,1),(1,0,1,0,1,0,0).$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Esfera 13:

$$(1,0,0,0,0,1,1),(0,0,0,0,0,1,1),(1,1,0,0,0,1,1),(1,0,1,0,0,1,1)$$
$$(1,0,0,1,0,1,1),(1,0,0,0,1,1,1),(1,0,0,0,0,0,1),(1,0,0,0,0,1,0).$$

Esfera 14:

$$(0,1,1,0,0,1,1),(1,1,1,0,0,1,1),(0,0,1,0,0,1,1),(0,1,0,0,0,1,1)$$
$$(0,1,1,1,0,1,1),(0,1,1,0,1,1,1),(0,1,1,0,0,0,1),(0,1,1,0,0,1,0).$$

Esfera 15:

$$(0,0,0,1,1,1,1),(1,0,0,1,1,1,1),(0,1,0,1,1,1,1),(0,0,1,1,1,1,1)$$
$$(0,0,0,0,1,1,1),(0,0,0,1,0,1,1),(0,0,0,1,1,0,1),(0,0,0,1,1,1,0).$$

Esfera 16:

$$(1,1,1,1,1,1,1),(0,1,1,1,1,1,1),(1,0,1,1,1,1,1),(1,1,0,1,1,1,1)$$
$$(1,1,1,0,1,1,1),(1,1,1,1,0,1,1),(1,1,1,1,1,0,1),(1,1,1,1,1,1,0).$$

Recibida una palabra cualquiera, se busca la esfera en que está; la palabra transmitida es el centro de esa esfera.

Sabemos que esas esferas son disjuntas. ¿Cuántos elementos hay en total? Como hay 16 esferas a 8 palabras cada una, el total de palabras en todas las esferas es de $16 \cdot 8 = 128 = 2^7$. En el espacio ambiente también hay 2^7 palabras. Todas las palabras del espacio ambiente están, pues, a una distancia de 0 ó 1 de una del código, o sea, que las esferas recubren todo el espacio ambiente. Este código es, entonces, perfecto y se llama *de Hamming*, que estudiaremos extensamente después.

7.4. Errores y síndromes

Sea K un cuerpo finito, $\mathcal{C} \subset K^n$ un código lineal con matriz generadora A y matriz de control A_c. Supongamos que el peso del código es $w(\mathcal{C}) \geq 2t+1$, con $t > 0$, lo que que implica que $\mathcal{C}$ corrige t errores a lo más. En la sección 7.3 vimos cómo se pueden corregir errores construyendo una tabla que contenga a todas las bolas con centros las palabras del código y radio t. Intente quien esto lea contruir otras tablas semejantes, con cuerpos o códigos un poco mayores. Experimentando, pronto se dará cuenta de que, o bien se obtiene un flujo de información enorme, o

bien se tarda muchísimo tiempo en construir la tabla, si es que el computador da para ello, o, más corrientemente, ambas cosas. Es decir, la técnica de corrección por listado de esferas tiene limitaciones que se alcanzan enseguida.

¿Por qué los cálculos crecen tan rápidamente? El problema está en que crecen rápidamente el número de palabras y el de errores. Si K tiene q elementos, y A es de dimensiones $s \times n$, el número de palabras del código es, evidentemente, q^s. Como se ve, esta expresión crece fortísimamente con q y s.

Sin embargo, el número de errores crece más. ¿Cuántos errores de peso a lo más t hay sobre K? Tantos como elementos tiene una bola fija de centro una palabra del código. De hecho, los errores son los elementos de la bola $B_{\mathbf{0}}$ de centro $\mathbf{0}$. Los elementos de la bola $B_{\mathbf{a}}$ de centro $\mathbf{a}$ se obtienen sumando $\mathbf{a}$ a todos los elementos de $B_{\mathbf{0}}$. El total de errores de peso $\leq t$ está ya calculado en el teorema 2.4.14, y es

$$N(q,n,t) = -1 + \sum_{i=0}^{t} \binom{n}{i} (q-1)^i = \sum_{i=1}^{t} \binom{n}{i} (q-1)^i \,.$$

El -1 viene porque hay que eliminar el centro de la bola, que no es un error. Este número crece enormemente con t porque la fórmula es polinómica. Por ejemplo, un código en dimensión 9 sobre el cuerpo con $8 = 2^3$ elementos, tiene

$$\binom{9}{1}7 + \binom{9}{2}7^2 = 1827$$

errores de pesos 1 ó 2. Y el número de errores de peso ≤ 3 es

$$\binom{9}{1}7 + \binom{9}{2}7^2 + \binom{9}{3}7^3 = 30639\,.$$

Ya se ve que esto se vuelve inmanejable bien pronto.

En esta sección vamos a dar un método de corrección ligeramente distinto: el de síndromes y errores. Este método no evita calcular tantísimos errores, o sea que tiene los mismos inconvenientes que el anterior. Sin embargo, algo se gana. La información contenida en la tabla de bolas es redundante. Se puede reducir usando síndromes.

Definición 7.4.1.– *Se llama síndrome de una palabra* $\mathbf{y} \in K^n$ *respecto de la matriz de control* A_c *a la palabra* $\mathbf{y}A_c$.

Notas 7.4.2.–

7.4.2.1. Evidentemente una palabra tiene síndrome cero si y sólo si pertenece al código, es decir,

$$\mathbf{y} \in \mathcal{C} \Longleftrightarrow \mathbf{y}A_c = 0\,,$$

UNIVERSIDAD DE SEVILLA

porque ésta es la definición de la matriz de control.

7.4.2.2. Sea $\mathbf{x} \in \mathcal{C}$, $\mathbf{e} \in K^n$ un error de peso $\leq t$, $\mathbf{y} = \mathbf{x} + \mathbf{e}$. Entonces el síndrome de $\mathbf{y}$ es el mismo que el de $\mathbf{e}$ porque

$$\mathbf{y}A_c = (\mathbf{x} + \mathbf{e})A_c = \mathbf{x}A_c + \mathbf{e}A_c = \mathbf{e}A_c$$

Esto permite reducir la escritura de la información de la tabla de bolas en el sentido que vamos a explicar.

7.4.2.3. Una fila de la tabla de bolas está formada por el resultado de sumar a todas las palabras del código un mismo error. Todas las palabras de esa fila tienen el mismo síndrome. Vamos a demostrar a continuación que, para corregir errores, basta con conocer los síndromes, no las filas enteras. Como hemos dicho, esto reduce algo los cálculos pero, sobre todo, la cantidad de resultados escritos.

Proposición 7.4.3.– *Sean* $\mathbf{e}_1 \neq \mathbf{e}_2$ *dos errores de peso* $\leq t$. *Entonces sus síndromes son distintos, es decir,* $\mathbf{e}_1 A_c \neq \mathbf{e}_2 A_c$.

Demostración: Si fuese $\mathbf{e}_1 A_c = \mathbf{e}_2 A_c$, sería

$$0 = \mathbf{e}_1 A_c - \mathbf{e}_2 A_c = (\mathbf{e}_1 - \mathbf{e}_2)A_c \,,$$

luego $\mathbf{e}_1 - \mathbf{e}_2 \in \mathcal{C}$. Esto es imposible porque el peso de $(\mathbf{e}_1 - \mathbf{e}_2)$ es $w(\mathbf{e}_1 - \mathbf{e}_2) \leq 2t < w(\mathcal{C})$. □

Notas 7.4.4.– Tablas de síndromes y errores: corrección
Supongamos calculada una lista de todos los errores de peso $\leq t$ y, para cada error, calculamos su síndrome.

7.4.4.1. Construimos ahora una tabla en la cual hay una primera columna con los síndromes y una segunda con el (único) error que tiene cada síndrome. Se la llama la *tabla de síndromes y errores*.

7.4.4.2. El proceso de corrección es ahora obvio. Se emite una palabra $\mathbf{x} \in \mathcal{C}$, desconocida por el receptor (en cuyo lugar nos situamos), que recibe $\mathbf{y} \in K^n$. El receptor halla el síndrome $\mathbf{y}A_c$ de $\mathbf{y}$. Si este síndrome no aparece en la columna correspondiente de la tabla, la transmisión ha introducido más de t errores (o, más exactamente si se quiere, un error de peso mayor que t), con lo cual no hay nada que hacer: $\mathbf{x}$ es irrecuperable.

7.4.4.3. Supongamos que el síndrome $\mathbf{y}A_c$ de $\mathbf{y}$ aparece en la tabla. Si $\mathbf{e}$ es el error correspondiente, entonces $\mathbf{x} = \mathbf{y} - \mathbf{e}$ por 7.4.2.2. Esto corrige la palabra.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Ejemplo 7.4.5.– Tomamos como cuerpo base $K = \mathbb{Z}/\mathbb{Z}5$ y el código $\mathcal{C} \subset K^6$ de matriz generadora

$$A = \begin{pmatrix} 4 & 4 & 4 & 4 & 1 & 0 \\ 3 & 1 & 4 & 2 & 0 & 1 \end{pmatrix}$$

y matriz de control

$$A_{\mathcal{C}} = \begin{pmatrix} 3 & 2 & 1 & 2 \\ 2 & 1 & 3 & 4 \\ 2 & 3 & 1 & 1 \\ 3 & 3 & 2 & 3 \\ 0 & 4 & 2 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

El código tiene, evidentemente, 25 palabras y su polinomio de pesos es $1 + 24\,Y^5$. Así $w(\mathcal{C}) = 5 = 2 \cdot 2 + 1$, luego $\mathcal{C}$ corrige errores de peso menor o igual que 2. El número de errores de peso 1 es $6 \cdot 4 = 24$ porque hay seis posiciones en las palabras y cada una de ellas puede ser rellenada con cuetro escalares: 1, 2, 3 y 4. El número de errores de peso 2 se calcula así:

1. Al haber seis posiciones, hay
$$\binom{6}{2} = 15$$
maneras de selecciones dos de ellas.

2. En cada selección de dos posiciones caben $4^2 = 16$ escalares, luego el número de errores de peso 2 es $15 \cdot 16 = 240$.

Por tanto, el número de errores de peso ≤ 2 es $24 + 240 = 264$. No los vamos a escribir, porque harían una lista enorme. Escribimos sólo diez errores de peso dos con sus síndromes:

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Errores	Síndromes
$(2,0,3,0,0,0)$	$(2,3,0,2)$
$(3,0,3,0,0,0)$	$(0,0,1,4)$
$(4,0,3,0,0,0)$	$(3,2,2,1)$
$(1,0,4,0,0,0)$	$(1,4,0,1)$
$(2,0,4,0,0,0)$	$(4,1,1,3)$
$(3,0,4,0,0,0)$	$(2,3,2,0)$
$(4,0,4,0,0,0)$	$(0,0,3,2)$
$(1,0,0,1,0,0)$	$(1,0,3,0)$
$(2,0,0,1,0,0)$	$(4,2,4,2)$
$(3,0,0,1,0,0)$	$(2,4,0,4)$

Supongamos que, en un proceso de transmisión, recibimos la palabra $(1,4,4,1,3,2)$. Hallamos su síndrome, que es $(1,4,4,1,3,2)A_{\mathcal{C}} = (2,3,2,0)$. Como ese sídrome aparece en la lista, tomamos el error correspondiente, $(3,0,4,0,0,0)$ y se lo restamos a la palabra recibida:

$$\begin{aligned}&(1,4,4,1,3,2) - (3,0,4,0,0,0) = \\ &(1,4,4,1,3,2) + (2,0,1,0,0,0) = \\ &(3,4,0,1,3,2)\end{aligned}$$

El resultado $(3,4,0,1,3,2)$ es la palabra transmitida. Decodificándola, vemos que procede de la palabra de información $(3,2)$.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 8

Diseño de códigos

La teoría de códigos correctores de errores aborda dos problemas esenciales:

1. Encontrar métodos para construir un código con un peso dado.
2. Crear algoritmos computacionales para manejarlo.

Vamos a abordar, principalmente, el primero de los problemas.

8.1. Vandermonde

Ciudadano activista conocido durante la revolución francesa, hacemos aquí memoria de él por otro tema. Se supone, naturalmente, fijado el cuerpo base. ¿Cual es el problema central del diseño de códigos de peso fijo? Encontrar una matriz A_c, de dimensiones $n \times r$, $r < n$, que tenga independientes todos los posibles subconjuntos de r filas, es decir, que toda submatriz $r \times r$ de A_c tenga determinante distinto de cero. En este caso, la matriz A_c puede ser tomada por la matriz de control de un código de dimensión $s = n - r$ y peso $r + 1$, por el teorema 7.2.5, que además es MDS porque se alcanza la igualdad en la cota de Singleton: $r + 1 = n - (n - r) + 1$. La condición de ser MDS, o sea que la matriz de control tenga r columnas y todos los conjuntos de r filas sean linealmente independientes se impone por simplicidad combinatoria. Es claro que sería más complicado exigir de una matriz $n \times r$ que tuviera todos los conjuntos de r' filas ($r' < r$) linealmente independientes, y algún conjunto de $r' + 1$ linealmente dependiente.

El lograr una matriz con esa propiedad no tiene nada de trivial: equivale a construir conjuntos de n puntos de un espacio proyectivo $\mathbb{P}^{r-1}$ sobre un cuerpo finito

UNIVERSIDAD DE SEVILLA

tales que cualesquiera r de entre ellos estén en posición general. Esta construcción tiene aspectos teóricos aún inexplorados. Nosotros vamos a dar aquí un método de conseguir unos conjuntos de ese tipo, con unas ciertas restricciones, claro. Por ello recordamos a Vandermonde.

Definición 8.1.1.– *Sea K un cuerpo finito, $\alpha = (\alpha_1, \ldots, \alpha_r)$ un vector de elementos de K^r, distintos y distintos de cero, $n \geq r$ un entero. La matriz de Vandermonde asociada es*

$$V(\alpha, n) = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \cdots & \alpha_r^{n-1} \end{pmatrix}.$$

El resultado clave sobre las matrices de Vandermonde, que no demostraremos porque pertenece al álgebra lineal elemental, es el siguiente:

Teorema 8.1.2.– *El determinante de una matriz cuadrada $V(\alpha, r)$ de Vandermonde vale*

$$\det(V(\alpha, r)) = \det \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{r-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \cdots & \alpha_r^{r-1} \end{pmatrix} = \prod_{1 \leq i < j \leq r} (\alpha_j - \alpha_i),$$

que es distinto de cero porque los α_l son distintos.

¿Cómo se pueden usar las matrices de Vandermonde para crear códigos de distancia mínima dada? Fijamos un cuerpo K de característica p, con p^e elementos, y sea $k = \mathbb{Z}/\mathbb{Z}\,p \subset K$ el cuerpo primo. Elegimos una raíz primitiva de la unidad $\alpha \in K^*$, es decir, un elemento $\alpha \in K^*$ tal que

$$K^* = \{\alpha^i \mid i \in \mathbb{Z}\} = \{\alpha^i \mid 0 \leq i < p^e - 1\},$$

(ver definición 5.2.4 y antecedentes). Nótese que $\operatorname{card}(K^*) = p^e - 1$. Por ejemplo, si $K = (\mathbb{Z}/\mathbb{Z}\,2)[x]/(\mathbb{Z}/\mathbb{Z}\,2)[x]\,(x^4 + x^3 + 1)$, vemos que x es una raíz primitiva de K^* y la tabla de sus potencias es

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

x^1	x
x^2	x^2
x^3	x^3
x^4	x^3+1
x^5	x^3+x+1
x^6	x^3+x^2+x+1
x^7	x^2+x+1
x^8	x^3+x^2+x
x^9	x^2+1
x^{10}	x^3+x
x^{11}	x^3+x^2+1
x^{12}	$x+1$
x^{13}	x^2+x
x^{14}	x^3+x^2
x^{15}	1

Una tabla como ésta se llama la *tabla de los logaritmos discretos* del cuerpo porque da cada elemento del cuerpo a la derecha como potencia de uno de ellos. La totalidad de raíces primitivas de K^* es x, x^2, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}.

Quien esto lea debe prestar mucha atención a un hecho fundamental. Es absolutamente falso que, dado un cuerpo finito en la forma $K = (\mathbb{Z}/\mathbb{Z}\,p)[x]/(\mathbb{Z}/\mathbb{Z}\,p)[x]\,(f(x))$ donde $f(x) \in (\mathbb{Z}/\mathbb{Z}\,p)[x]$ es un polinomio irreducible arbitrario, entonces x sea una raíz primitiva de K^*.

