USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Estructura de las unidades en módulo m

Ángel Martínez González

Curso Académico 2019/2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Estructura de las unidades módulo m

Ángel Martínez González

07/2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Estructura de las unidades módulo m
Breve descrición do contido
Estudio de la estructura de las unidades en el anillo $\mathbb{Z}_m$ y su aplicación para la resolución de congruencias (mod m) y de ecuaciones en $\mathbb{Z}[x]$.
Recomendacións
Estudio previo de estructuras algébricas para algunas partes.
Outras observacións

Índice general

Resumen

Estudio de la estructura de los grupos de unidades en módulo $m \in \mathbb{Z}$, $m > 1$ arbitrario, denotado como $\mathbb{U}_m$, y trabajando con la definición del anillo $\mathbb{Z}_m$, dando su definición y propiedades de los elementos de este anillo y del grupo $\mathbb{U}_m$. Por otro lado, veremos también el teorema de Euler, el teorema de Fermat y el teorema de Wilson, resultados que nos serán útiles para probar las propiedades de los conjuntos anteriormente descritos. Esto nos ayudará a la resolución de congruencias de una variable (mod m) tanto lineales como de grado superior, analizando, además, sistemas de congruencias de distintos módulos. Para ello se verán, además, la definición de raíz primitiva de un m que las admita, recalcando la forma de aquellos números enteros que los tienen; así como la definición de índice, que nos ayudará a la hora de afrontar congruencias de forma $ax^n \equiv b \pmod{m}$. Usaremos también el teorema de Lagrange para ver cuantas soluciones posibles puede haber. Para finalizar, se explicarán formas de ver si un elemento de $\mathbb{U}_m$ es un resto cuadrático, centrándonos en especial en los módulos primos para definir el símbolo de Legendre, y partiendo del criterio de Euler.

Abstract

Study of the structure of the group of units modulo $m \in \mathbb{Z}$, $m > 1$ arbitrary, writing it as $\mathbb{U}_m$, and working with the definition of the ring $\mathbb{Z}_m$, explaining its definition and the properties of this ring and the $\mathbb{U}_m$ group. On the other hand, we will see Euler's theorem, Fermat's theorem and Wilson's theorem too; and these tools will be useful in order to proof the properties of the sets previously described. This will help us for solving linear congruences or higher-degree polinomial congruences in one variable (mod m), and we will also explain how to see a solution to a system of simultaneous linear congruences with different moduli. In order to help with this goal, we will see the definition of primitive root of a valid m, describing the way these integer numbers are; and the definition of index,

useful when we want to solve $ax^n \equiv b \pmod{m}$ congruences. We will see the Lagrange's theorem to see the possible number of solutions a congruence has. Finally, we will explain different modes for see if an element of $\mathbb{U}_m$ is a quadratic residue, placing an emphasis on prime integer moduli in order to define the Legendre symbol, and explaining also the Euler's criterion.

Introducción

El objetivo de este trabajo es el de proporcionar resultados completos sobre la estructura de los grupos de unidades en módulo m, para sus posteriores aplicaciones en el estudio de congruencias (en especial, lineales), raíces primitivas, índices y restos cuadráticos.

En el primer capítulo introduciremos los anillos $\mathbb{Z}_m$, con $m > 1$, $m \in \mathbb{Z}$, de los que se parte para describir después el grupo de unidades módulo m que está contenido. También se adelantan resultados importantes para el resto de apartados.

En el segundo se explicarán los elementos de $\mathbb{Z}_m$ que son unidades, incluyendo cuantos pueden ser y las propiedades que cumplen los elementos dentro del grupo. Daremos, también, la definición de orden.

El capítulo tres está dedicado a la solución de congruencias lineales de una variable, así como al estudio de sistemas de congruencias lineales con varios módulos. Se explicará, para este fin, el teorema chino de los restos y las propiedades necesarias para la resolución de sistemas de congruencias con módulos arbitrarios.

El cuarto se dedica a dar resultados de congruencias de grados mayores a 1 (congruencias no lineales), con atención especial a las de grado 2 y a los restos n-potenciales. A parte, se explicará el teorema de Lagrange.

El capítulo cinco habla de las raíces primitivas y de los números enteros que los pueden tener, añadiendo propiedades de los elementos del grupo de unidades y profundizando en la estructura del grupo a partir de la posibilidad de existencia o no existencia de raíces primitivas del módulo m.

En el sexto capítulos aplicaremos lo visto en el anterior para la resolución de congruencias. Para esto, introduciremos el índice a partir de una raíz primitiva del módulo m, así como el vector de índices para aquellos enteros que no tengan raíces primitivas. También veremos como construir tablas de índices y de vectores de índices y algunos resultados derivados de las propiedades de índices.