Volvemos a nuestro cuerpo K, con una raíz primitiva $\alpha \in K^*$ elegida, y vamos a ver cómo aprovechar las matrices de Vandermonde para construir un código en dimensión n que corrija errores de peso a lo más t. Todo esto tiene unas restricciones, que ahora veremos.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Consideremos la matriz de Vandermonde

$$V(\alpha,t,n)=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2t} & \alpha^{2(2t)} & \cdots & \alpha^{(n-1)(2t)} \end{pmatrix} \tag{8.1}$$

sometida a dos restricciones, para garantizar la independencia lineal de las filas y de cualesquiera $2t$ columnas:

1. $2t < n$ y
2. $n < p^e - 1$, para no repetir la primera columna.

Hay un teorema un poco enrevesado sobre esta matriz, y es el siguiente:

Teorema 8.1.3.– *En la matriz $V(\alpha,t,n)$ anterior, cualesquiera $2t$ columnas son linealmente independientes.*

Demostración: El orden máximo de los menores de esta matriz es $2t$. Cualquier menor de orden máximo es un múltiplo no nulo de un determinante de Vandermonde. En efecto, un menor de orden $2t$ de esa matriz es de la forma

$$M=\begin{vmatrix} \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{2t}} \\ \alpha^{2j_1} & \alpha^{2j_2} & \cdots & \alpha^{2j_{2t}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(2t)j_1} & \alpha^{(2t)j_2} & \cdots & \alpha^{(2t)j_{2t}} \end{vmatrix},$$

o sea,

$$M=\begin{vmatrix} \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{2t}} \\ (\alpha^2)^{j_1} & (\alpha^2)^{j_2} & \cdots & (\alpha^2)^{j_{2t}} \\ \vdots & \vdots & & \vdots \\ (\alpha^{2t})^{j_1} & (\alpha^{2t})^{j_2} & \cdots & (\alpha^{2t})^{j_{2t}} \end{vmatrix},$$

con $0 \le j_1 < j_2 < \cdots < j_{2t} \le n-1$. Sacando factores comunes de las columnas tenemos:

$$M=\alpha^{j_1+\cdots+j_{2t}}\begin{vmatrix} 1 & 1 & \cdots & 1 \\ (\alpha^1)^{j_1} & (\alpha^1)^{j_2} & \cdots & (\alpha^1)^{j_{2t}} \\ (\alpha^2)^{j_1} & (\alpha^2)^{j_2} & \cdots & (\alpha^2)^{j_{2t}} \\ \vdots & \vdots & & \vdots \\ (\alpha^{2t-1})^{j_1} & (\alpha^{2t-1})^{j_2} & \cdots & (\alpha^{2t-1})^{j_{2t}} \end{vmatrix},$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

o sea

$$M = (\alpha^a)^{j_1+\cdots+j_{2t}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ (\alpha^{j_1})^1 & (\alpha^{j_2})^1 & \cdots & (\alpha^{j_{2t}})^1 \\ (\alpha^{j_1})^2 & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_{2t}})^2 \\ \vdots & \vdots & & \vdots \\ (\alpha^{j_1})^{2t-1} & (\alpha^{j_2})^{2t-1} & \cdots & (\alpha^{j_{2t}})^{2t-1} \end{vmatrix}.$$

El determinante es de Vandermonde y su valor es

$$\prod_{1\le i<l\le 2t} \left(\alpha^{j_l} - \alpha^{j_i}\right).$$

Todas estas diferencias son distintas de cero porque las potencias correspondientes son distintas. En efecto, se trata de potencias de exponentes distintos, menores que $p^e - 1$, de una raíz primitiva. □

Terminamos esta sección con una nota indicando cómo aprovechar todo esto para el fin propuesto.

Nota 8.1.4.– La traspuesta de la matriz (8.1) se puede tomar como matriz de control de un código en K^n, de dimensión $s = n - 2t$, y peso exactamente igual a $2t + 1$. Esta construcción de un código se llama la *técnica de Vandermonde*.

Ejemplo 8.1.5.– Tomamos el cuerpo $K = (\mathbb{Z}/\mathbb{Z}\,2)[x]/(\mathbb{Z}/\mathbb{Z}\,2)[x]\,(x^3 + x + 1)$ con su tabla de logaritmos discretos, respecto de x que es una raíz primitiva:

x	x
x^2	x^2
x^3	$x + 1$
x^4	$x^2 + x$
x^5	$x^2 + x + 1$
x^6	$x^2 + 1$
x^7	1

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Una matriz de Vandermonde, que es la traspuesta de la de control de un código que corrije 2 errores sería

$$\begin{pmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 \\ 1 & x^2 & x^4 & x^6 & x^8 & x^{10} \\ 1 & x^3 & x^6 & x^9 & x^{12} & x^{15} \\ 1 & x^4 & x^8 & x^{12} & x^{16} & x^{20} \end{pmatrix}.$$

Usando la tabla de logaritmos discretos del cuerpo vemos que esa matriz es igual a

$$\begin{pmatrix} 1 & x & x^2 & x+1 & x^2+x & x^2+x+1 \\ 1 & x^2 & x^2+x & x^2+1 & x & x+1 \\ 1 & x+1 & x^2+1 & x^2 & x^2+x+1 & x \\ 1 & x^2+x & x & x^2+x+1 & x^2 & x^2+1 \end{pmatrix}.$$

Conocida la matriz de control, podemos hallar fácilmente una generadora, que es

$$\begin{pmatrix} x+1 & x & 1 & x+1 & 1 & 0 \\ x^2+1 & x^2+1 & 1 & x^2 & 0 & 1 \end{pmatrix},.$$

La palabras de información tienen dos letras, luego hay $8^2 = 64$ palabras de información y, por tanto, de código. Haciendo un barrido a través de ellas vemos que el polinomio de pesos es $1 + 42\,Y^5 + 21\,Y^6$, lo que confirma que el peso del código es 5 y, por tanto, corrige dos errores.

8.2. Códigos de Hamming

Vamos a limitarnos a los códigos de Hamming sobre los cuerpos primos.

Notas 8.2.1.– Sea K un cuerpo de característica p con p^e elementos, $e > 1$, y escribamos $n = p^e - 1$.

8.2.1.1. Consideremos una matriz de una fila

$$H = (1\,, \alpha\,, \alpha^2\,, \cdots, \alpha^{n-1})\,,$$

donde α es una raíz primitiva de K^*. Si tomamos H^t como la matriz de control de un código, éste tiene dimensión n y peso 2, que no es muy útil.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

8.2.1.2. Vamos a practicar con esta matriz lo que vamos a describir como *técnica de descenso de cuerpo*. Como siempre, escribimos $K = (\mathbb{Z}/\mathbb{Z}\,p)[x]$, donde x satisface un polinomio mónico irreducible de grado e. Cada elemento α^i lo escribimos como un polinomio en x. Escribimos los coeficientes de α^i como una columna de una matriz $e \times 1$ (contando los ceros para guardar lugares), ordenados de menor exponente a mayor, de arriba abajo. Se dice que esta matriz procede de la primera, por descenso de cuerpo. Designamos a esta matriz por $H_c(p, e)$. Por ejemplo, usando el cuerpo del ejemplo 8.1.5 y $\alpha = x$, tenemos

$$\begin{aligned} H &= (1, x, x^2, x^3, x^4, x^5, x^6) \\ &= (1, x, x^2, x+1, x^2+x, x^2+x+1, x^2+1) \end{aligned}$$

luego

$$H_c(2,3) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

8.2.1.3. La matriz traspuesta de $H_c(p, e)$ es la matriz de control de un código en un espacio ambiente de dimensión $p^e - 1$, siendo la dimensión del código $p^e - e - 1$. En efecto, para demostrar que la traspuesta de $H_c(p, e)$ es la matriz de control de un código hay que probar que tiene rango e. Como α es una raíz primitiva, los elementos de H son todos los de K^*. En particular, en $H_c(p, e)$ estarán las columnas correspondientes a $1, x, \ldots, x^{e-1}$, que son las de la matriz unidad $e \times e$. Designamos por $H(p, e)$ a una matriz generadora del código.

Nota 8.2.2.– La cuestión del peso del código es más difícil. Hay un caso muy sencillo.

Si $p = 2$, el código de matriz generadora $H(2, e)$ es de peso 3, y se llama *código binario de Hamming* de exponente e. En efecto, $H_c(2, e)$ no puede tener dos columnas linealmente dependientes porque la única constante distinta de cero que hay para multiplicar es 1. Para ver que hay tres columnas linealmente dependientes, tenemos en cuenta que, representando las columnas de arriba abajo números en binario, están todos desde 1 hasta $2^e - 1$. Así pues, están las columnas $(1, 0, \ldots, 0)^t$, $(0, 1, \ldots, 0)^t$, $(1, 1, \ldots, 0)^t$, correspondientes a los números decimales $1, 2, 3$, que son linealmente dependientes.

Si $p > 2$, el código claramente es de peso 2: en $H_c(p, e)$ aparecen las columnas $(1, 0, \ldots, 0)^t$ y $(2, 0, \ldots, 0)^t$, que son linealmente dependientes. Sin embargo, en este caso, no se toma la traspuesta de $H_c(p, e)$ como matriz de control del código de Hamming en característica p y con exponente e, sino una submatriz de ella.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Notas 8.2.3.– Sea K un cuerpo con p^e elementos, $p \geq 2$, $e > 1$, y sea $x \in K^*$ una raíz primitiva. Los elementos de K^* son entonces todos los polinomios en x de grado a lo más igual a $e-1$.

8.2.3.1. Como ya apuntamos en la sección 2.2, si nos quedamos con los coeficientes de todos los polinomios en x, de grado a lo más igual a $e-1$, ordenados de mayor a menor, de izquierda a derecha, obtenemos todos los números escritos en base p que, en representación decimal, van del 1 hasta el p^e-1. De esta forma se pueden poner los elementos de K^* en correspondencia biunívoca con los números decimales desde el 1 hasta el p^e-1. Esto indica que las columnas de $H_c(p,e)$ son todos los números entre 1 y p^e-1, escritos en base p, posiblemente ordenados en un orden distinto del natural.

8.2.3.2. Vamos a escribir las columnas de $H_c(p,e)$, con $p > 2$, ordenadas de tal manera que, de izquierda a derecha, los números correspondientes en base p crezcan. Ahora vamos a dar un algoritmo que deje solamente aquéllas columnas que formen un conjunto completo de representantes de las rectas vectoriales de $(\mathbb{Z}/\mathbb{Z}\,p)^e$. Es decir, procediendo de izquierda a derecha, vamos a eliminar toda columna que sea un múltiplo constante de una anterior (es decir, a su izquierda).

8.2.3.3. Para hacer lo anterior pensemos en todos los números desde el 1 hasta el p^e-1 escritos (en base p) en las columnas de una matriz, de menor a mayor, de izquierda a derecha; podemos suponer que, salvo orden de columnas, esta matriz es $H_c(p,e)$. La primera columna es siempre $(1,0,\ldots,0)^t$. Entonces, desplazándonos de izquierda a derecha en la matriz, eliminamos toda columna que sea un múltiplo constante de una anterior. Nótese que, después de eliminar así, hay una submatriz $e \times e$ igual a la matriz unidad porque, para cada $i > 1$, el número correspondiente a la columna $(0,\overset{i-1)}{\ldots},0,1,0\ldots,0)^t$ es p^{i-1}, y es mayor que todos los que le preceden. Queda, pues, una matriz de rango e, que volvemos a denotar por $H_c(p,e)$ porque la anterior no se usará más. Dos columnas cualesquiera de esta matriz son linealmente independientes, pero hay 3 que son linealmente dependientes: las $(1,0,\ldots,0)^t$, $(0,1,\ldots,0)^t$, $(1,1,\ldots,0)^t$, que corresponden a $1, p, p+1$.

8.2.3.4. Naturalmente, para escribir la matriz $H_c(p,e)$ de esta forma, no hace falta la raíz primitiva α. Las columnas salen en distinto orden. Se puede, si se quiere, volver a ordenar según las potencias de α y, en este caso, no aparecerán todas.

Ejemplo 8.2.4.– Tomamos el cuerpo de 9 elementos

$$K = (\mathbb{Z}/\mathbb{Z}\,3)[x]/(\mathbb{Z}/\mathbb{Z}\,3)[x]\,(x^2+x+2)$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

La matriz formada por todos los números del 1 al 8, escritos en base 3 en las columnas de una matriz, como antes, son

$$\begin{pmatrix} 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \end{pmatrix}.$$

Recorriendo la matriz de izquierda a derecha, suprimiendo las columnas múltiplos de las anteriores tenemos

$$H_c(3,2) = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Una matriz generadora del código es, entonces,

$$H(3,2) = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

y el polinomio de pesos es $1 + 32\,Y^3 + 48\,Y^4$.

La siguiente proposición 8.2.5 no versa sobre códigos de Hamming, sino sobre códigos cuya matriz generadora sea una matriz de control de un código de Hamming binario.

Proposición 8.2.5.– *El polinomio de pesos del código de matriz generadora $H_c(2,e)$ es*

$$P(X) = 1 + (2^e - 1)X^{2^{e-1}}.$$

Demostración: Basta de demostrar que toda palabra no nula del código tiene peso 2^{e-1}. Las columnas de $H_c(2,e)$ son todos los vectores no nulos de $(\mathbb{Z}/\mathbb{Z}\,2)^e$. Si $(x_1,\ldots,x_e)H_c(2,e)$ es una palabra, $(x_1,\ldots,x_e) \neq 0$, entonces el número de sus componentes nulas es igual al número de vectores de $(\mathbb{Z}/\mathbb{Z}\,2)^e$ que son ortogonales[1] a $(x_1,\ldots,x_e)$. Este número es $2^{e-1}-1$. En efecto, si, digamos, $x_1 \neq 0$ y $(\alpha_1,\ldots,\alpha_e)$ es ortogonal a $(x_1,\ldots,x_e)$, se tiene que

$$\alpha_1 = \sum_{i=2}^{e} x_i\alpha_i$$

de donde se pueden dar a las α_i, $i = 2,\ldots,e$ todos los valores exceptuando el cero simultáneo. De ahí la conclusión es obvia. Por tanto, el número de componentes no cero de $(x_1,\ldots,x_e)H_c(2,e)$ es

$$(2^e - 1) - (2^{e-1} - 1) = 2^{e-1},$$

lo que completa nuestra demostración. □

[1]En el sentido de la dualidad en espacios vectoriales

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Terminamos esta sección con un resultado notable:

Teorema 8.2.6.– *Los códigos de Hamming sobre el cuerpo primo son perfectos.*

Demostración: La matriz $H_c(p,e)$ tiene e filas y tantas columnas cuantas rectas vectoriales hay en $(\mathbb{Z}/\mathbb{Z}\,p)^e$, que son

$$\frac{p^e-1}{p-1}\,;$$

así pues, ésta es la dimensión del espacio ambiente del código. La matriz $H(p,e)$ tiene rango

$$s=\frac{p^e-1}{p-1}-e\,,$$

luego el código tiene p^s palabras. Como el código corrige un error, hemos de considerar las esferas de centros las palabras de él, y radio 1. Por el teorema 2.4.14, cada una de estas esferas tiene

$$1+\frac{p^e-1}{p-1}(p-1)=p^e$$

palabras. Como esas esferas son disjuntas, la unión de esas esferas tiene

$$p^s p^e=p^{(p^e-1)/(p-1)-e}p^e=p^{(p^e-1)/(p-1)}$$

palabras, que es igual al número de palabras del espacio ambiente. Esto prueba el teorema. □

Quizás el interés de los códigos de Hamming sea más teórico que práctico. El hecho de ser perfectos, y de haber tan pocos códigos perfectos, les da una relevancia especial.

8.3. Códigos de Reed-Solomon: introducción

Definición 8.3.1.– *Sea K un cuerpo finito de característica p con $q=p^e$ elementos, y sea $n=p^e-1=\operatorname{card}(K^*)$. Sea α una raíz primitiva y $t\in\mathbb{Z}_+$ tal que $2t<n$. Se llama código de Reed-Solomon relativo a esos datos al código en K^n cuya matriz de control es la matriz de Vandermonde (8.1), es decir*

$$V(\alpha,t,n)=\begin{pmatrix}1&\alpha&\alpha^2&\cdots&\alpha^{n-1}\\1&\alpha^2&\alpha^4&\cdots&\alpha^{2(n-1)}\\\vdots&\vdots&\vdots&&\vdots\\1&\alpha^{2t}&\alpha^{2(2t)}&\cdots&\alpha^{(n-1)(2t)}\end{pmatrix}$$

UNIVERSIDAD DE SEVILLA

Obsérvese que, por el teorema 8.1.4, el código de Reed-Solomon de matriz de control como en la definición 8.3.1 tiene peso exactamente igual a $2t+1$.

Ejemplo 8.3.2.– Si $K = \mathbb{Z}/\mathbb{Z}\,11$, tomamos $\alpha = 2$ como raíz primitiva de K^*, la matriz de control del correspondiente código de Reed-Solomon que corrige tres errores es

$$\begin{pmatrix} 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \\ 1 & 9 & 4 & 3 & 5 & 1 & 9 & 4 & 3 & 5 \end{pmatrix}^t$$

y una generadora es

$$\begin{pmatrix} 2 & 8 & 2 & 7 & 5 & 6 & 1 & 0 & 0 & 0 \\ 10 & 9 & 7 & 4 & 10 & 2 & 0 & 1 & 0 & 0 \\ 7 & 5 & 5 & 4 & 5 & 9 & 0 & 0 & 1 & 0 \\ 4 & 1 & 9 & 8 & 3 & 6 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

El polinomio de pesos del código es

$$P(Y) = 1 + 1200\,Y^7 + 1800\,Y^8 + 6100\,Y^9 + 5540\,Y^{10}$$

y, como $P(1) = 14641 = 11^4$, ése es el número de palabras del código y éste corrige, evidentemente, tres errores.

Por otra parte, empleando el cuerpo

$$K = (\mathbb{Z}/\mathbb{Z}\,2)[x]/(\mathbb{Z}/\mathbb{Z}\,2)[x]\,(x^3 + x + 1)$$

y la raíz primitiva x, el correspondiente código de Reed-Solomon que corrige 2 errores tiene como matriz de control

$$\begin{pmatrix} 1 & x & x^2 & x+1 & x^2+x & x^2+x+1 & x^2+1 \\ 1 & x^2 & x^2+x & x^2+1 & x & x+1 & x^2+x+1 \\ 1 & x+1 & x^2+1 & x^2 & x^2+x+1 & x & x^2+x \\ 1 & x^2+x & x & x^2+x+1 & x^2 & x^2+1 & x+1 \end{pmatrix}^t$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

y como matriz generadora

$$\begin{pmatrix} x+1 & x & 1 & x+1 & 1 & 0 & 0 \\ x^2+1 & x^2+1 & 1 & x^2 & 0 & 1 & 0 \\ x^2+x+1 & x^2+x & 1 & x^2+x & 0 & 0 & 1 \end{pmatrix}.$$

Su polinomio de pesos es

$$P(Y) = 1 + 147\,Y^5 + 147\,Y^6 + 217\,Y^7$$

en el que se ven todas los aspectos del código.

Vamos a tratar un aspecto esencial de los códigos de Reed-Solomon, que nos servirá de introducción a los códigos cíclicos, que daremos más adelante.

Notas 8.3.3.– Sea K un cuerpo finito de característica p con p^e elementos, y sea $n = p^e - 1 = \operatorname{card}(K^*)$. Sea α una raíz primitiva y $t \in \mathbb{Z}_+$ tal que $2t < n$. Sea

$$V(\alpha, t, n) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2t} & \alpha^{2(2t)} & \cdots & \alpha^{(n-1)(2t)} \end{pmatrix}$$

la matriz de control de un código de Reed-Solomon $\mathcal{C} \subset K^n$.

8.3.3.1. Sea $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in K^n$. La numeración de las coordenadas desde 0 hasta $n-1$ en lugar de la usual, desde 1 hasta n, no tiene ninguna importancia y ayudará a la comprensión. Entonces

$$\mathbf{a} \in \mathcal{C} \Longleftrightarrow V(\alpha, t, n) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0\,,$$

lo que es equivalente a que

$$\begin{aligned} a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} &= 0 \\ a_0 + a_1\alpha^2 + a_2\alpha^4 + \cdots + a_{n-1}\alpha^{2(n-1)} &= 0 \\ \vdots & \quad \vdots \\ a_0 + a_1\alpha^{2t} + a_2\alpha^{2(2t)} + \cdots + a_{n-1}\alpha^{(n-1)(2t)} &= 0\,. \end{aligned}$$

UNIVERSIDAD DE SEVILLA

8.3.3.2. Las relaciones de 8.3.3.1 se pueden interpretar de otra forma. Consideremos el polinomio

$$P(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_{n-1} Z^{n-1} \in K[Z]\,,$$

donde Z es una variable. Entonces esas relaciones se pueden interpretar como que

$$0 = P(\alpha) = P(\alpha^2) = \cdots P(\alpha^{2t})\,. \tag{8.2}$$

Como las potencias α^i, $i = 1, \ldots, 2t$ son distintas, por el teorema de Ruffini, las relaciones (8.2) son equivalentes a que $P(Z)$ sea divisible por

$$f(Z) = (Z - \alpha)(Z - \alpha^2) \cdots (Z - \alpha^{2t})\,.$$

A este polinomio, que es de grado $2t$, se le llama *generador* del código de Reed-Solomon.

8.3.3.3. Es decir, tenemos:

1. que podemos interpretar las palabras de K^n como polinomios en $K[Z]$ de grado, a lo más, $n-1$. Esta interpretación es biunívoca y, obviamente, es un isomorfismo lineal (es decir, de espacios vectoriales)

2. y que una palabra-polinomio $P(Z)$ pertenece al código $\mathcal{C}$ si y sólo si es múltiplo de $f(Z)$

8.3.3.4. En toda esta situación hay algo que necesita ser perfilado con cuidado. Los polinomios de $K[Z]$ de grado, a lo más, $n-1$ forman un espacio vectorial de dimensión n, con base $\{1, Z, \ldots, Z^{n-1}\}$. Sin embargo, multiplicando un polinomio de estos por uno de grado adecuado, ya nos salimos fuera del dominio de estos polinomios. Y, de todas maneras, hay que multiplicar para hallar múltiplos de $f(Z)$ porque ¿es una palabra del código, por ejemplo, $Z^{n+1} f(Z)$? La respuesta debe ser afirmativa porque $Z^{n+1} f(Z)$ se anula sobre las potencias α^i, $i = 1, \ldots, 2t$. Sin embargo, se trata de un polinomio de grado mayor que n. ¿cómo aclarar esto?

Ejemplo 8.3.4.– Consideremos un código de Reed-Solomon definido por los datos siguientes:

1. el cuerpo base K es el de 25 elementos,

   $$K = (\mathbb{Z}/\mathbb{Z}\,25)[x]/(\mathbb{Z}/\mathbb{Z}\,25)[x]\,(x^2 + 3\,x + 3)\,,$$

   con raíz primitiva x. Recordemos que K^* tiene 24 elementos; por tanto, otra raíz primitiva será, por ejemplo, $\alpha = x^5$.

2. la raíz primitiva que tomamos es $\alpha = x^5$.

3. Si t es el máximo peso de error que puede corregir el código, ha de ser $2t$ menor que la dimensión ambiente, o sea $2t < 24$, que quiere decir $t < 12$. Tomamos $t = 3$.

En estas circunstancias, el polinomio generador del código de Reed-Solomon es

$$f(Z) = Z^6 + (4\,x + 4)\,Z^5 + (3\,x + 3)\,Z^4 + (4\,x + 4)\,Z^3 + xZ^2 + 2\,Z + 3\,x + 2$$

Notas 8.3.5.– La solución a nuestro problema está en las congruencias de polinomios. Como necesitamos quedarnos con los polinomios de grado, a lo más, $n - 1$, con una estructura multiplicativa, la solución es operar con congruencias módulo un polinomio de grado n. Así, los restos de la división por este polinomio, tendrán grado $n - 1$ a lo más.

8.3.5.1. ¿Qué polinomio debemos tomar como módulo para que las cosas funcionen? Como las las potencias α^i, $i = 1, \ldots, 2t$ marcan la pauta, y como $(\alpha^i)^n = 1$, el polinomio $Z^n - 1 \in K[Z]$ se anula sobre todas ellas y, por tanto, es múltiplo de $f(Z)$. Tenemos así un candidato ideal a módulo de congruencias.

8.3.5.2. Así pues, de ahora en adelante, identificaremos los polinomios de $K[Z]$ de grado menor o igual que $n - 1$ con las congruencias módulo $Z^n - 1$. Así tenemos una buena estructura multiplicativa, que nos permite expresar coherentemente las palabras del código.

8.3.5.3. Sea $h(Z) \in K[Z]$ un polinomio cualquiera; entonces existe un polinomio $h'(Z)$ de grado menor o igual que $n - 1 - 2t$ tal que el resto de dividir $h(Z)f(Z)$ entre $Z^n - 1$ es $h'(Z)f(Z)$. En otras palabras, el concepto de "múltiplo de $f(Z)$" se conserva por paso a congruencias. En efecto, como $f(Z)|(Z^n - 1)$, podemos escribir $Z^n - 1 = h''(Z)f(Z)$. La división de polinomios da

$$h(Z)f(Z) = q(Z)(Z^n - 1) + r(Z)\,,$$

con $r(Z) = 0$ ó $\mathrm{gr}\,(r(Z)) < n$. Así,

$$h(Z)f(Z) = q(Z)h''(Z)f(Z) + r(Z)\,,$$

o sea,

$$(h(Z) - q(Z)h''(Z))f(Z) = r(Z)\,,$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

luego, poniendo $h'(Z) = h(Z) - q(Z)h''(Z)$ tenemos el resultado.

Ejemplo 8.3.6.– Continuamos con el ejemplo 8.3.4. Tomando $h(Z) = Z^{20}$ y $f_1(Z) = h(Z)f(Z)$ tenemos que

$$\begin{aligned} f_1(Z) = {} & (Z^2 + (4\,x+4)Z + 3\,x + 3)(Z^{24} - 1) + \\ & (4\,x+4)Z^{23} + xZ^{22} + 2\,Z^{21} + (3\,x+2)Z^{20} + Z^2 + \\ & (4\,x+4)Z + 3\,x + 3\,; \end{aligned}$$

designamos por f_2 al resto, que es de grado 23.

Ahora hallamos $h'(Z)$. Comprobamos que f_2 es múltiplo de f dividiendo y viendo que da resto cero. El cociente será h':

$$\begin{aligned} h'(Z) \;=\; & (4\,x+4)\,Z^{17} + (2\,x+2)\,Z^{16} + 2\,Z^{15} + (2\,x+3)\,Z^{14} + \\ & (4\,x+4)\,Z^{13} + (2\,x+1)\,Z^{12} + 3\,xZ^{11} + 4\,Z^{10} + (2\,x+3)\,Z^9 + \\ & (3\,x+1)\,Z^8 + 3\,xZ^7 + (4\,x+3)\,Z^6 + 2\,xZ^5 + (2\,x+2)\,Z^4 + \\ & (3\,x+4)\,Z^3 + (x+3)\,Z^2 + (4\,x+3)\,Z + 4\,x + 2 \end{aligned}$$

Notas 8.3.7.– De las notas 8.3.5, especialmente de 8.3.5.3, nos quedamos con el hecho de que toda palabra del código es un múltiplo de f con factor de grado $n-1-2t$.

8.3.7.1. Eso significa que, dentro del espacio ambiente $K[Z]_{n-1}$, una base del código es

$$\{f(Z), Z\,f(Z), \ldots, Z^{n-1-2t}\,f(Z)\}\,.$$

Se obtiene una matriz generadora del código escribiendo los coeficientes de los polinomios de la base anterior como las filas de una matriz. Para ello tomamos como base de $K[Z]_{n-1}$ los monomios

$$\{1, Z, Z^2, \ldots, Z^{n-1}\}$$

en este orden. Si escribimos

$$f(Z) = (Z-\alpha)(Z-\alpha^2)\cdots(Z-\alpha^{2t}) = Z^{2t} + a_{2t-1}Z^{2t-1} + \cdots + a_1 Z + a_0\,,$$

una matriz generadora es

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_{2t-1} & 1 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{2t-2} & a_{2t-1} & 1 & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & a_{2t-3} & a_{2t-2} & a_{2t-1} & \ldots & 1 \end{pmatrix}.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

8.3.7.2. La matriz A tiene $n-2t$ filas. Una palabra de información sería un vector $(b_0, b_1, \ldots, b_{n-2t-1})$, escrito como un polinomio

$$b_0 + b_1\, Z + \ldots + b_{n-2t-1}\, Z^{n-2t-1}\,.$$

Fácilmente se ve que la palabra del código correspondiente, es decir,

$$(b_0, b_1, \ldots, b_{n-2t-1}) \begin{pmatrix} a_0 & a_1 & \ldots & a_{2t-1} & 1 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{2t-2} & a_{2t-1} & 1 & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & a_{2t-3} & a_{2t-2} & a_{2t-1} & \ldots & 1 \end{pmatrix},$$

corresponde al polinomio

$$(b_0 + b_1\, Z + \ldots + b_{n-2t-1}\, Z^{n-2t-1}) f(Z)\,.$$

Esto no es más que una consecuencia de la regla del producto de matrices y de la del producto de polinomios.

8.3.7.3. Como conclusión, codificar una palabra-polinomio respecto de esa matriz generadora es multiplicarla por $f(Z)$.

Terminamos aquí esta parte. Recordemos que teníamos pendientes dos problemas:

1. diseñar códigos que corrigiesen errores de peso t dado.
2. dar algoritmos eficientes de corrección de errores, al menos más eficientes que el de la tabla de síndromes y errores.

Hemos avanzado bastante en el primer problema, al introducir la técnica de Vandermonde y su ejemplo principal, el de los códigos de Reed-Solomon. Del segundo no hemos dicho nada aún; queda pendiente para lo que sigue.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 9

Códigos cíclicos

9.1. Preliminares

Sea K un cuerpo finito de característica p con p^e elementos. Sea Z una indeterminada, $K[Z]$ el correspondiente anillo de polinomios, n un entero positivo no divisible por p, y consideremos el anillo de congruencias $R = K[Z]/K[Z] \cdot (Z^n - 1)$, al que denominaremos también $K[Z]_{n-1}$ por estar representado por los polinomios de grado menor o igual que $n-1$ (restos de divisiones por $Z^n - 1$). El lema siguiente generaliza 8.3.5.3.

Lema 9.1.1.– *Sea $f(Z)$ un divisor de $Z^n - 1$ de grado $u < n$, y sea $h(Z)f(Z)$ un múltiplo cualquiera de $f(Z)$. Existe un polinomio $h'(Z)$ de grado menor o igual que $n - 1 - u$ tal que el resto de dividir $h(Z)f(Z)$ entre $Z^n - 1$ es $h'(Z)f(Z)$. En otras palabras, el concepto de "múltiplo de $f(Z)$" se conserva por paso a congruencias.*

Demostración: Como $f(Z)|(Z^n - 1)$, podemos escribir $Z^n - 1 = h''(Z)f(Z)$. La división de polinomios da

$$h(Z)f(Z) = q(Z)(Z^n - 1) + r(Z)\,,$$

con $r(Z) = 0$ ó $\mathrm{gr}\,(r(Z)) < n$. Así,

$$h(Z)f(Z) = q(Z)h''(Z)f(Z) + r(Z)\,,$$

o sea,

$$(h(Z) - q(Z)h''(Z))f(Z) = r(Z)\,,$$

luego, poniendo $h'(Z) = h(Z) - q(Z)h''(Z)$ tenemos el resultado. □

Definición 9.1.2.– *Dado un anillo*[1] *A cualquiera, un ideal es un subconjunto $I \subset A$ que verifica:*

1. *para todo $a, b \in I$ es $a - b \in I$, es decir, I es un subgrupo del grupo aditivo.*
2. *para todo $a \in I$, $b \in A$, es $ba \in I$.*

Nótese que $\{0\}$ y A son ideales de A.