Para finalizar, los dos últimos capítulos se dedicarán a restos cuadráticos, definiendo este término y el símbolo de Legendre, que indicará si un elemento es resto cuadrático o no de un módulo primo, junto con sus propiedades. También se verá la ley de reciprocidad

cuadrática, que agilizará el estudio de si un elemento es o no resto cuadrático para un módulo primo. También veremos, de forma más abreviada, qué sucede en el caso de un módulo compuesto.

Capítulo 1

Congruencias. Teoremas de Euler, Fermat y Wilson.

Empezaremos con la definición de congruencia, así como algunas de sus propiedades. También daremos algunos resultados importantes que serán útiles para sucesivos capítulos.

1.1. Congruencias.

Definición 1.1. Sea $m \in \mathbb{Z}$, $m > 1$. Se dice que $a, b \in \mathbb{Z}$ son **congruentes módulo** m si m divide a la diferencia $a - b$ (denotando por $m \mid a - b$ la divisibilidad). Otras formas de definirlo son que $a - b = km$, con $k \in \mathbb{Z}$ (esta es equivalente a la definición ya dada); o que a y b están en la misma progresión aritmética de diferencia m. Se denotará la congruencia de a y b en módulo m como $a \equiv b \pmod{m}$.

Definición 1.2. Sea $a \in \mathbb{Z}$ fijado. Tenemos que los $x \in \mathbb{Z}$ que cumplen $x \equiv a \pmod{m}$ son de la forma $x = a + mk$, con $k \in \mathbb{Z}$. Esta progresión se denomina **clase de restos módulo** m. Conocido el módulo (sea m), lo denotamos por $\overline{a}$. También se puede denotar a la sucesión como $(a)_m$.

Las clases de restos (mod m) forman una partición de $\mathbb{Z}$. Esto se ve fácilmente gracias al siguiente resultado:

Teorema 1.3. *Sean $a, b \in \mathbb{Z}$ arbitrarios y fijemos $m \in \mathbb{Z}$. $a \equiv b \pmod{m} \Leftrightarrow a$ y b tienen el mismo resto no negativo al dividirlos por m.*

Demostración. Probamos las dos implicaciones:

"$\Rightarrow$"

Partimos de $a \equiv b \pmod{m}$. Esto implica que $a = b + mk$, para un $k \in \mathbb{Z}$. Por otro lado, dividiendo b por m, tenemos $b = qm + r$, para $q \in \mathbb{Z}$ y con $0 \leq r < m$. Por tanto, $a = b + km = r + qm + km = (q + k)m + r$. Así, a y b tienen el mismo resto r, lo que prueba esta implicación.

"$\Leftarrow$"

Sean $a = q_1 m + r$ y $b = q_2 m + r$, con $0 \leq r < m$ y $q_1, q_2 \in \mathbb{Z}$. Entonces $a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2)m$. Esto significa que $m \mid (a - b)$, pero esto equivale a que $a \equiv b \pmod{m}$. (1.1) □

Por tanto, con $m \in \mathbb{Z}$, $m > 1$ fijado, tenemos que las distintas clases de restos, $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$, forman una partición de $\mathbb{Z}$ y cada entero está en una única clase de restos. En general usaremos la nomenclatura sin la línea para referirnos a su clase de restos cuando no haya confusión.

Teorema 1.4. *Sean $m \in \mathbb{Z}$, $m > 1$ fijado. Congruencia (mod m) es una relación de equivalencia.*

Demostración. Siendo a, b, c enteros, tiene que cumplirse:

1.- $a \equiv a \pmod{m}$.

Cierto por $a - a = 0$ y todo número dividir a 0.

2.- $a \equiv b \Rightarrow b \equiv a$.

$a \equiv b \pmod{m} \Rightarrow a - b = km$, con $k \in \mathbb{Z}$. Así, $b - a = -(a - b) = -(km) = (-k)m$. $k \in \mathbb{Z} \Rightarrow -k \in \mathbb{Z}$, por lo que $b \equiv a \pmod{m}$.

3.- $\left.\begin{array}{l} a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{array}\right\} \Rightarrow a \equiv c \pmod{m}$

$a \equiv b \pmod{m} \Leftrightarrow a - b = km$, $k \in \mathbb{Z}$ y $b \equiv c \pmod{m} \Leftrightarrow b - c = qm$, $q \in \mathbb{Z}$
$a - c = (a - b) + (b - c) = km - qm = (k - q)m \Leftrightarrow a \equiv c \pmod{m}$.

□

Observación 1.5. La demostración anterior se basa en la propia definición de congruencia (1.1)

Partiendo entonces de que la congruencia es una relación de equivalencia, tenemos el siguiente resultado:

Teorema 1.6. *Sean a, b, c, d, $m \in \mathbb{Z}$, con $m > 1$. Se cumple:*

$$\left.\begin{array}{l} a \equiv b \ (mod\ m) \\ c \equiv d \ (mod\ m) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a + c \equiv b + d \ (mod\ m) \\ ac \equiv bd \ (mod\ m) \end{array}\right.$$

Definiendo suma y producto de clases de restos con las operaciones $\overline{a} + \overline{c} = \overline{a + c}$ y $\overline{a} \cdot \overline{c} = \overline{ac}$, entonces $\mathbb{Z}_m$ es un anillo y la aplicación definida como $\phi(a) = \overline{a}$ es homomorfismo de $\mathbb{Z}$ a $\mathbb{Z}_m$.

Demostración. Dividimos la demostración en cuatro partes:

- Suma y producto con congruencias

  $\left.\begin{array}{l} m \mid (a - b) \\ m \mid (c - d) \end{array}\right\} \Rightarrow m \mid ((a + c) - (b + d))$ da congruencia de suma.

  Para el producto, sabemos que $m \mid ((a - b)(c - d))$ al serlo de cada factor. Por ser $(a-b)(c-d) = ac - bd + b(d-c) + d(b-a)$ y los dos últimos sumandos son divisibles por m, entonces se cumple $m \mid (ac - bd)$ y tenemos congruencia para el producto.

- Clases de sumas y productos de clases de restos.

  $\overline{a} + \overline{c} = \overline{a + c}$ significa que la suma de clase de restos dada por a y c es la misma en la que está la suma $a + c$. Dicho de otro modo, si sumamos dos clases de restos (mod m), sean C y C' las clases, elegimos un elemento de cada uno, los sumamos, y definimos $C + C'$ como C'' clase con su suma. La suma es única si (y sólo si) los resultados de C'' se dan sin importar los elementos escogidos en C y C'. Como $\left.\begin{array}{l} a \equiv b \ (\text{mod } m) \\ c \equiv d \ (\text{mod } m) \end{array}\right\} \Rightarrow a + c \equiv b + d \ (\text{mod } m)$, siendo $a, b \in C$ y $c, d \in C' \Rightarrow a + c$, $b + d \in C''$. Para el producto tenemos un razonamiento análogo.

- $\mathbb{Z}_m$ es un anillo.

  Para $\mathbb{Z}_m$, muchas propiedades se heredan de $\mathbb{Z}$:

  - $a + b = b + a$ en $\mathbb{Z} \Rightarrow \overline{a} + \overline{b} = \overline{b} + \overline{a}$ en $\mathbb{Z}_m$
  - $a + 0 = a$ en $\mathbb{Z} \Rightarrow \overline{a} + \overline{0} = \overline{a}$ en $\mathbb{Z}_m$
  - $a \cdot 1 = a$ en $\mathbb{Z} \Rightarrow \overline{a} \cdot 1 = \overline{a}$ en $\mathbb{Z}_m$

  Sólo nos quedaría ver que $1 \neq 0$. Pero esto es cierto al ser $m > 1$ y $m \nmid 1$. Por tanto, $\mathbb{Z}_m$ es anillo. Notar que con estas operaciones, $\mathbb{Z}_m$ es cerrado.

- Homomorfismo entre $\mathbb{Z}$ y $\mathbb{Z}_m$.

  Por $\mathbb{Z}_m$ ser anillo (al heredar las propiedades de anillo de $\mathbb{Z}$), tenemos entonces que la aplicación

$$\begin{aligned} \phi\colon \mathbb{Z} &\longrightarrow \mathbb{Z}_m \\ a &\longmapsto \phi(a) = \overline{a} \end{aligned}$$

  es un homomorfismo de anillos entre $\mathbb{Z}$ y $\mathbb{Z}_m$

□

Además, gracias a este teorema, tenemos el siguiente resultado:

Corolario 1.7. $\left.\begin{array}{l} f(x_1, ..., x_n) \textit{ polinomio sobre } \mathbb{Z} \\ a_j \equiv b_j \textit{ (mod m), con } j \in \{1, ..., n\} \end{array}\right\} \Rightarrow$
$f(a_1, ..., a_n) \equiv f(b_1, ..., b_n)$ *(mod m).*

Observación 1.8. Llevado al álgebra actual, tenemos que el conjunto $m\mathbb{Z}$ de los múltiplos de m es un ideal, es decir, un grupo aditivo contenido en un anillo de modo que $ka \in m\mathbb{Z}$ $\Rightarrow k \in \mathbb{Z}$, $a \in m\mathbb{Z}$.

Con todo esto, podremos ver cuando una ecuación es resoluble en $\mathbb{Z}$. En el caso general, $f(x, y, ..., z) = 0$ resoluble en $\mathbb{Z}$ si lo es en $\mathbb{Z}_m$, con $m \in \mathbb{Z}^+$. Dicho de otro modo, no hay solución en $\mathbb{Z}$ si no hay solución en $\mathbb{Z}_m$ para algún $m \in \mathbb{Z}^+$. Para esto, observaremos ciertas propiedades que se deben cumplir para que haya solución de una ecuación en $\mathbb{Z}_m$.