Ejemplo 9.1.3.– Los ideales de $\mathbb{Z}$ son los múltiplos de un entero no negativo. Los ideales de $K[Z]$ son los múltiplos de un polinomio[2]. La demostración se hace exclusivamente con el uso de la división; detallaremos la de los polinomios, entendiendo que la de enteros es análoga.

Si $I = \{0\}$, no hay nada que probar; supongamos $I \neq \{0\}$. Sea $0 \neq f(Z) \in I$ un polinomio de grado mínimo; claramente los múltiplos $K[Z] \cdot f(Z)$ de $f(Z)$ pertenecen a I, o sea, $K[Z] \cdot f(Z) \subset I$. Recíprocamente, sea $g(Z) \in I$ y sea $g(Z) = q(Z)f(Z) + r(Z)$ la división. Entonces $r(Z) = g(Z) - q(Z)f(Z) \in I$ luego, por minimalidad del grado de $f(Z)$, debe ser $r(Z) = 0$. Así $K[Z] \cdot f(Z) \supset I$.

En el caso de los enteros, observamos que, si $a \in I$, entonces $0 - a = -a \in I$, luego I contiene elementos positivos si $I \neq \{0\}$. Entonces, para la demostración tomamos el menor número positivo que pertenece a I.

Nota 9.1.4.– Sea A un anillo, $I \neq \{0\}$ un ideal de A. Entonces, por definición de ideal, es claro que $I = A$ si y sólo si $1 \in I$. También, $I = A$ si y sólo si I contiene a una unidad de A.

Proposición 9.1.5.– *Los ideales $I \neq \{0\}$ de $K[Z]_{n-1}$ son los conjuntos de congruencias múltiplos de un divisor $f(Z)$ de $Z^n - 1$ de grado menor que n. Este polinomio $f(Z)$ se llama generador del ideal I, y está unívocamente determinado salvo producto por constantes.*

Demostración: Si $I = A$ el resultado es claro: $f(Z) = 1$. Así pues, supondremos $I \neq A$. Cada elemento de I es una congruencia, representada por un polinomio de grado menor que n. Sea $I' \subset K[Z]$ el conjunto de todos los polinomios constituyentes de las congruencias de I, es decir, el conjunto de polinomios cuyo resto de la división

[1] Esencialmente un conjunto con dos operaciones, adición y multiplicación, verificando las propiedades formales usuales: para la adición es un grupo conmutativo y la multiplicación es asociativa, conmutativa, tiene un elemento unidad, y es distributiva respecto de la adición.

[2] Aquí no se usa la hipótesis de cuerpo finito; el resultado es cierto para cualquier cuerpo

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

por $Z^n - 1$ es un elemento de I. Entonces I' es un ideal de $K[Z]$. Esto es así por las propiedades de las congruencias: la congruencia de la suma (resp. producto) de dos polinomios es la suma (resp. producto) de las congruencias de cada polinomio. Por el ejemplo 9.1.3, $I' = K[Z] \cdot f(Z)$, para un cierto $f(Z) \in K[Z]$, que es un polinomio de grado mínimo entre los de I'.

La división polinómica en $K[Z]$ permite escribir $Z^n - 1 = q(Z)f(Z) + r(Z)$, donde $r(Z) = 0$ ó $\mathrm{gr}\,(r(Z)) < \mathrm{gr}\,(f(Z))$. En congruencias es $0 = q(Z)f(Z) + r(Z)$, o sea, $r(Z) = -q(Z)f(Z) \in I$, con lo que el polinomio $r(Z)$ debe pertenecer a I'. Eso obliga a que $r(Z) = 0$. Por tanto, por el lema 9.1.1, $I = K[Z]_{n-1} \cdot f(Z)$.

Si fuese $\mathrm{gr}\,(f(Z)) = n$, entonces $Z^n - 1$ sería un múltiplo constante de $f(Z)$, o sea, existe $\alpha \in K$ tal que $Z^n - 1 = \alpha\, f(Z)$. Así, $f(Z) = (1/\alpha)(Z^n - 1)$, luego la congruencia de $f(Z)$ es cero. Así sería $I = \{0\}$ porque los elementos de I son los múltiplos de $f(Z)$. Esto contradice el enunciado.

La última afirmación del enunciado es clara: todo otro polinomio generador de I genera I', luego es un múltiplo constante de $f(Z)$. □

Corolario 9.1.6.– *Si* $\mathrm{m.c.d}\,(n, p) = 1$*, entonces* $Z^n - 1$ *no tiene factores irreducibles múltiples. Si tiene* v *factores irreducibles (que son distintos), entonces el número de ideales de* $K[Z]_{n-1}$ *es (contando el cero y el total)*

$$\binom{v}{0} + \binom{v}{1} + \cdots \binom{v}{v-1} + \binom{v}{v} = 2^v$$

Demostración: Si $Z^n - 1$ tuviese un factor irreducible de multiplicidad mayor que 1, este factor debería dividir también a la derivada. Como ésta es $nZ^{n-1} \neq 0$ porque p no divide a n, se ve que no es posible esta situación. La afirmación referente al número de ideales es la descripción del número de divisores de $Z^n - 1$ contando todos los productos posibles de los factores irreducibles (de 1 en 1, de 2 en 2, etc). □

Ejemplo 9.1.7.– Veamos un ejemplo de factores irreducibles de un polinomio $Z^n - 1 \in K[Z]$. Sea K el cuerpo con $8 = 2^3$ elementos,

$$K = (\mathbb{Z}/\mathbb{Z}\,2)[x]/(\mathbb{Z}/\mathbb{Z}\,2)[x]\,(x^3 + x + 1)\,,$$

y consideremos el polinomio $Z^9 - 1 = Z^9 + 1 \in K[Z]$. Su descomposición factorial es

$$\begin{aligned} Z^9 - 1 \;\; = \;\; & (Z^2 + (x^2 + x)Z + 1)(Z^2 + xZ + 1)(Z^2 + Z + 1) \\ & (Z + 1)(Z^2 + x^2 Z + 1)\,. \end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

9.2. Códigos cíclicos

Consideremos el espacio vectorial K^n, identificado con el anillo de congruencias $K[Z]_{n-1}$, haciendo iguales vectores a polinomios en la forma siguiente:

$$(a_0, \ldots, a_{n-1}) \longleftrightarrow a_0 + a_1 Z + \cdots a_{n-1} Z^{n-1} .$$

Hay que tener muy presente esta identificación porque con ella se operará en el futuro frecuentemente.

Obsérvese que, por definición de ideal, todo ideal de $K[Z]_{n-1}$ es un subespacio vectorial, luego un código lineal en K^n.

Definición 9.2.1.– *Un código cíclico es un código $\mathcal{C} \subset K^n$ que es un ideal de $K[Z]_{n-1}$.*

Teorema 9.2.2.– *Sea $\mathcal{C} \subset K^n$ un código lineal; las condiciones siguientes son equivalentes:*

1. *$\mathcal{C}$ es un código cíclico*
2. *para toda palabra $(a_0, \ldots, a_{n-1}) \in \mathcal{C}$, es $(a_n, a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$. Al paso de la primera palabra a la segunda lo llamamos una permutación cíclica de la palabra con un elemento.*

La segunda condición es equivalente a que todas las permutaciones cíclicas posibles, a saber

$$(a_n, a_0, a_1, \ldots, a_{n-1}) , \quad (a_{n-1}, a_n, a_0, \ldots, a_{n-2}) , \quad (a_1, a_2, \ldots, a_n, a_0)$$

pertenezcan a $\mathcal{C}$.

Demostración: Comencemos con una observación de tipo general. Sea

$$u = a_0 + a_1 Z + \cdots + a_{n-1} Z^{n-1} \in K[Z]_{n-1} ;$$

entonces

$$\begin{aligned} Z\,u &= a_0 Z + a_1 Z^2 + \cdots + a_{n-2} Z^{n-1} + a_{n-1} Z^n \\ &= a_{n-1} + a_0 Z + a_1 Z^2 + \cdots + a_{n-2} Z^{n-1} \end{aligned}$$

UNIVERSIDAD DE SEVILLA

En otras palabras, multiplicar por Z revierte a obtener una permutación cíclica de las componentes u, la más sencilla, la que consiste en pasar la última componente al primer lugar, desplazando todas las otras un lugar a la derecha. Así,

$$\begin{aligned} Z\,u &= a_{n-1} + a_0 Z + a_1 Z^2 + \cdots + a_{n-2} Z^{n-1} \\ Z^2\,u &= a_{n-2} + a_{n-1} Z + a_0 Z^2 + a_1 Z^3 + \cdots + a_{n-3} Z^{n-1} \\ \vdots &\quad \ddots \\ Z^{n-1}\,u &= a_1 + a_2 Z + \cdots + a_{n-1} Z^{n-2} + a_0 Z^{n-1} \end{aligned}$$

La condición de ideal es, obviamente, equivalente a la siguiente:

$$u \in \mathcal{C} \Longrightarrow Zu \in \mathcal{C}\,,$$

y ésta es equivalente a

$$u \in \mathcal{C} \Longrightarrow Zu \in \mathcal{C}\,, \quad Z^2u \in \mathcal{C}\,, \quad \ldots \quad Z^{n-1}u \in \mathcal{C}\,.$$

Como productos por potencias de Z se traducen en permutaciones cíclicas de componentes, el enunciado es ya claro. □

Ejemplo 9.2.3.– El ejemplo típico de códigos cíclicos son los códigos de Reed-Solomon (véase 8.3.3.2)

A partir de ahora vamos a ver cómo, en el manejo de los códigos cíclicos, se puede sustituir el álgebra lineal por el álgebra de los polinomios. Éste es nuestro objetivo inmediato, que va en la línea de nuestro problema de simplificar algoritmos de corrección. Comenzamos sustituyendo una matriz generadora por un polinomio generador y reduciendo la codificación a operaciones con polinomios.

Notas 9.2.4.– Sea $\mathcal{C} \subset K[Z]_{n-1}$ un código cíclico. El polinomio $f(Z)$ tal que $\mathcal{C} = K[Z]_{n-1} \cdot f(Z)$ está determinado salvo producto por constantes. Cualquiera de ellos se llama un *polinomio generador* de $\mathcal{C}$. Elegiremos siempre el mónico, es decir, el que tiene coeficiente de la máxima potencia igual a 1.

9.2.4.1. Sea $f(Z)$ el polinomio generador de $\mathcal{C}$ y sea $n - s = \mathrm{gr}\,(f(Z))$. Por el lema 9.1.1, todo elementos de $\mathcal{C}$ es de la forma $h(Z)f(Z)$, donde $\mathrm{gr}\,(h(Z)) <= n - 1 - (n - s) = s - 1$. Entonces es evidente que una base de $\mathcal{C}$ como K-espacio vectorial es

$$\{f(Z)\,, Z\,f(Z)\,, Z^{s-1}\,f(Z)\}$$

Así pues, si

$$f(Z) = a_0 + a_1 Z + \cdots + a_{n-s-1} Z^{n-s-1} + a_{n-s} Z^{n-s}\,, \quad a_s \neq 0\,,$$

se obtiene una matriz generadora creando s filas con los coeficientes de $f(Z)$, desplazados en cada una un lugar respecto del anterior y rellenados los huecos con ceros. Es decir, una matriz generadora es

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-s-1} & a_{n-s} & 0 & \dots & 0 \\ 0 & a_0 & \dots & a_{n-s-2} & a_{n-s-1} & a_{n-s} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & a_{n-2s+3} & a_{n-2s+2} & a_{n-2s+1} & \dots & a_{n-s} \end{pmatrix}$$

9.2.4.2. La matriz generadora A tiene s filas. Las palabras del código se obtienen multiplicando todos los elementos $(a_0, \dots, a_{s-1}) \in K^s$ por A. Por construcción de la matriz A, si se identifica la palabra $(a_0, \dots, a_{s-1})$ con el polinomio $a_0 + a_1 Z + \cdots + a_{s-1} Z^{s-1}$, entonces $(a_0, \dots, a_{s-1})A$ se identifica con el producto de polinomios $(a_0 + a_1 Z + \cdots + a_{s-1} Z^{s-1}) f(Z)$. En otras palabras, la codificación con respecto a la matriz A se puede efectuar multiplicando polinomios. Por tanto, hemos sustituido una de las tres operaciones básicas (codificar, corregir, decodificar) por operaciones en álgebra polinómica, en lugar del álgebra lineal.

9.2.4.3. En este marco, la decodificación se hace por división de polinomios. Dada una palabra del código $h(Z)f(Z)$ con $\operatorname{gr}(h(Z)) < s$, se obtiene $h(Z)$ como el cociente de dividir código $h(Z)f(Z)$ por $f(Z)$.

Ejemplo 9.2.5.– Creamos un código de Reed-Solomon de cuerpo base

$$K = (\mathbb{Z}/\mathbb{Z}\,2)[x]/(\mathbb{Z}/\mathbb{Z}\,2)[x]\,(x^3 + x + 1)$$

con 8 elementos, que corrige dos errores, usando la raíz primitiva x^2 para variar, con matriz de control

$$\begin{pmatrix} 1 & x^2 & x^2+x & x^2+1 & x & x+1 & x^2+x+1 \\ 1 & x^2+x & x & x^2+x+1 & x^2 & x^2+1 & x+1 \\ 1 & x^2+1 & x^2+x+1 & x^2+x & x+1 & x^2 & x \\ 1 & x & x^2 & x+1 & x^2+x & x^2+x+1 & x^2+1 \end{pmatrix}^t$$

y polinomio generador

$$f(Z) = Z^4 + \left(x^2+1\right) Z^3 + Z^2 + x^2 Z + x^2 + 1$$

UNIVERSIDAD DE SEVILLA

Ahora olvidamos que estamos con un código de Reed-Solomon, quedándonos con que tenemos un código cíclico, de polinomio generador $f(Z)$, y construimos una matriz generadora como en 9.2.4.1:

$$\begin{pmatrix} x^2+1 & x^2 & 1 & x^2+1 & 1 & 0 & 0 \\ 0 & x^2+1 & x^2 & 1 & x^2+1 & 1 & 0 \\ 0 & 0 & x^2+1 & x^2 & 1 & x^2+1 & 1 \end{pmatrix}.$$

Comprobamos que se trata de una matriz generadora del código viendo que el producto por la matriz de control escrita antes es cero.

Técnicamente, una palabra de información es un polinomio de grado menor o igual que $s-1=2$, que se codifica multiplicándolo por $f(Z)$. Sin embargo, por el lema 9.1.1, si multiplicamos por $f(Z)$ un polinomio de grado arbitrario, eso es igual a multiplicar por $f(Z)$ un polinomio de grado menor o igual que $s-1=2$, como congruencias módulo $Z^n-1=Z^7-1$. Por ejemplo, la congruencia de $Z^{10}f(Z)$ módulo Z^7-1 es

$$p=\left(x^2+1\right)Z^6+Z^5+x^2Z^4+\left(x^2+1\right)Z^3+1\,,$$

que es la codificación de la palabra de información

$$p'=\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+x\,.$$

Ésta se obtiene por decodificación de p, es decir, dividiendo p por $f(Z)$.

9.3. Síndromes y errores

Vamos reinterpretar en los códigos cíclicos la noción de síndrome en los códigos lineales, para adaptarla al álgebra polinómica. Siempre llevamos a la vista nuestro objetivo de reemplazar el álgebra lineal por la polinómica, que es más rápida y efectiva en términos algorítmicos.

Fijamos un cuerpo finito K de característica p con $q=p^e$ elementos, un entero positivo $n>1$ no divisible por p y un divisor $f(Z)\in K[Z]$ de Z^n-1. Consideramos fijo también el código cíclico $\mathcal{C}$ de polinomio generador $f(Z)$.

Notas 9.3.1.– Dada una palabra $P(Z)\in K[Z]_{n-1}$ el síndrome (en el sentido del álgebra lineal) es un cierto vector que se asocia a $P(Z)$ y que es cero si y sólo si $P(Z)\in\mathcal{C}$.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

9.3.1.1. En códigos cíclicos podemos pensar en un polinomio, como reinterpretación de un vector. Por tanto, podemos pensar que el síndrome debe ser un polinomio, y hay que hacer esta idea compatible con lo que sabemos.

9.3.1.2. Un polinomio que verifique las condiciones del síndrome de $P(Z)$ puede ser el resto de dividir $P(Z)$ por $f(Z)$. Evidentemente será cero si y sólo si $P(Z)$ es múltiplo de $f(Z)$, o sea, pertenece al código.

9.3.1.3. Supongamos calculados ordenadamente los síndromes de $\{1 = Z^0, Z, Z^2, \ldots, Z^{n-1}\}$, como restos de la división por f; serán polinomios de grado $n - s - 1$, que designaremos por

$$r_0(Z) = 1\,,\ r_1(Z)\,,\ \ldots\,,\ r_{n-1}(Z)\,.$$

Se les puede interpretar como vectores de K^s tomando la lista de sus coeficientes, ordenados de izquierda a derecha de menor a mayor. Se les puede poner ordenadamente uno encima de otro, hasta constituir una matriz $n \times s$, que designamos por A_1. Haciendo esto, hay un hecho clave, que reseñamos en 9.3.1.4.

9.3.1.4. Se verifica que A_1 es una matriz de control de $\mathcal{C}$. En efecto, el resto de dividir

$$P(Z) = a_0 + a_1 Z + \cdots + a_{n-1} Z^{n-1}$$

por $f(Z)$ es

$$a_0 r_0(Z) + a_1 r_1(Z) + \cdots + a_{n-1} r_{n-1}(Z)\,,$$

que, interpretado como vector, es

$$(a_0, a_1, \ldots, a_{n-1}) A_1\,.$$

Así,

$$P(Z) \in \mathcal{C} \iff \sum_{i=0} a_i r_i(Z) = 0 \iff (a_0, a_1, \ldots, a_{n-1}) A_1 = 0\,.$$

Esto prueba que A_1 es una matriz de control y que el síndrome de una palabra-polinomio coincide con el de una palabra-vector, previa reinterpretación.

Notas 9.3.2.– Las notas 9.3.1 permiten construir una tabla de síndromes y errores, como hacíamos con los códigos lineales, pero esta vez reinterpretando todo en términos polinómicos. Puestos a hablar de errores y síndromes, con vistas a corrección, podemos hacerlo mucho mejor aquí que en los códigos lineales generales. La idea es que, para obtener una tabla de síndromes y errores, y decodificar con ella, nos basta considerar sólo los errores-polinomios con término independiente distinto de cero. Supongamos construída una tabla con estos errores y sus síndromes.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

9.3.2.1. Sea $P(Z) \in \mathcal{C}$ una palabra-polinomio, y sea $e(Z) \in K[Z]_{n-1}$ un error de peso t (que $\mathcal{C}$ pueda corregir) y grado u. Supongamos que se transmite $P(Z)$ y se recibe $P'(Z) = P(Z) + e(Z)$. Si $e(Z)$ tiene término independiente distinto de cero, entonces el síndrome de $P'(Z)$ está en la tabla. Si no, la palabra

$$Z^{n-u}P'(Z) = Z^{n-u}P(Z) + Z^{n-u}e(Z)$$

es tal que:

1. $Z^{n-u}P(Z) \in \mathcal{C}$, por definición de código cíclico, y
2. el error $Z^{n-u}e(Z)$ tiene término independiente distinto de cero, que es el coeficiente de la máxima potencia de $e(Z)$, porque $Z^n = 1$ como congruencias.

Así pues, podemos recuperar la palabra $Z^{n-u}P(Z)$ conocida $Z^{n-u}P'(Z)$ usando la tabla de síndromes y errores con término independiente distinto de cero. Recuperamos $P(Z)$ multiplicando $Z^{n-u}P(Z)$ por Z^u.

9.3.2.2. Por supuesto que, en 9.3.2.1 no conocemos el grado u del error $e(Z)$. Entonces, el procedimiento es ir multiplicando $P'(Z)$ por las sucesivas potencias de Z, desde la de exponente cero hasta la de exponente $n-1$, y hallando su síndrome, hasta éste que aparezca en la tabla. No puede ocurrir que se complete el ciclo de las multiplicaciones sin que aparezca el síndrome en la tabla, porque ello significaría que el error tiene un peso mayor que el que $\mathcal{C}$ puede corregir.

Ejemplo 9.3.3.– Seguimos con el ejemplo 9.2.5, en el que K es el cuerpo con 8 elementos y $\mathcal{C}$ es el código de Reed-Solomon (en dimensión 7) generado por el polinomio $f = Z^4 + (x^2+1)Z^3 + Z^2 + x^2Z + x^2 + 1$. Vemos una sesión completa: codificación, transmisión con introducción de error de peso 2, corrección y decodificación.

Previamente hemos de construir una tabla de errores con término independiente distinto de cero y sus síndromes. Esta tabla es

Errores	Síndromes
1	1
x	x
$x+1$	$x+1$
x^2	x^2
x^2+1	x^2+1

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

x^2+x	x^2+x
x^2+x+1	x^2+x+1
$Z+1$	$Z+1$
$xZ+1$	$xZ+1$
$(x+1)Z+1$	$(x+1)Z+1$
x^2Z+1	x^2Z+1
$\left(x^2+1\right)Z+1$	$\left(x^2+1\right)Z+1$
$\left(x^2+x\right)Z+1$	$\left(x^2+x\right)Z+1$
$\left(x^2+x+1\right)Z+1$	$\left(x^2+x+1\right)Z+1$
Z^2+1	Z^2+1
xZ^2+1	xZ^2+1
$(x+1)Z^2+1$	$(x+1)Z^2+1$
x^2Z^2+1	x^2Z^2+1
$\left(x^2+1\right)Z^2+1$	$\left(x^2+1\right)Z^2+1$
$\left(x^2+x\right)Z^2+1$	$\left(x^2+x\right)Z^2+1$
$\left(x^2+x+1\right)Z^2+1$	$\left(x^2+x+1\right)Z^2+1$
Z^3+1	Z^3+1
xZ^3+1	xZ^3+1
$(x+1)Z^3+1$	$(x+1)Z^3+1$
x^2Z^3+1	x^2Z^3+1
$\left(x^2+1\right)Z^3+1$	$\left(x^2+1\right)Z^3+1$
$\left(x^2+x\right)Z^3+1$	$\left(x^2+x\right)Z^3+1$
$\left(x^2+x+1\right)Z^3+1$	$\left(x^2+x+1\right)Z^3+1$
Z^4+1	$\left(x^2+1\right)Z^3+Z^2+x^2Z+x^2$
xZ^4+1	$Z^3+xZ^2+(x+1)Z$
$(x+1)Z^4+1$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z+1+x^2$
x^2Z^4+1	$xZ^3+x^2Z^2+\left(x^2+x\right)Z+1+x$
$\left(x^2+1\right)Z^4+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ+x+x^2$
$\left(x^2+x\right)Z^4+1$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z+x$
$\left(x^2+x+1\right)Z^4+1$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z+1+x^2+x$
Z^5+1	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z+x+x^2$
xZ^5+1	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z+x^2$
$(x+1)Z^5+1$	$Z^3+(x+1)Z^2+xZ+1+x$
x^2Z^5+1	$\left(x^2+1\right)Z^3+x^2Z^2+Z$
$\left(x^2+1\right)Z^5+1$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+1+x^2+x$
$\left(x^2+x\right)Z^5+1$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z+1+x^2$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

$\left(x^2+x+1\right)Z^5+1$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z+x$
Z^6+1	xZ^3+Z^2+xZ+x
xZ^6+1	$x^2Z^3+xZ^2+x^2Z+1+x^2+x$
$(x+1)Z^6+1$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z+x^2$
x^2Z^6+1	$(x+1)Z^3+x^2Z^2+(x+1)Z+x+x^2$
$\left(x^2+1\right)Z^6+1$	$Z^3+\left(x^2+1\right)Z^2+Z+1+x^2$
$\left(x^2+x\right)Z^6+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z$
$\left(x^2+x+1\right)Z^6+1$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z+1+x$
$Z+x$	$Z+x$
$xZ+x$	$xZ+x$
$(x+1)Z+x$	$(x+1)Z+x$
x^2Z+x	x^2Z+x
$\left(x^2+1\right)Z+x$	$\left(x^2+1\right)Z+x$
$\left(x^2+x\right)Z+x$	$\left(x^2+x\right)Z+x$
$\left(x^2+x+1\right)Z+x$	$\left(x^2+x+1\right)Z+x$
Z^2+x	Z^2+x
xZ^2+x	xZ^2+x
$(x+1)Z^2+x$	$(x+1)Z^2+x$
x^2Z^2+x	x^2Z^2+x
$\left(x^2+1\right)Z^2+x$	$\left(x^2+1\right)Z^2+x$
$\left(x^2+x\right)Z^2+x$	$\left(x^2+x\right)Z^2+x$
$\left(x^2+x+1\right)Z^2+x$	$\left(x^2+x+1\right)Z^2+x$
Z^3+x	Z^3+x
xZ^3+x	xZ^3+x
$(x+1)Z^3+x$	$(x+1)Z^3+x$
x^2Z^3+x	x^2Z^3+x
$\left(x^2+1\right)Z^3+x$	$\left(x^2+1\right)Z^3+x$
$\left(x^2+x\right)Z^3+x$	$\left(x^2+x\right)Z^3+x$
$\left(x^2+x+1\right)Z^3+x$	$\left(x^2+x+1\right)Z^3+x$
Z^4+x	$\left(x^2+1\right)Z^3+Z^2+x^2Z+1+x^2+x$
xZ^4+x	$Z^3+xZ^2+(x+1)Z+1+x$
$(x+1)Z^4+x$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z+x+x^2$
x^2Z^4+x	$xZ^3+x^2Z^2+\left(x^2+x\right)Z$
$\left(x^2+1\right)Z^4+x$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ+1+x^2$
$\left(x^2+x\right)Z^4+x$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z+1$
$\left(x^2+x+1\right)Z^4+x$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z+x^2$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Z^5+x	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z+1+x^2$
xZ^5+x	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z+1+x^2+x$
$(x+1)Z^5+x$	$Z^3+(x+1)Z^2+xZ$
x^2Z^5+x	$\left(x^2+1\right)Z^3+x^2Z^2+Z+1+x$
$\left(x^2+1\right)Z^5+x$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+x^2$
$\left(x^2+x\right)Z^5+x$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z+x+x^2$
$\left(x^2+x+1\right)Z^5+x$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z+1$
Z^6+x	xZ^3+Z^2+xZ+1
xZ^6+x	$x^2Z^3+xZ^2+x^2Z+x^2$
$(x+1)Z^6+x$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z+1+x^2+x$
x^2Z^6+x	$(x+1)Z^3+x^2Z^2+(x+1)Z+1+x^2$
$\left(x^2+1\right)Z^6+x$	$Z^3+\left(x^2+1\right)Z^2+Z+x+x^2$
$\left(x^2+x\right)Z^6+x$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z+1+x$
$\left(x^2+x+1\right)Z^6+x$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z$
$Z+x+1$	$Z+x+1$
$xZ+x+1$	$xZ+x+1$
$(x+1)Z+x+1$	$(x+1)Z+x+1$
x^2Z+x+1	x^2Z+x+1
$\left(x^2+1\right)Z+x+1$	$\left(x^2+1\right)Z+x+1$
$\left(x^2+x\right)Z+x+1$	$\left(x^2+x\right)Z+x+1$
$\left(x^2+x+1\right)Z+x+1$	$\left(x^2+x+1\right)Z+x+1$
Z^2+x+1	Z^2+x+1
xZ^2+x+1	xZ^2+x+1
$(x+1)Z^2+x+1$	$(x+1)Z^2+x+1$
x^2Z^2+x+1	x^2Z^2+x+1
$\left(x^2+1\right)Z^2+x+1$	$\left(x^2+1\right)Z^2+x+1$
$\left(x^2+x\right)Z^2+x+1$	$\left(x^2+x\right)Z^2+x+1$
$\left(x^2+x+1\right)Z^2+x+1$	$\left(x^2+x+1\right)Z^2+x+1$
Z^3+x+1	Z^3+x+1
xZ^3+x+1	xZ^3+x+1
$(x+1)Z^3+x+1$	$(x+1)Z^3+x+1$
x^2Z^3+x+1	x^2Z^3+x+1
$\left(x^2+1\right)Z^3+x+1$	$\left(x^2+1\right)Z^3+x+1$
$\left(x^2+x\right)Z^3+x+1$	$\left(x^2+x\right)Z^3+x+1$
$\left(x^2+x+1\right)Z^3+x+1$	$\left(x^2+x+1\right)Z^3+x+1$
Z^4+x+1	$\left(x^2+1\right)Z^3+Z^2+x^2Z+x+x^2$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

xZ^4+x+1	$Z^3+xZ^2+(x+1)Z+x$
$(x+1)Z^4+x+1$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z+1+x^2+x$
x^2Z^4+x+1	$xZ^3+x^2Z^2+\left(x^2+x\right)Z+1$
$\left(x^2+1\right)Z^4+x+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ+x^2$
$\left(x^2+x\right)Z^4+x+1$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z$
$\left(x^2+x+1\right)Z^4+x+1$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z+1+x^2$
Z^5+x+1	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z+x^2$
xZ^5+x+1	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z+x+x^2$
$(x+1)Z^5+x+1$	$Z^3+(x+1)Z^2+xZ+1$
x^2Z^5+x+1	$\left(x^2+1\right)Z^3+x^2Z^2+Z+x$
$\left(x^2+1\right)Z^5+x+1$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+1+x^2$
$\left(x^2+x\right)Z^5+x+1$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z+1+x^2+x$
$\left(x^2+x+1\right)Z^5+x+1$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z$
Z^6+x+1	xZ^3+Z^2+xZ
xZ^6+x+1	$x^2Z^3+xZ^2+x^2Z+1+x^2$
$(x+1)Z^6+x+1$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z+x+x^2$
x^2Z^6+x+1	$(x+1)Z^3+x^2Z^2+(x+1)Z+x^2$
$\left(x^2+1\right)Z^6+x+1$	$Z^3+\left(x^2+1\right)Z^2+Z+1+x^2+x$
$\left(x^2+x\right)Z^6+x+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z+x$
$\left(x^2+x+1\right)Z^6+x+1$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z+1$
$Z+x^2$	$Z+x^2$
$xZ+x^2$	$xZ+x^2$
$(x+1)Z+x^2$	$(x+1)Z+x^2$
x^2Z+x^2	x^2Z+x^2
$\left(x^2+1\right)Z+x^2$	$\left(x^2+1\right)Z+x^2$
$\left(x^2+x\right)Z+x^2$	$\left(x^2+x\right)Z+x^2$
$\left(x^2+x+1\right)Z+x^2$	$\left(x^2+x+1\right)Z+x^2$
Z^2+x^2	Z^2+x^2
xZ^2+x^2	xZ^2+x^2
$(x+1)Z^2+x^2$	$(x+1)Z^2+x^2$
$x^2Z^2+x^2$	$x^2Z^2+x^2$
$\left(x^2+1\right)Z^2+x^2$	$\left(x^2+1\right)Z^2+x^2$
$\left(x^2+x\right)Z^2+x^2$	$\left(x^2+x\right)Z^2+x^2$
$\left(x^2+x+1\right)Z^2+x^2$	$\left(x^2+x+1\right)Z^2+x^2$
Z^3+x^2	Z^3+x^2
xZ^3+x^2	xZ^3+x^2