Lo primero a decir es que $a \equiv b \pmod{m} \Rightarrow ca \equiv cb \pmod{m}$ $\forall c \in \mathbb{Z}$ ((1.6) con $c = d$). Sin embargo, la otra implicación no es cierta. Por ejemplo, $2{\cdot}3 \equiv 2{\cdot}0 \pmod 6$, pero no es cierto $3 \equiv 0 \pmod 6$. Tenemos, entonces, algunas condiciones para cancelar factores.

Teorema 1.9. *Sean $m \in \mathbb{Z}$, $m > 1$, $0 \neq k \in \mathbb{Z}$ y mcd(k, m)= d.*
Entonces $ka \equiv kb$ (mod m) $\Rightarrow a \equiv b$ (mod $\frac{m}{d}$).

Demostración. $\text{mcd}(k, m) = d \Leftrightarrow \text{mcd}((\frac{k}{d}), (\frac{m}{d})) = 1$. Por $ka \equiv kb \pmod m$, $m \mid (ka - kb)$ $\Leftrightarrow m \mid k(a - b) \Leftrightarrow \frac{m}{d} \mid \frac{k}{d}(a - b)$, y esto nos da el resultado deseado por (1.1). □

De este resultado obtenemos dos resultados muy importantes. Suponiendo $k, n, p \in \mathbb{Z}$:

Corolario 1.10. $\left.\begin{array}{l} ka \equiv kb \textit{ (mod m)} \\ \textit{mcd(k, m)= 1} \end{array}\right\} \Rightarrow a \equiv b \textit{ (mod m).}$

Corolario 1.11. $\left.\begin{array}{l} ka \equiv kb \textit{ (mod p)} \\ p \nmid k, \textit{ p primo} \end{array}\right\} \Rightarrow a \equiv b \textit{ (mod p).}$

Combinando ambos corolarios, tenemos que $p \in \mathbb{Z}$, p primo, entonces $ab \equiv 0 \pmod{p}$ $\Rightarrow a \equiv 0$ o $b \equiv 0$, cosa que, como hemos visto antes, no se da en general. Con esto, llegamos al siguiente teorema:

Teorema 1.12. *Para un $m \in \mathbb{Z}^+$, m compuesto, $\mathbb{Z}_m$ anillo no dominio, es decir, existen elementos distintos de 0 cuyo producto es 0 (por lo visto arriba). Si $p \in \mathbb{Z}$ es primo, $\mathbb{Z}_p$ es un cuerpo, es decir, todo elemento salvo el $\overline{0}$ es invertible.*

Demostración. Sólo probaremos que $\mathbb{Z}_p$ con p primo es cuerpo.

$\forall 0 \neq a \in \mathbb{Z}_p$ es invertible. Siendo así, tenemos que $ax = 1$ solución única en $\mathbb{Z}_p$. Esto equivale a $ax = 1 + py$ en $\mathbb{Z}$. $0 \neq a \in \mathbb{Z}_p$ implica que $p \nmid a$, por lo que esta ecuación se resuelve y el conjunto de x válidos están en una clase de restos (mod p). □

Así, será importante saber cuáles enteros son números primos. Antes de seguir con el siguiente capítulo, daremos unos resultados que serán importantes para ver qué valores enteros son primos y algunas propiedades que se utilizarán en otros capítulos.

1.2. Teoremas de Euler, de Fermat y de Wilson.

Comenzaremos hablando del **Pequeño teorema de Fermat**, y de resultados que parten de este teorema. Primero daremos la definición de sistema completo de restos.

Definición 1.13. Sea $m \in \mathbb{Z}^+$. Un **sistema completo de restos** (mod m) es un conjunto de enteros con las siguientes propiedades:

1.- Es un conjunto con m elementos, que denotaremos $\{a_1, ..., a_m\}$.

2.- Estos elementos son enteros incongruentes (mod m). Dicho de otro modo,

$a_i \equiv a_j \pmod{m} \Rightarrow i = j$.

3.- Cada clase (mod m) está representada una única vez. Es decir, $\forall a \in \mathbb{Z}$, $\exists^o a_i$, elemento del sistema, de modo que $a_i \equiv a \pmod{m}$.

Sea el sistema completo de restos definido anteriormente, y sean b, $k \in \mathbb{Z}$, siendo m y k coprimos, entonces $ka_1 + b$, ..., $ka_m + b$ forman un sistema de restos completo (mod m), y esto da una permutación de los elementos de a_1, ..., a_m.

Ejemplo 1.14. Tomemos $m = 5$. Un sistema completo de restos (mod 5) es el conjunto $\{0, 1, 2, 3, 4\}$. Otro sistema de restos completo (mod 5) sería $\{2, 4, 6, 8, 10\}$. En efecto, pues $2 \equiv 2$, $4 \equiv 4$, $6 \equiv 1$, $8 \equiv 3$, $10 \equiv 0 \pmod{5}$. Por otro lado, $\{2, 4, -6, 8, 10\}$ no es un sistema de restos completo, pues $-6 \equiv 4 \pmod{5}$.