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

$(x+1)Z^3+x^2$	$(x+1)Z^3+x^2$
$x^2Z^3+x^2$	$x^2Z^3+x^2$
$\left(x^2+1\right)Z^3+x^2$	$\left(x^2+1\right)Z^3+x^2$
$\left(x^2+x\right)Z^3+x^2$	$\left(x^2+x\right)Z^3+x^2$
$\left(x^2+x+1\right)Z^3+x^2$	$\left(x^2+x+1\right)Z^3+x^2$
Z^4+x^2	$\left(x^2+1\right)Z^3+Z^2+x^2Z+1$
xZ^4+x^2	$Z^3+xZ^2+(x+1)Z+1+x^2$
$(x+1)Z^4+x^2$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z$
$x^2Z^4+x^2$	$xZ^3+x^2Z^2+\left(x^2+x\right)Z+x+x^2$
$\left(x^2+1\right)Z^4+x^2$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ+1+x$
$\left(x^2+x\right)Z^4+x^2$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z+1+x^2+x$
$\left(x^2+x+1\right)Z^4+x^2$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z+x$
Z^5+x^2	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z+1+x$
xZ^5+x^2	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z+1$
$(x+1)Z^5+x^2$	$Z^3+(x+1)Z^2+xZ+x+x^2$
$x^2Z^5+x^2$	$\left(x^2+1\right)Z^3+x^2Z^2+Z+1+x^2$
$\left(x^2+1\right)Z^5+x^2$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+x$
$\left(x^2+x\right)Z^5+x^2$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z$
$\left(x^2+x+1\right)Z^5+x^2$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z+1+x^2+x$
Z^6+x^2	$xZ^3+Z^2+xZ+1+x^2+x$
xZ^6+x^2	$x^2Z^3+xZ^2+x^2Z+x$
$(x+1)Z^6+x^2$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z+1$
$x^2Z^6+x^2$	$(x+1)Z^3+x^2Z^2+(x+1)Z+1+x$
$\left(x^2+1\right)Z^6+x^2$	$Z^3+\left(x^2+1\right)Z^2+Z$
$\left(x^2+x\right)Z^6+x^2$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z+1+x^2$
$\left(x^2+x+1\right)Z^6+x^2$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z+x+x^2$
$Z+x^2+1$	$Z+x^2+1$
$xZ+x^2+1$	$xZ+x^2+1$
$(x+1)Z+x^2+1$	$(x+1)Z+x^2+1$
x^2Z+x^2+1	x^2Z+x^2+1
$\left(x^2+1\right)Z+x^2+1$	$\left(x^2+1\right)Z+x^2+1$
$\left(x^2+x\right)Z+x^2+1$	$\left(x^2+x\right)Z+x^2+1$
$\left(x^2+x+1\right)Z+x^2+1$	$\left(x^2+x+1\right)Z+x^2+1$
Z^2+x^2+1	Z^2+x^2+1
xZ^2+x^2+1	xZ^2+x^2+1
$(x+1)Z^2+x^2+1$	$(x+1)Z^2+x^2+1$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$x^2Z^2+x^2+1$	$x^2Z^2+x^2+1$
$\left(x^2+1\right)Z^2+x^2+1$	$\left(x^2+1\right)Z^2+x^2+1$
$\left(x^2+x\right)Z^2+x^2+1$	$\left(x^2+x\right)Z^2+x^2+1$
$\left(x^2+x+1\right)Z^2+x^2+1$	$\left(x^2+x+1\right)Z^2+x^2+1$
Z^3+x^2+1	Z^3+x^2+1
xZ^3+x^2+1	xZ^3+x^2+1
$(x+1)Z^3+x^2+1$	$(x+1)Z^3+x^2+1$
$x^2Z^3+x^2+1$	$x^2Z^3+x^2+1$
$\left(x^2+1\right)Z^3+x^2+1$	$\left(x^2+1\right)Z^3+x^2+1$
$\left(x^2+x\right)Z^3+x^2+1$	$\left(x^2+x\right)Z^3+x^2+1$
$\left(x^2+x+1\right)Z^3+x^2+1$	$\left(x^2+x+1\right)Z^3+x^2+1$
Z^4+x^2+1	$\left(x^2+1\right)Z^3+Z^2+x^2Z$
xZ^4+x^2+1	$Z^3+xZ^2+(x+1)Z+x^2$
$(x+1)Z^4+x^2+1$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z+1$
$x^2Z^4+x^2+1$	$xZ^3+x^2Z^2+\left(x^2+x\right)Z+1+x^2+x$
$\left(x^2+1\right)Z^4+x^2+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ+x$
$\left(x^2+x\right)Z^4+x^2+1$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z+x+x^2$
$\left(x^2+x+1\right)Z^4+x^2+1$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z+1+x$
Z^5+x^2+1	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z+x$
xZ^5+x^2+1	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z$
$(x+1)Z^5+x^2+1$	$Z^3+(x+1)Z^2+xZ+1+x^2+x$
$x^2Z^5+x^2+1$	$\left(x^2+1\right)Z^3+x^2Z^2+Z+x^2$
$\left(x^2+1\right)Z^5+x^2+1$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+1+x$
$\left(x^2+x\right)Z^5+x^2+1$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z+1$
$\left(x^2+x+1\right)Z^5+x^2+1$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z+x+x^2$
Z^6+x^2+1	$xZ^3+Z^2+xZ+x+x^2$
xZ^6+x^2+1	$x^2Z^3+xZ^2+x^2Z+1+x$
$(x+1)Z^6+x^2+1$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z$
$x^2Z^6+x^2+1$	$(x+1)Z^3+x^2Z^2+(x+1)Z+x$
$\left(x^2+1\right)Z^6+x^2+1$	$Z^3+\left(x^2+1\right)Z^2+Z+1$
$\left(x^2+x\right)Z^6+x^2+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z+x^2$
$\left(x^2+x+1\right)Z^6+x^2+1$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z+1+x^2+x$
$Z+x^2+x$	$Z+x^2+x$
$xZ+x^2+x$	$xZ+x^2+x$
$(x+1)Z+x^2+x$	$(x+1)Z+x^2+x$
x^2Z+x^2+x	x^2Z+x^2+x

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$\left(x^2+1\right)Z+x^2+x$	$\left(x^2+1\right)Z+x^2+x$
$\left(x^2+x\right)Z+x^2+x$	$\left(x^2+x\right)Z+x^2+x$
$\left(x^2+x+1\right)Z+x^2+x$	$\left(x^2+x+1\right)Z+x^2+x$
Z^2+x^2+x	Z^2+x^2+x
xZ^2+x^2+x	xZ^2+x^2+x
$(x+1)Z^2+x^2+x$	$(x+1)Z^2+x^2+x$
$x^2Z^2+x^2+x$	$x^2Z^2+x^2+x$
$\left(x^2+1\right)Z^2+x^2+x$	$\left(x^2+1\right)Z^2+x^2+x$
$\left(x^2+x\right)Z^2+x^2+x$	$\left(x^2+x\right)Z^2+x^2+x$
$\left(x^2+x+1\right)Z^2+x^2+x$	$\left(x^2+x+1\right)Z^2+x^2+x$
Z^3+x^2+x	Z^3+x^2+x
xZ^3+x^2+x	xZ^3+x^2+x
$(x+1)Z^3+x^2+x$	$(x+1)Z^3+x^2+x$
$x^2Z^3+x^2+x$	$x^2Z^3+x^2+x$
$\left(x^2+1\right)Z^3+x^2+x$	$\left(x^2+1\right)Z^3+x^2+x$
$\left(x^2+x\right)Z^3+x^2+x$	$\left(x^2+x\right)Z^3+x^2+x$
$\left(x^2+x+1\right)Z^3+x^2+x$	$\left(x^2+x+1\right)Z^3+x^2+x$
Z^4+x^2+x	$\left(x^2+1\right)Z^3+Z^2+x^2Z+1+x$
xZ^4+x^2+x	$Z^3+xZ^2+(x+1)Z+1+x^2+x$
$(x+1)Z^4+x^2+x$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z+x$
$x^2Z^4+x^2+x$	$xZ^3+x^2Z^2+\left(x^2+x\right)Z+x^2$
$\left(x^2+1\right)Z^4+x^2+x$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ+1$
$\left(x^2+x\right)Z^4+x^2+x$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z+1+x^2$
$\left(x^2+x+1\right)Z^4+x^2+x$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z$
Z^5+x^2+x	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z+1$
xZ^5+x^2+x	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z+1+x$
$(x+1)Z^5+x^2+x$	$Z^3+(x+1)Z^2+xZ+x^2$
$x^2Z^5+x^2+x$	$\left(x^2+1\right)Z^3+x^2Z^2+Z+1+x^2+x$
$\left(x^2+1\right)Z^5+x^2+x$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z$
$\left(x^2+x\right)Z^5+x^2+x$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z+x$
$\left(x^2+x+1\right)Z^5+x^2+x$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z+1+x^2$
Z^6+x^2+x	$xZ^3+Z^2+xZ+1+x^2$
xZ^6+x^2+x	$x^2Z^3+xZ^2+x^2Z$
$(x+1)Z^6+x^2+x$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z+1+x$
$x^2Z^6+x^2+x$	$(x+1)Z^3+x^2Z^2+(x+1)Z+1$
$\left(x^2+1\right)Z^6+x^2+x$	$Z^3+\left(x^2+1\right)Z^2+Z+x$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

$\left(x^2+x\right)Z^6+x^2+x$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z+1+x^2+x$
$\left(x^2+x+1\right)Z^6+x^2+x$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z+x^2$
$Z+x^2+x+1$	$Z+x^2+x+1$
$xZ+x^2+x+1$	$xZ+x^2+x+1$
$(x+1)Z+x^2+x+1$	$(x+1)Z+x^2+x+1$
x^2Z+x^2+x+1	x^2Z+x^2+x+1
$\left(x^2+1\right)Z+x^2+x+1$	$\left(x^2+1\right)Z+x^2+x+1$
$\left(x^2+x\right)Z+x^2+x+1$	$\left(x^2+x\right)Z+x^2+x+1$
$\left(x^2+x+1\right)Z+x^2+x+1$	$\left(x^2+x+1\right)Z+x^2+x+1$
Z^2+x^2+x+1	Z^2+x^2+x+1
xZ^2+x^2+x+1	xZ^2+x^2+x+1
$(x+1)Z^2+x^2+x+1$	$(x+1)Z^2+x^2+x+1$
$x^2Z^2+x^2+x+1$	$x^2Z^2+x^2+x+1$
$\left(x^2+1\right)Z^2+x^2+x+1$	$\left(x^2+1\right)Z^2+x^2+x+1$
$\left(x^2+x\right)Z^2+x^2+x+1$	$\left(x^2+x\right)Z^2+x^2+x+1$
$\left(x^2+x+1\right)Z^2+x^2+x+1$	$\left(x^2+x+1\right)Z^2+x^2+x+1$
Z^3+x^2+x+1	Z^3+x^2+x+1
xZ^3+x^2+x+1	xZ^3+x^2+x+1
$(x+1)Z^3+x^2+x+1$	$(x+1)Z^3+x^2+x+1$
$x^2Z^3+x^2+x+1$	$x^2Z^3+x^2+x+1$
$\left(x^2+1\right)Z^3+x^2+x+1$	$\left(x^2+1\right)Z^3+x^2+x+1$
$\left(x^2+x\right)Z^3+x^2+x+1$	$\left(x^2+x\right)Z^3+x^2+x+1$
$\left(x^2+x+1\right)Z^3+x^2+x+1$	$\left(x^2+x+1\right)Z^3+x^2+x+1$
Z^4+x^2+x+1	$\left(x^2+1\right)Z^3+Z^2+x^2Z+x$
xZ^4+x^2+x+1	$Z^3+xZ^2+(x+1)Z+x+x^2$
$(x+1)Z^4+x^2+x+1$	$x^2Z^3+(x+1)Z^2+\left(x^2+x+1\right)Z+1+x$
$x^2Z^4+x^2+x+1$	$xZ^3+x^2Z^2+\left(x^2+x\right)Z+1+x^2$
$\left(x^2+1\right)Z^4+x^2+x+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+1\right)Z^2+xZ$
$\left(x^2+x\right)Z^4+x^2+x+1$	$(x+1)Z^3+\left(x^2+x\right)Z^2+\left(x^2+1\right)Z+x^2$
$\left(x^2+x+1\right)Z^4+x^2+x+1$	$\left(x^2+x\right)Z^3+\left(x^2+x+1\right)Z^2+Z+1$
Z^5+x^2+x+1	$\left(x^2+x\right)Z^3+Z^2+\left(x^2+x+1\right)Z$
xZ^5+x^2+x+1	$\left(x^2+x+1\right)Z^3+xZ^2+\left(x^2+1\right)Z+x$
$(x+1)Z^5+x^2+x+1$	$Z^3+(x+1)Z^2+xZ+1+x^2$
$x^2Z^5+x^2+x+1$	$\left(x^2+1\right)Z^3+x^2Z^2+Z+x+x^2$
$\left(x^2+1\right)Z^5+x^2+x+1$	$(x+1)Z^3+\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+1$
$\left(x^2+x\right)Z^5+x^2+x+1$	$xZ^3+\left(x^2+x\right)Z^2+x^2Z+1+x$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

$\left(x^2+x+1\right)Z^5+x^2+x+1$	$x^2Z^3+\left(x^2+x+1\right)Z^2+(x+1)Z+x^2$
Z^6+x^2+x+1	$xZ^3+Z^2+xZ+x^2$
xZ^6+x^2+x+1	$x^2Z^3+xZ^2+x^2Z+1$
$(x+1)Z^6+x^2+x+1$	$\left(x^2+x\right)Z^3+(x+1)Z^2+\left(x^2+x\right)Z+x$
$x^2Z^6+x^2+x+1$	$(x+1)Z^3+x^2Z^2+(x+1)Z$
$\left(x^2+1\right)Z^6+x^2+x+1$	$Z^3+\left(x^2+1\right)Z^2+Z+1+x$
$\left(x^2+x\right)Z^6+x^2+x+1$	$\left(x^2+x+1\right)Z^3+\left(x^2+x\right)Z^2+\left(x^2+x+1\right)Z+x+x^2$
$\left(x^2+x+1\right)Z^6+x^2+x+1$	$\left(x^2+1\right)Z^3+\left(x^2+x+1\right)Z^2+\left(x^2+1\right)Z+1+x^2$

Tomamos la palabra de información

$$p'=\left(x^2+1\right)Z^2+\left(x^2+x\right)Z+x\,,$$

que codificamos multiplicándola por $f(Z)$, obteniendo la palabra

$$p=\left(x^2+1\right)Z^6+Z^5+x^2Z^4+\left(x^2+1\right)Z^3+1\,,$$

que transmitimos. En el proceso de transmisión se introduce un error de peso 2, por ejemplo $e=Z^4+Z^3$, recibiendo la palabra

$$p_1=\left(x^2+1\right)Z^6+Z^5+\left(x^2+1\right)Z^4+x^2Z^3+1$$

Hallamos el síndrome de p_1, que es el resto de dividirla por f, a saber

$$s_1=x^2Z^3+Z^2+x^2Z+1+x^2\,.$$

Buscamos este síndrome en la tabla y no lo hallamos. Hallamos el síndrome de Zp_1, que es el resto de dividirla por f, a saber

$$(x+1)Z^3+(x+1)Z+x\,.$$

Buscamos este síndrome en la tabla y no lo hallamos. Hallamos el síndrome de Z^2p_1, que es el resto de dividirla por f, a saber

$$x^2Z^3+\left(x^2+1\right)Z+x^2\,.$$

Buscamos este síndrome en la tabla y no lo hallamos. Hallamos el síndrome de Z^3p_1, que es el resto de dividirla por f, a saber

$$xZ^3+Z^2+xZ+x\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Buscamos este síndrome en la tabla, lo encontramos y vemos que corresponde al error $1 + Z^6$. Es decir, tenemos una palabra

$$p_2 = Z^3 p_1 = \left(x^2+1\right) Z^9 + Z^8 + \left(x^2+1\right) Z^7 + x^2 Z^6 + Z^3$$

cuyo síndrome es el del error $1 + Z^6$. Entonces

$$\begin{aligned} p_3 &= p_2 - (1+Z^6) = p_2 + (1+Z^6) \\ &= \left(x^2+1\right) Z^9 + Z^8 + \left(x^2+1\right) Z^7 + \left(x^2+1\right) Z^6 + Z^3 + 1 \end{aligned}$$

es una palabra del código, aunque no la transmitida. Como, en congruencias, $Z^7 = 1$, la palabra transmitida debe ser

$$Z^4 p_3 = \left(x^2+1\right) Z^{13} + Z^{12} + \left(x^2+1\right) Z^{11} + \left(x^2+1\right) Z^{10} + Z^7 + Z^4$$

que, dividida por $Z^7 - 1$, da

$$\left(x^2+1\right) Z^6 + Z^5 + x^2 Z^4 + \left(x^2+1\right) Z^3 + 1$$

que es la palabra transmitida.

Nótese que, en la tabla de errores y síndromes, hay errores que coinciden con sus síndromes. Son aquéllos errores de peso 2 cuya máxima potencia de Z es Z^3. Así pues, puede haber casos en que sea posible corregir una palabra sin usar la tabla.