Teniendo esta definición, podemos ver ahora el teorema de Fermat.

Teorema 1.15 (Pequeño teorema de Fermat)**.** *Sean a, $p \in \mathbb{Z}^+$, con p primo y $p \nmid a$. Entonces $a^{p-1} \equiv 1$ (mod p).*

Demostración. Tomamos los primeros $p-1$ múltiplos de a (a, $2a$,...,$(p-1)a$). Ninguno es congruente a 0 ni lo son dos a dos (pues si $1 \leq r < s \leq p-1$, en $ra \equiv sa \pmod{p}$ se puede cancelar a (1.11) y tenemos $r \equiv s \pmod{p}$, lo que es imposible). De este modo, el conjunto de múltiplos (con el $0 = 0 \cdot a$) es un sistema de restos completo, es decir, esos múltiplos son congruentes (mod p) a uno y sólo uno de los restos 1, 2, ..., $p-1$. Tenemos entonces el siguiente resultado es cierto (1.6): $a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$. Operando, tenemos que $a^{p-1}(p-1)! \equiv (p-1)!$, o lo que es lo mismo, por cumplirse $p \nmid (p-1)!$, $a^{p-1} \equiv 1 \pmod{p}$. □

Un resultado inmediato de este teorema, extendiendo la definición $\forall a \in \mathbb{Z}$, y $p \in \mathbb{Z}$ primo, es que $a^p \equiv a \pmod{p}$. Además, tenemos una generalización $\forall m \in \mathbb{Z}$ módulo, dada por Euler.

Teorema 1.16 (Teorema de Euler)**.** *Sean a, $m \in \mathbb{Z}$. Si mcd(a, m)= 1, entonces $a^{\varphi(m)} \equiv 1$ (mod m), donde $\varphi(m)$ denota la cantidad de números enteros positivos menores a m y que son coprimos con m.*

Demostración. Por definición de $\varphi(m)$, tomamos a_1, ..., $a_{\varphi(m)}$ que cumplen las condiciones descritas en el teorema. Por (1.10), tenemos que aa_1, ..., $aa_{\varphi(m)}$ son congruentes (mod m) en algún orden a a_1, ..., $a_{\varphi(m)}$. Multiplicando las congruencias, tenemos $(aa_1) \cdot \ldots \cdot (aa_{\varphi(m)}) \equiv a_1 \cdot \ldots \cdot a_{\varphi(m)} \pmod{m} \Leftrightarrow a^{\varphi(m)} \cdot a_1 \cdot \ldots \cdot a_{\varphi(m)} \equiv a_1 \cdot \ldots \cdot a_{\varphi(m)} \pmod{m}$. Como los distintos a_i son coprimos a m, su producto lo es, por lo que tenemos $a^{\varphi(m)} \equiv 1 \pmod{m}$, y se prueba el teorema. □

Observación 1.17. La función $\varphi(m)$ de (1.16) se denomina **función φ de Euler**. Profundizaremos más sobre esta función en el siguiente capítulo.

Otro resultado importante con el nombre de Euler es el **criterio de Euler**, utilizado para ver restos cuadráticos de un módulo primo. Lo analizaremos en otro capítulo. Lo que sí veremos ahora, y que será utilizado para el resultado citado, es el **teorema de Wilson**.

Teorema 1.18 (de Wilson)**.** *Sea $p \in \mathbb{Z}$ primo. Entonces $(p-1)! \equiv -1$ (mod p).*

Demostración. Si p es 2 o 3, esto es evidente, pues $1! = 1 \equiv -1 \pmod{2}$, $2! = 2 \equiv -1 \pmod{3}$.

Sea $p > 3$ primo y sea a uno de los enteros positivos 1, ..., $(p-1)$. Por ser p primo, (1.12) nos dice que todos esos elementos, al ser distintos de 0, tienen un único inverso en $\mathbb{Z}_p$. Llamemos a' al inverso de a.

Por p primo, tenemos $a = a' \Leftrightarrow a$ es 1 o $p-1$, pues $a \equiv 1 \pmod{p} \Leftrightarrow (a+1)\cdot(a-1) \equiv 0 \pmod{p}$, por lo que $a-1 \equiv 0 \pmod{p}$ y $a = 1$ o $a+1 \equiv 0 \pmod{p}$ y $a \equiv -1 \pmod{p}$, por lo que $a = p-1$.

Omitiendo estos elementos, los restantes 2, ..., $p-2$ se ordenan en pares de elementos distintos a, a' de modo que $aa' \equiv 1 \pmod{p}$. Tenemos $\frac{p-3}{2}$ congruencias. Al hacer su producto, y reordenando, se cumple que $2\cdot\ldots\cdot(p-2) \equiv 1 \pmod{p}$, es decir, $(p-2)! \equiv 1 \pmod{p}$. Por tanto, multiplicando por $p-1$, tenemos $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. $\square$

Con esto, tenemos casi todas las herramientas básicas necesarias para los siguientes capítulos.

Capítulo 2

Estructura unidades (mod m).

En este capítulo veremos como es la estructura de las unidades en los anillos $\mathbb{Z}_m$, con $m \in \mathbb{Z}^+$ arbitrario. Antes de profundizar en esto, hablaremos de la función φ de Euler y veremos sus propiedades, que serán útiles tanto en este como en siguientes capítulos.

2.1. La función φ de Euler.

Definición 2.1. Sea $m \in \mathbb{Z}$, $m > 0$. Se denota por $\varphi(m)$ a la cantidad de números enteros positivos menores o iguales a m y coprimos con m. Esta función se denomina **función φ de Euler**.

Tenemos que $\varphi(1) = 1$, pues mcd(1, 1)= 1. Si $m > 1$, mcd(m, m)= $m \neq 1$. Por tanto, si tomamos $m > 1$, $\varphi(m)$ es la cantidad de números enteros positivos menores a m y coprimos con m.

Ejemplo 2.2. Veremos el valor de $\varphi(m)$ en un par de casos.

1.- Para el número $9 = 3^2$, tenemos que los números coprimos menores que 9 son $\{1, 2, 4, 5, 7, 8\}$. Un total de 6 elementos. Por tanto, $\varphi(9) = 6$

2.- Para el número $12 = 2^2 \cdot 3$, tenemos que los números coprimos menores a 12 son $\{1, 5, 7, 11\}$. Un total de 4 elementos. Por tanto, $\varphi(12) = 4$.

Si $m \in \mathbb{Z}$ es un número primo, tenemos que $\forall a \in \mathbb{Z}$, con $a < m$, mcd(a, m)= 1, por lo que $\varphi(m) = m - 1$. Con m compuesto, la cosa cambia. Sea $d \in \mathbb{Z}$ un divisor de m, por lo que $1 < d < m$. Por ello, hay al menos dos números enteros entre 1, 2, ..., m no coprimos con m, que serán al menos d y m. Por tanto, $\varphi(m) \leq m - 2$.

Teniendo una acotación de la función φ de Euler, vamos a ver como saber que valor tiene $\varphi(m)$ dependiendo de $m \in \mathbb{Z}$.

Teorema 2.3. *Sea $p \in \mathbb{Z}$, con p primo y $k \in \mathbb{Z}^+$. Entonces, $\varphi(p^k) = p^k - p^{k-1} = p^k(1-\frac{1}{p})$.*

Demostración. Sea $n \in \mathbb{Z}$. $p \nmid n \Leftrightarrow \text{mcd}(n, p^k) = 1$. Tenemos p^{k-1} números enteros entre 1 y p^k divisibles por p, que serán p, $2p$, ..., $(p^{k-1})p$. Por tanto, hay $p^k - p^{k-1}$ números enteros coprimos a p^k entre 1 y p^k. Por la definición de función de φ de Euler, entonces $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. □

Con esto, ya tenemos el valor de $\varphi(m)$ para $m \in \mathbb{Z}$ primo o potencia de primo.

Para un m arbitrario, tenemos que recurrir a la propiedad multiplicativa de la función φ de Euler.

Definición 2.4. Una función arbitraria f se dice que es **multiplicativa** si $f(mn) = f(m)f(n)$ cuando mcd(m,n)= 1.

Lema 2.5. *Sean a, b, $c \in \mathbb{Z}$. mcd(a, bc)= 1* $\Leftrightarrow \begin{cases} \text{mcd}(a,\ b) = 1 \\ \text{mcd}(a,\ c) = 1 \end{cases}$

Demostración. Probaremos las dos implicaciones:

"$\Rightarrow$"

Partimos de mcd(a, bc)= 1 y sea d =mcd(a,b) $\Rightarrow d \mid a$ y $d \mid b \Rightarrow d \mid a$, $d \mid bc \Rightarrow$ mcd$(a, bc) \geq d \Rightarrow d = 1$. Esto es análogo para mcd(a, c)= 1.

"$\Leftarrow$"

Partimos de mcd(a,b)= 1 =mcd(a,c). Sea mcd(a,bc)= $d_1 > 1$. d_1 tiene un divisor primo $p > 1$. $d_1 \mid bc \Rightarrow p \mid bc \Rightarrow p \mid b$ o $p \mid c$. Si $p \mid b$, como $p \mid a$, entonces mcd(a, b)$\geq p$, lo que es una contradicción. Análogo si $p \mid c$. Por tanto, solo queda que $d_1 = 1$. □

Teorema 2.6. *La función φ de Euler es multiplicativa.*

Demostración. $\varphi(1) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ es válido con m, $n = 1$.