9.4. Dualidad

En esta sección vamos a estudiar los códigos duales. La noción es bien sencilla de describir. Sea K un cuerpo finito de característica p con $q = p^e$ elementos. A veces consideraremos en el espacio vectorial K^n la forma cuadrática definida por la matriz unidad en la base canónica. El producto escalar es, entonces,

$$\mathbf{a} = (a_0, \ldots, a_{n-1}), \quad \mathbf{b} = (b_0, \ldots, b_{n-1}), \quad \langle a, b \rangle = \sum_{i=0}^{n-1} a_i b_i .$$

Por álgebra lineal elemental, es evidente que la variedad ortogonal a una $\mathcal{C}$ dada, de dimensión s, es una variedad lineal de dimensión $r = n - s$.

Definición 9.4.1.– *Dado un código lineal $\mathcal{C} \subset K^n$, de dimensión s, el código dual es el subespacio $\mathcal{C}^\perp$ ortogonal a $\mathcal{C}$. Tiene dimensión $r = n - s$. Si B es una matriz generadora de $\mathcal{C}^\perp$, es evidente que B^t es una matriz de control de $\mathcal{C}$.*

UNIVERSIDAD DE SEVILLA

Nuestro objetivo inmediato es ahora demostrar que el dual de un código cíclico es un código cíclico.

Se pueden estudiar la matriz de control y las características del código dual viendo la relación entre el producto de matrices y el de polinomios. Partimos de dos polinomios

$$f(Z) = \sum_{i=0}^{s} a_i Z^i \,, \quad g(Z) = \sum_{i=0}^{r} b_j Z^j \,,$$

de grados respectivos s y r. Recordamos que la fórmula del producto de polinomios es

$$f(Z)g(Z) = \sum_{l=0}^{s+r} \left(\sum_{i+j=l} a_i b_j \right) Z^l \,;$$

pongamos

$$c_l = \left(\sum_{i+j=l} a_i b_j \right) \,.$$

Vamos a ver que el producto de polinomios se puede interpretar como producto de matrices, o a la inversa.

Creamos matrices línea con $s + r$ elementos por las reglas siguientes:

1. Primero se crean dos matrices básicas, que van a dar origen a otras, y que son las siguientes:

   a) Una matriz fila con los coeficientes de $f(Z)$ ordenados de menor a mayor potencia y rellenada con ceros:

   $$U_0 = (a_0 \,, a_1 \,, \ldots \,, a_s \,, 0 \,, \overset{r-1)}{\ldots} \,, 0)$$

   b) Una matriz columna (escrita como matriz fila con el superíndice de traspuesta, para ahorrar espacio de papel) rellenada con ceros y con los coeficientes de $g(Z)$ ordenados de mayor a menor potencia:

   $$V_0 = (0 \,, \overset{s-1)}{\ldots} \,, 0 \,, b_r \,, b_{r-1} \,, \ldots \,, b_0)^t$$

2. A partir de U_0 se crean $r-1$ matrices más (dando un total de r) por la siguiente regla: se van poniendo al principio cada uno de los ceros del final, desplazando todos los elementos un lugar a la derecha cada vez que se hace esta operación:

$$\begin{aligned} U_1 &= (0 \,, a_0 \,, a_1 \,, \ldots \,, a_s \,, 0 \,, \overset{r-2)}{\ldots} \,, 0) \\ \vdots &\quad \vdots \\ U_{r-1} &= (0 \,, \overset{r-1)}{\ldots} \, 0 \,, a_0 \,, a_1 \,, \ldots \,, a_s) \end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

3. A partir de V_0 se crean $s-1$ matrices más (dando un total de s) por la siguiente regla: se van poniendo al final cada uno de los ceros del principio, desplazando todos los elementos un lugar a la izquierda cada vez que se hace esta operación:

$$\begin{aligned} V_1 &= (0\,,\overset{s-2)}{\ldots}\,,0\,,b_r\,,b_{r-1}\,,\ldots\,,b_0\,,0)^t \\ \vdots &\quad\ \vdots \\ V_{s-1} &= (b_r\,,b_{r-1}\,,\ldots\,,b_0\,,0\,,\overset{s-1)}{\ldots}\,0)^t \end{aligned}$$

A partir de aquí queda ya claro que

$$\begin{array}{l} U_0V_0 = c_{r+s-1}\ ,\ U_0V_1 = c_{r+s-2}\ ,\ \ldots\ ,\ U_0V_{s-1} = c_r \\ U_1V_0 = c_{r+s-2}\ ,\ U_1V_1 = c_{r+s-3}\ ,\ \ldots\ ,\ U_1V_{s-1} = c_{r-1} \\ \vdots \\ U_{r-1}V_0 = c_s\ ,\ U_{r-1}V_1 = c_{s-1}\ ,\ \ldots\ ,\ U_{r-1}V_{s-1} = c_1 \end{array}$$

En resumen, llamando U a la matriz que tiene como filas a las U_i ordenadas de arriba abajo y V a la matriz que tiene como columnas a las V_j ordenadas de izquierda a derecha, tenemos

$$UV = \begin{pmatrix} U_0 \\ U_1 \\ \vdots \\ U_r \end{pmatrix} \begin{pmatrix} V_0 & V_1 & \ldots & V_s \end{pmatrix} = \begin{pmatrix} c_{r+s-1} & c_{r+s-2} & \ldots & c_r \\ c_{r+s-2} & c_{r+s-3} & \ldots & c_{r-1} \\ \vdots & \vdots & & \vdots \\ c_s & c_{s-1} & \ldots & c_1 \end{pmatrix}$$

La aplicación de esto a nuestro caso es fácil. Sea $f(Z)$ el polinomio generador de un código cíclico $\mathcal{C} \subset R = K[Z]/(Z^n-1)$ y sea $g(Z) = (Z^n-1)/f(Z)$. Supongamos que $s = \mathrm{gr}\,(f(Z))$ y escribamos $r = n-s = \mathrm{gr}\,(g(Z))$. Escribamos asimismo

$$\begin{aligned} f(Z) &= a_0 + a_1Z + \cdots + a_sZ^s \\ g(Z) &= b_0 + b_1Z + \cdots + b_rZ^r\,; \end{aligned}$$

la matriz

$$\begin{pmatrix} U_0 \\ U_1 \\ \vdots \\ U_r \end{pmatrix}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

de antes es la generadora de $\mathcal{C}$. Se verifica que $UV = 0$ porque en UV están todos los coeficientes c_i de $f(Z)g(Z) = Z^n - 1$ excepto el de la máxima potencia, c_{r+s}, y el término independiente, -1. Así, V es una matriz de control de $\mathcal{C}$.

Finalmente hay que interpretar la traspuesta de V, que es

$$V^t = \begin{pmatrix} V_0^t \\ V_1^t \\ \vdots \\ V_{s-1}^t \end{pmatrix}.$$

Si la leemos de derecha a izquierda, es la matriz generadora del código $\mathcal{C}'$ de polinomio generador g. Esta forma de leer no altera absolutamente nada, porque podemos escribir las coordenadas de derecha a izquierda, en lugar de la habitual de izqauierda a derecha. Quiere esto decir que V^t es la matriz de control de un código cíclico. Todas estas reflexiones se resumen en el siguiente

Teorema 9.4.2.– *Sea $f(Z) \in K[Z]$ un polinomio generador de un código cíclico en dimensión n y sea $g(Z) = (Z^n - 1)/f(Z)$. Sea $n - s$ el grado de $f(Z)$ y s el de $g(Z)$. Sea B la matriz generadora del código cíclico $\mathcal{C}'$ generado por $g(Z)$, con los dos requerimientos siguientes:*

1. *las filas de B son los vectores*

$$g(Z), Zg(Z), \ldots, Z^{n-s-1}g(Z),$$

y

2. *las coordenadas de esos vectores están escritas de derecha a izquierda.*

Entonces B es una matriz de control del código cíclico $\mathcal{C}$ engendrado por $f(Z)$. En particular, el dual del código cíclico engendrado por $f(Z)$ es el código cíclico engendrado por $g(Z)$ (con la salvedad de la escritura).

Definición 9.4.3.– *En la situación del teorema 9.4.2, al polinomio $g(Z) = (Z^n - 1)/f(Z)$ se le llama un polinomio de control del código cíclico $\mathcal{C}$ generado por $f(Z)$.*

Ejemplo 9.4.4.– Retomamos el ejemplo 9.2.5, en el que creamos un código de Reed-Solomon con cuerpo base el de 8 elementos, usando la raíz primitiva x^2, y que corrige dos errores. Su polinomio generador es

$$f(Z) = Z^4 + \left(x^2 + 1\right) Z^3 + Z^2 + x^2 Z + x^2 + 1$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

y la matriz generadora asociada es

$$A = \begin{pmatrix} x^2+1 & x^2 & 1 & x^2+1 & 1 & 0 & 0 \\ 0 & x^2+1 & x^2 & 1 & x^2+1 & 1 & 0 \\ 0 & 0 & x^2+1 & x^2 & 1 & x^2+1 & 1 \end{pmatrix}.$$

Por otra parte vemos que

$$g(Z) = \frac{Z^7-1}{f(Z)} = Z^3 + \left(x^2+1\right) Z^2 + \left(x^2+x\right) Z + x$$

y, construyendo la matriz generadora del código cíclico de polinomio $g(Z)$, a la manera descrita antes, tenemos

$$B = \begin{pmatrix} 0 & 0 & 0 & 1 & x^2+1 & x^2+x & x \\ 0 & 0 & 1 & x^2+1 & x^2+x & x & 0 \\ 0 & 1 & x^2+1 & x^2+x & x & 0 & 0 \\ 1 & x^2+1 & x^2+x & x & 0 & 0 & 0 \end{pmatrix},$$

viéndose inmediatamente que $AB^t = 0$.

Nota 9.4.5.– Nótese que no todos los códigos cíclicos son códigos de Reed-Solomon. En el ejemplo 9.4.4, el código cíclico determinado por $g(Z)$ no es un código de Reed-Solomon porque el grado del polinomio generador de éstos es siempre par.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Facultad de Matemáticas
Departamento de Álgebra

Capítulo 10

Ejemplos de códigos cíclicos

Hasta ahora hemos usado como ejemplo estrella de los códigos cíclicos los códigos de Reed-Solomon. Hay muchos otros, bien interesantes.

10.1. Los códigos de Hamming

Ya hemos estudiado los códigos de Hamming sobre el cuerpo primo en la sección 8.2. Recordemos brevemente el caso de característica 2 únicamente, por simplicidad, y porque considerar otra característica no aporta nada nuevo en cuanto a corrección.

Notas 10.1.1.– Sea K un cuerpo de característica 2 con 2^e elementos, $e > 1$, y escribamos $n = 2^e - 1$. Pongamos, como de costumbre, $K = (\mathbb{Z}/\mathbb{Z}\,2)[x]$, donde x es una raíz primitiva de K^*.

10.1.1.1. Consideremos una matriz de una fila

$$H_c = (1\,, \alpha\,, \alpha^2\,, \cdots\,, \alpha^{n-2})\,,$$

donde α es una raíz primitiva de K^*. Escribiendo cada potencia como un polinomio en x tenemos unas expresiones

$$\alpha^i = a_{i,0} + a_{i,1}x + \cdots + a_{i,e-1}x^{e-1}\,, \quad a_{i,j} \in \mathbb{Z}/\mathbb{Z}\,p\,, \quad i = 1, \ldots, n-2\,.$$

UNIVERSIDAD DE SEVILLA

Poniendo los coeficientes de esas expresiones en columna, obtenemos una matriz, que seguimos designando por H_c,

$$\begin{pmatrix} 1 & a_{10} & a_{20} & \cdots & a_{n-2,0} \\ 0 & a_{11} & a_{21} & \cdots & a_{n-2,1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{1,e-1} & a_{2,e-1} & \cdots & a_{n-2,e-1} \end{pmatrix}.$$

10.1.1.2. La traspuesta de H_c es la matriz de control de un código de Hamming. El conjunto de palabras del código de Hamming es el conjunto de vectores $(b_0, \ldots, b_{n-2}) \in (\mathbb{Z}/\mathbb{Z}\,2)^{n-1}$ tales que

$$\begin{pmatrix} 1 & a_{10} & a_{20} & \cdots & a_{n-2,0} \\ 0 & a_{11} & a_{21} & \cdots & a_{n-2,1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{1,e-1} & a_{2,e-1} & \cdots & a_{n-2,e-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-2} \end{pmatrix} = 0\,,$$

o, lo que es lo mismo,

$$(1, \alpha, \alpha^2, \ldots, \alpha^{n-2}) \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-2} \end{pmatrix} = 0\,.$$

10.1.1.3. El apartado 10.1.1.2 nos indica que el código de Hamming se puede identificar con el conjunto de los polinomios que se anulan en α. Es fácil describir este conjunto. Se ve fácilmente cómo, para todo elemento[1] $\beta \in K$, poniendo $k = \mathbb{Z}/\mathbb{Z}\,2$, existe un polinomio $f(Z) \in k[Z]$, irreducible y mónico, tal que $f(\beta) = 0$. Más aún, todo polinomio de $k[Z]$ que se anula sobre β es múltiplo de $f(Z)$. Por eso se llama a $f(Z)$ el *polinomio mínimo* de β sobre k. La razón viene de que, al ser K finito, debe haber un conjunto de potencias linealmente independientes $\{1, \beta, \ldots, \beta_{u-1}\}$ tal que $\{1, \beta, \ldots, \beta_{u-1}, \beta_u\}$ son linealmente dependientes. Al expresar β_u como combinación lineal de las anteriores, se obtiene el polinomio mínimo. En el caso del cuerpo con 8 elementos del ejemplo 9.4.4, el polinomio $Z^3 + Z^2 + 1$ es el polinomio mínimo de

[1]Este razonamiento es válido para cualquier cuerpo finito K y cualquier subcuerpo $k \subset K$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

$x+1$, x^2+1 y x^2+x+1. En cambio, Z^3+Z+1 es el polinomio mínimo de x, x^2 y x^2+x.

10.1.1.4. Así pues, podemos identificar el código de Hamming con el conjunto de los polinomios múltiplos del polinomio mínimo $f(Z)$ de α sobre $\mathbb{Z}/\mathbb{Z}\,2$. Por tanto, el código de Hamming es un código cíclico de polinomio generador $f(Z)$.

10.2. Los códigos de Golay binarios

La desomposición factorial de $Z^{23}+1$ sobre $\mathbb{Z}/\mathbb{Z}\,2$ es

$$\begin{aligned} Z^{23}+1 &= (Z+1)(Z^{11}+Z^{10}+Z^6+Z^5+Z^4+Z^2+1) \\ &\quad (Z^{11}+Z^9+Z^7+Z^6+Z^5+Z+1)\,. \end{aligned}$$

Pongamos

$$\begin{aligned} f_1 &= Z^{11}+Z^{10}+Z^6+Z^5+Z^4+Z^2+1 \\ f_2 &= Z^{11}+Z^9+Z^7+Z^6+Z^5+Z+1 \end{aligned}$$

y consideremos los códigos cíclicos $\mathcal{C}_1$ y $\mathcal{C}_2$ engendrados por f_1 y f_2, respectivamente. Ambos tienen a $(\mathbb{Z}/\mathbb{Z}\,2)^{23}$ como espacio ambiente.

Proposición 10.2.1.– *Los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$ son equivalentes.*

Demostración: Pensemos en las palabras del código $\mathcal{C}_1$ como polinomios de grado menor que 23. La sustitución de Z por Z^5 induce una permutación de las potencias Z^i, $i=0,1,\ldots,22$, llevando Z^i sobre Z^{5i}, donde $5i$ se considera como una congruencia módulo 23. La correspondencia está ilustrada en las matrices siguientes, donde las primeras filas están constituidas por las potencias ordinarias, y las segundas por las imágenes bajo esa sustitución:

$$\begin{pmatrix} 1 & Z & Z^2 & Z^3 & Z^4 & Z^5 & Z^6 & Z^7 & Z^8 & Z^9 & Z^{10} & Z^{11} \\ 1 & Z^5 & Z^{10} & Z^{15} & Z^{20} & Z^2 & Z^7 & Z^{12} & Z^{17} & Z^{22} & Z^4 & Z^9 \end{pmatrix}$$

$$\begin{pmatrix} Z^{12} & Z^{13} & Z^{14} & Z^{15} & Z^{16} & Z^{17} & Z^{18} & Z^{19} & Z^{20} & Z^{21} & Z^{22} \\ Z^{14} & Z^{19} & Z & Z^6 & Z^{11} & Z^{16} & Z^{21} & Z^3 & Z^8 & Z^{13} & Z^{18} \end{pmatrix}$$

Así pues, esa sustitución induce un automorfismo φ del espacio vectorial $(\mathbb{Z}/\mathbb{Z}\,2)[Z]_{22}$ de los polinomios de grado menor que 23. Vamos a probar que ese automorfismo

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

lleva $\mathcal{C}_1$ sobre $\mathcal{C}_2$. Nótese que φ^{-1} está dado por la sustitución de Z por Z^{14}, ya que $(Z^5)^{14} = Z^{70} = Z^{3\cdot 23+1} = Z$ como congruencia módulo $Z^{23}+1$. Para terminar basta, pues, demostrar que $\varphi(f_1) \in \mathcal{C}_2$ y $\varphi^{-1}(f_2) \in \mathcal{C}_1$. Tenemos que, como congruencia módulo $Z^{23}+1$,

$$\begin{aligned}\varphi(f_1) &= Z^{20}+Z^{10}+Z^9+Z^7+Z^4+Z^2+1\\ &= (Z^9+Z^7+Z^4+Z+1)f_2\end{aligned}$$

luego $\varphi(\mathcal{C}_1) \subset \mathcal{C}_2$. También tenemos que, como congruencia módulo $Z^{23}+1$, es

$$\begin{aligned}\varphi^{-1}(f_2) &= Z^{16}+Z^{15}+Z^{14}+Z^{11}+Z^6+Z+1\\ &= (Z^5+Z^3+Z^2+Z+1)f_1\end{aligned}$$

luego $\varphi^{-1}(\mathcal{C}_2) \subset \mathcal{C}_1$. Esto prueba que φ es un isomorfismo de $\mathcal{C}_1$ sobre $\mathcal{C}_2$. □

Nótese que, al ser equivalentes, se pueden considerar como el mismo código. Hay que hacer notar que el automorfismo de sustitución en el que se basa la demostración no es algo casual, sino producto de una parte de la aritmética que se llama *residuos cuadráticos*. El mismo papel jugaría otra sustitución de Z por Z^n, $1 < n < 23$, siempre que n no tenga raíz cuadrada en $\mathbb{Z}/\mathbb{Z}\,23$.

Definición 10.2.2.– *El código de Golay binario $\mathcal{G}_{23}$ es cualquiera de los dos códigos $\mathcal{C}_1$, $\mathcal{C}_2$ anteriores, es decir, el código cíclico en dimensión 23 engendrado por cualquiera de los polinomios:*

$$\begin{aligned}f_1 &= Z^{11}+Z^{10}+Z^6+Z^5+Z^4+Z^2+1\\ f_2 &= Z^{11}+Z^9+Z^7+Z^6+Z^5+Z+1\end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Notas 10.2.3.– Las matrices generadoras de $\mathcal{C}_1$ y $\mathcal{C}_2$ son, respectivamente,

$$A_1 = \begin{pmatrix}
1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1
\end{pmatrix}$$

$$A_2 = \begin{pmatrix}
1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1
\end{pmatrix}$$

10.2.3.1. El polinomio de pesos común a ambos códigos es

$$1 + 253\,Y^7 + 506\,Y^8 + 1288\,Y^{12} + 1288\,Y^{11} + 506\,Y^{15} + 253\,Y^{16} + Y^{23}$$

que nos indica que la palabra formada toda por unos pertenece a ambos códigos. Es la única no nula común a ambos códigos. En efecto, por álgebra lineal sabemos que, al ser 12 la dimensión de ambos códigos, calculando el rango de la matriz formada por A_1 puesta encima de A_2, y viendo que nos da 23, es $\dim(\mathcal{C}_1 \cap \mathcal{C}_2) = 1$.

10.2.3.2. El apartado 10.2.3.1 nos dice que $\mathcal{G}_{23}$ corrige errores de peso 3.

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

Teorema 10.2.4.– *El código de Golay $\mathcal{G}_{23}$ es perfecto.*

Demostración: El código $\mathcal{G}_{23}$ tiene $2^{12} = 4096$ palabras, mientras que el espacio ambiente tiene $2^{23} = 8388608$. El número de palabras en cada esfera de centro una palabra del código y radio 3 es

$$u = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11}\,.$$

Como las esferas son disjuntas, en todas las esferas habrá $2^{12} \cdot 2^{11} = 2^{23}$ palabras, lo que cubre todo el espacio ambiente. Así, $\mathcal{G}_{23}$ es perfecto. □

Definición 10.2.5.– *Se llama código de Golay binario $\mathcal{G}_{24}$ al código lineal que se obtiene de $\mathcal{G}_{23}$ añadiendo a la matriz generadora un bit de paridad, que es la suma (módulo 2) de los elementos de cada fila.*

Como los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$ anteriores son equivalentes, lo siguen siendo al añadir un bit de paridad. Por tanto, operaremos sólo con la matriz A_2. Al añadir el bit de paridad obtenemos la matriz

$$B_2 = \begin{pmatrix}
1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&1
\end{pmatrix}$$

El polinomio de pesos es

$$1 + 759\,Y^8 + 2576\,Y^{12} + 759\,Y^{16} + Y^{24}\,,$$

en el que se ve que todas las palabras tienen peso múltiplo de 4. Al tener peso 8 el código, corrige errores de peso 3.

Teorema 10.2.6.– *El código de Golay binario $\mathcal{G}_{24}$ es autodual.*

UNIVERSIDAD DE SEVILLA

Demostración: La comprobación es meramente calculística. Basta ver que $B_1 B_1^t = 0$. □

Notas 10.2.7.– Vamos a dar un esquema de corrección de errores en $\mathcal{G}_{24}$. La idea es reducirla la corrección en $\mathcal{G}_{23}$. Tomamos como hipótesis de trabajo que las palabras recibidas tienen, como mucho, un error de peso 3. Para toda palabra $\mathbf{x} \in \mathcal{G}_{24}$, designamos por $\mathbf{x}'$ el resultado de suprimir en $\mathbf{x}$ el bit de paridad. Supongamos transmitida una palabra $\mathbf{x} \in \mathcal{G}_{24}$ y recibida una palabra $\mathbf{y} = \mathbf{x} + \mathbf{e}$, donde el peso de $\mathbf{e}$ es menor o igual que 3.

10.2.7.1. Tomando la palabra $\mathbf{y}' \in \mathcal{G}_{23}$, en ella puede haber, como máximo 3 errores. Se halla la palabra transmitida $\mathbf{z}' \in \mathcal{G}_{23}$ y se le añade el bit de paridad adecuado. Ésa es la palabra transmitida $\mathbf{x} \in \mathcal{G}_{24}$.

10.2.7.2. Razonamos la afirmación de 10.2.7.1. Nótese, antes de nada, que si en $\mathbf{y}'$ hay tres errores, el bit de paridad de la palabra recibida tiene que estar desajustado. Lo contrario significaría cuatro errores en $\mathbf{y}$. Se pueden considerar cuatro casos:

1. Si en $\mathbf{y}'$ no hay error, y el bit de paridad de $\mathbf{y}$ está ajustado, entonces $\mathbf{x} = \mathbf{y}$. Si el bit de paridad no está ajustado, se cambia y hay un error en $\mathbf{y}$.

2. Si en $\mathbf{y}'$ hay un error de peso 1, y el bit de paridad de $\mathbf{y}$ está ajustado, entonces se corrige $\mathbf{y}'$ y se ajusta el bit de paridad. Así, $\mathbf{y}$ tiene dos errores. Si el bit de paridad no está ajustado, se corrige el error de $\mathbf{y}'$ y se deja el mismo bit de paridad.

3. Si en $\mathbf{y}'$ hay un error de peso 2, y el bit de paridad de $\mathbf{y}$ está ajustado, entonces se corrige $\mathbf{y}'$ y se deja el bit de paridad. Así, $\mathbf{y}$ tiene dos errores. Si el bit de paridad no está ajustado, se corrige el error de $\mathbf{y}'$ y cambia el bit de paridad. Así $\mathbf{y}$ tiene un error de peso 3.

4. Si en $\mathbf{y}'$ hay un error de peso 3, entonces se corrige $\mathbf{y}'$ y se deja el bit de paridad. Así, $\mathbf{y}$ tiene tres errores.

10.2.7.3. La corrección de errores en $\mathcal{G}_{23}$ puede hacerse por el método general de todos los códigos cíclicos. Calculemos el número de errores de peso menor o igual que 3, en $\mathcal{G}_{23}$, con la primera componente igual a 1 (el término independiente en lenguaje polinómico). El número de errores de peso menor o igual que 3 es

$$n_3 = 1 + \binom{22}{1} + \binom{22}{2} = 254\,.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Éste es un número de errores bajo, que se puede calcular en pocos segundos en un computador estándar.

10.2.7.4. Una vez escritos los errores, el cálculo de síndromes es inmediato, por la aritmética polinómica. Puede durar escasos segundos en el caso más largo. De todas maneras, hablar de tiempos en la construcción de tablas de síndromes y errores es poco útil. Estas tablas se construyen de una vez para siempre, y se puede emplear en este proceso todo el tiempo que se desee. Lo que tiene importancia es el proceso de corrección. El caso peor se presenta cuando la palabra tiene un error en la segunda posición, en que hay que hacer 21 multiplicaciones y divisiones polinómicas. De todas formas, esto es razonable.

10.2.7.5. Hay un método clásico de corrección de errores en $\mathcal{G}_{24}$, que se puede ver en la bibliografía especializada. No lo reseñamos aquí porque no merece la pena, en tiempo de computación.

10.3. Los códigos de Golay ternarios

Comenzamos hallando la descomposición factorial de $Z^{11}-1$ sobre $\mathbb{Z}/\mathbb{Z}\,3$:

$$Z^{11}-1=(Z+2)(Z^5+2\,Z^3+Z^2+2\,Z+2)(Z^5+Z^4+2\,Z^3+Z^2+2)\,.$$

Pongamos

$$\begin{aligned} f_1 &= Z^5+2\,Z^3+Z^2+2\,Z+2\\ f_2 &= Z^5+Z^4+2\,Z^3+Z^2+2\,. \end{aligned}$$

y consideremos los códigos cíclicos $\mathcal{C}_1$ y $\mathcal{C}_2$ engendrados por f_1 y f_2, respectivamente. Ambos tienen a $(\mathbb{Z}/\mathbb{Z}\,3)^{11}$ como espacio ambiente.

Proposición 10.3.1.– *Los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$ son equivalentes.*

Demostración: Pensemos en las palabras del código $\mathcal{C}_1$ como polinomios de grado menor que 11. La sustitución de Z por Z^2 induce una permutación de las potencias Z^i, $i=0,1,\ldots,10$, llevando Z^i sobre Z^{2i}, donde $2i$ se considera como una congruencia módulo 11. La correspondencia está ilustrada en la matriz siguiente, donde la primera fila está constituida por las potencias ordinarias, y la segunda por las imágenes bajo esa sustitución:

$$\begin{pmatrix} 1 & Z & Z^2 & Z^3 & Z^4 & Z^5 & Z^6 & Z^7 & Z^8 & Z^9 & Z^{10}\\ 1 & Z^2 & Z^4 & Z^6 & Z^8 & Z^{10} & Z & Z^3 & Z^5 & Z^7 & Z^9 \end{pmatrix}.$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Así pues, esa sustitución induce un automorfismo φ del espacio vectorial $(\mathbb{Z}/\mathbb{Z}\,3)[Z]_{10}$ de los polinomios de grado menor que 11. Vamos a probar que ese automorfismo lleva $\mathcal{C}_1$ sobre $\mathcal{C}_2$. Nótese que φ^{-1} está dado por la sustitución de Z por Z^2, ya que $(Z^2)^6 = Z^{12} = Z^{11+1} = Z$ como congruencia módulo $Z^{11} - 1$. Para terminar basta, pues, demostrar que $\varphi(f_1) \in \mathcal{C}_2$ y $\varphi^{-1}(f_2) \in \mathcal{C}_1$.

Tenemos que

$$\begin{aligned} f_1(Z^2) &= Z^{10} + 2\,Z^6 + Z^4 + 2\,Z^2 + 2 \\ &= (Z^5 + 2\,Z^4 + 2\,Z^3 + 2\,Z^2 + 1) f_2 \\ f_2(Z^6) &= Z^{30} + Z^{24} + 2\,Z^{18} + Z^{12} + 2 \\ &= (Z^{19} + Z^{13} + Z^8 + 2\,Z^7 + Z^2 + Z)(Z^{11-1}) \\ &\quad + (Z^8 + 2\,Z^7 + Z^2 + Z + 2) \end{aligned}$$

y

$$Z^8 + 2\,Z^7 + Z^2 + Z + 2 = (Z^3 + 2\,Z^2 + Z + 1) f_1\,,$$

lo que prueba nuestro aserto. □

Nótese que, al ser equivalentes, se pueden considerar como el mismo código. Hay que hacer notar que el automorfismo de sustitución en el que se basa la demostración no es algo casual, sino producto de una parte de la aritmética que se llama *residuos cuadráticos*. El mismo papel jugaría otra sustitución de Z por Z^n, $1 < n < 11$, siempre que n no tenga raíz cuadrada en $\mathbb{Z}/\mathbb{Z}\,11$.

Definición 10.3.2.– *El código de Golay ternario $\mathcal{G}_{11}$ es cualquiera de los dos códigos $\mathcal{C}_1$, $\mathcal{C}_2$ anteriores, es decir, el código cíclico en dimensión* 11 *engendrado por cualquiera de los polinomios:*

$$\begin{aligned} f_1 &= Z^5 + 2\,Z^3 + Z^2 + 2\,Z + 2 \\ f_2 &= Z^5 + Z^4 + 2\,Z^3 + Z^2 + 2\,. \end{aligned}$$

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD SEVILLA

Notas 10.3.3.– Las matrices generadoras de $\mathcal{C}_1$ y $\mathcal{C}_2$ son, respectivamente,

$$A_1 = \begin{pmatrix} 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 \end{pmatrix}.$$

10.3.3.1. El polinomio de pesos común es

$$1 + 132\,Y^5 + 132\,Y^6 + 330\,Y^8 + 110\,Y^9 + 24\,Y^{11}$$

con lo que corrige dos errores (o corrige errores de peso 2).

Teorema 10.3.4.– *El código de Golay $\mathcal{G}_{11}$ es perfecto.*

Demostración: El código $\mathcal{G}_{11}$ tiene $3^6 = 729$ palabras, mientras que el espacio ambiente tiene $3^{11} = 177147$. El número de palabras en cada esfera de centro una palabra del código y radio 2 es

$$u = 1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 2^2 243 = 3^5\,.$$

Como las esferas son disjuntas, en todas las esferas habrá $3^6 \cdot 3^5 = 3^{11}$ palabras, lo que cubre todo el espacio ambiente. Así, $\mathcal{G}_{11}$ es perfecto. □

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA

Definición 10.3.5.– *Se llama código de Golay ternario $\mathcal{G}_{12}$ al código lineal que se obtiene de $\mathcal{G}_{11}$ añadiendo a la matriz generadora un bit de paridad, que es el opuesto de la suma (módulo 3) de los elementos de cada fila.*

Como los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$ anteriores son equivalentes, lo siguen siendo al añadir un bit de paridad. Por tanto, operaremos sólo con la matriz A_1. Al añadir el bit de paridad obtenemos la matriz

$$B_1 = \begin{pmatrix} 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 1 \end{pmatrix}$$

El polinomio de pesos es

$$1 + 264\,Y^6 + 440\,Y^9 + 24\,Y^{12}$$

en el que se ve que todas las palabras tienen peso múltiplo de 3. Al tener peso 6 el código, corrige errores de peso 2.

Teorema 10.3.6.– *El código de Golay binario $\mathcal{G}_{12}$ es autodual.*

Demostración: La comprobación es meramente calculística. Basta ver que $B_1 B_1^t = 0$. □

Reina Mercedes s.n. - 41012 Sevilla - Tlfno: +34 954 55 6946 - Fax: +34 954 55 6938 - http://www.us.es/da

UNIVERSIDAD DE SEVILLA