Sean, pues, m, $n > 1$, y suponemos mcd(m, n)= 1. Consideramos:

$$\begin{array}{cccc} 0 & 1 & ... & m-1 \\ m & m+1 & ... & m+(m-1) \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ (n-1)m & (n-1)m+1 & ... & (n-1)m+(m-1) \end{array}$$

Tenemos que son mn enteros seguidos, por lo que son un sistema completo de restos (mod mn), y habrá $\varphi(mn)$ números coprimos con el número mn en la lista.

La primera fila es un sistema completo de restos (mod m), y todos los elementos de cada columna son congruentes (mod m), por lo que tenemos $\varphi(m)$ columnas con elementos coprimos con m.

Tomemos, ahora, una de estas columnas. Sus elementos son b, $m+b$, ..., $(n-1)m+b$, con $b \in \mathbb{Z}$, $0 \leq b < m$. Por (1.13), esto es un sistema completo de restos (mod n). Por ello, cada una de estas columnas tiene un total de $\varphi(n)$ elementos coprimos con n.

Por tanto, llegamos a que hay $\varphi(m)\varphi(n)$ elementos coprimos con m y n en el listado descrito. Como mcd(m, n)= 1, entonces $l \in \mathbb{Z}$ coprimo con $mn \Leftrightarrow l$ coprimo con m y n (2.5). Así, hay $\varphi(m)\varphi(n)$ elementos de la lista coprimos con mn. Por lo tanto, $\varphi(mn) = \varphi(m)\varphi(n)$. □

Con estas herramientas, tenemos entonces la forma de calcular $\varphi(m)$ $\forall m \in \mathbb{Z}$, tal como se muestra en el siguiente resultado.

Teorema 2.7. *Sea $m \in \mathbb{Z}$ con descomposición en primos $m = p_1^{e_1} ... \ p_r^{e_r}$, donde los p_i son primos distintos $\forall i \neq j$, y los e_i son enteros mayores o iguales a 0. Entonces, $\varphi(m) = \varphi(p_1^{e_1})...\varphi(p_r^{e_r}) = m(1-\frac{1}{p_1})...(1-\frac{1}{p_r})$.*

Demostración. Por inducción en r, número de primos distintos en los que se descompone m. Con $r = 1$ lo sabemos cierto (2.3). Lo suponemos válido para $r = i$. Como mcd($p_1^{e_1}...p_i^{e_i}$, $p_{i+1}^{e_{i+1}}$)= 1 (por ser primos distintos), y por ser φ de Euler multiplicativa, tenemos que $\varphi(m) = \varphi((p_1^{e_1}...p_i^{e_i})p_{i+1}^{e_{i+1}}) = \varphi(p_1^{e_1}...p_i^{e_i})\varphi(p_{i+1}^{e_{i+1}})$. Por hipótesis de inducción, sabemos que $\varphi((p_1^{e_1}...p_i^{e_i}) = \varphi(p_1^{e_1})... \ \varphi(p_i^{e_i})$, y por (2.3) en cada factor, tenemos el resultado deseado. □

Otro resultado importante sobre la función φ de Euler es el siguiente:

Teorema 2.8. *Sean d, $m \in \mathbb{Z}$ y $m > 0$. Entonces $\sum_{d|m} \varphi(d) = m$.*

Demostración. Es un caso especial del principio de cardinalidad de subgrupos de un grupo finito. Este resultado de teoría de grupos nos dice que un subgrupo de un grupo finito tiene un cardinal que es divisor del cardinal del grupo en el que está, y además la suma de cardinales de subgrupos que forman una partición del grupo tiene que ser el cardinal del propio grupo. En este caso, el conjunto se denomina $S = \{1, ..., m\}$, y las distintas clases se denotan como C_d, con $d \mid m$, siendo los elementos $a \in S$ de modo que se cumple mcd(a, m)= d. Reescribimos cada $a \in S$ de forma $a = bd$ (pues mcd(a, m)= d). De este modo, tenemos $1 \leq b \leq \frac{m}{d}$, siendo b y $\frac{m}{d}$ coprimos. La cantidad de b válidos es $\varphi(\frac{m}{d})$, y como d recorre los divisores de m, también recorre $\frac{m}{d}$, en orden inverso. Por tanto, $\sum_{d|m} \varphi(\frac{m}{d}) = \sum_{d|m} \varphi(d)$. □

Ejemplo 2.9. Tomando $m = 20 = 2^2 \cdot 5$. Sus divisores serán $\{1, 2, 4, 5, 10, 20\}$. Tenemos, entonces, que sumar φ de estos elementos. $\varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) = 1 + 1 + 2 + 4 + 4 + 8 = 20$.

Con esto, ya tenemos las herramientas necesarias para hablar de unidades en módulo m, con $m \in \mathbb{Z}$.

2.2. Estructura de unidades (mod m).

Sea $m \in \mathbb{Z}$. Tenemos que $\mathbb{Z}_m$ es un **grupo aditivo finito**, y es un grupo **cíclico**, es decir, se genera con un único elemento (en este caso, el 1). Por otro lado, si m es un número primo, el grupo multiplicativo $\mathbb{Z}_m^*$ de los elementos de $\mathbb{Z}_m$ distintos de 0 es cíclico. En caso de que m sea compuesto, entonces $\mathbb{Z}_m^*$ no es grupo, pero contiene un subconjunto importante que sí es grupo: el conjunto de las unidades de $\mathbb{Z}_m$.

Definición 2.10. Llamamos **grupo de unidades de** $\mathbb{Z}_m$ a los elementos de $\mathbb{Z}_m$ que tienen inverso. El elemento $u \in \mathbb{Z}_m$ es una unidad si, y sólo si, cumple una de estas condiciones (equivalentes):

- $ux = 1$ resoluble en $\mathbb{Z}_m$
- $ux \equiv 1 \pmod{m}$ resoluble
- $ux + my = 1$

De las dos primeras condiciones hablaremos en próximos capítulos. La tercera es equivalente a la condición de que mcd(u, m)= 1, es decir, las unidades de $\mathbb{Z}_m$ serán los elementos de este grupo que son coprimos con m. Denotamos al conjunto de unidades como $\mathbb{U}_m$, y, por lo visto antes, este grupo tendrá $\varphi(m)$ elementos.

Ejemplo 2.11. Volviendo a los casos vistos en (2.2), los elementos coprimos de 9 y 12 son los que están en esos conjuntos descritos; $\{1, 2, 4, 5, 7, 8\}$ y $\{1, 5, 7, 11\}$, respectivamente.

Proposición 2.12. *El conjunto $\mathbb{U}_m$ es un grupo multiplicativo, independientemente del anillo $\mathbb{Z}_m$ del que provenga.*

Demostración. Sea $m \in \mathbb{Z}$, $m > 1$. Por definición de grupo, tenemos que $\mathbb{U}_m$ grupo si cumple:

- $\forall x, y, z \in \mathbb{U}_m$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\exists e \in \mathbb{U}_m$ elemento neutro ($\forall x \in \mathbb{U}_m$, $e \cdot x = x = x \cdot e$).

- $\forall x \in \mathbb{U}_m \ \exists x^{-1} \in \mathbb{U}_m$ elemento simétrico de x ($x \cdot x^{-1} = e = x^{-1} \cdot x$, e elemento neutro).

Sea $u \in \mathbb{U}_m$. Por definición, tenemos que $\exists x \in \mathbb{U}_m / ux \equiv 1 \pmod{m}$. Pero esto equivale a $x \equiv u^{-1} \pmod{m}$. Por u arbitrario, entonces todo elemento tiene simétrico por definición.

Para elemento neutro, $\mathbb{U}_m \subset \mathbb{Z}_m$. $1 \in \mathbb{Z}_m$ elemento neutro para el producto en $\mathbb{Z}_m$. Por otro lado, $u \in \mathbb{U}_m \subset \mathbb{Z}_m$. Como mcd(1, m)= 1, tenemos $u \cdot 1 = u = 1 \cdot u$, siendo el mismo producto que en $\mathbb{Z}_m$.

Falta ver que es asociativa. x, y, $z \in \mathbb{U}_m$ implica que mcd(x, m)= 1, mcd (y, m)= 1 y mcd(z, m)= 1. Entonces, (xy, m)= 1 y (yz, m)= 1, por lo que xy, $yz \in \mathbb{U}_m$. Operando en $\mathbb{Z}_m$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ se cumple. Todos los elementos están en $\mathbb{U}_m$. Por tanto, se cumple en $\mathbb{U}_m$.

Por lo tanto, $\mathbb{U}_m$ grupo multiplicativo.

□

Tenemos entonces que el conjunto de las unidades (mod m) es un grupo multiplicativo. Veamos ahora algunas propiedades de los elementos de este grupo.

Definición 2.13. Se denomina **sistema de restos reducido (mod m)** a un conjunto de elementos de $\mathbb{Z}$ que representan los elementos del grupo $\mathbb{U}_m$. Cumple las siguientes propiedades:

a) Hay $\varphi(m)$ elementos, a_1, ..., $a_{\varphi(m)}$ coprimos con m.

b) Son enteros incongruentes (mod m).

c) $\forall a \in \mathbb{Z}$ coprimo con m, $\exists a_i \in \mathbb{Z}_m$ único de modo que $a_i \equiv a \pmod{m}$.

Además, teniendo un sistema de restos reducido (mod m), y siendo $k \in \mathbb{Z}$, k coprimo con m, entonces ka_1, ..., $ka_{\varphi(m)}$ también es sistema de restos reducido.

Definición 2.14. Sea $a \in \mathbb{U}_m$. Entonces a genera un subgrupo cíclico de $\mathbb{U}_m$ (o el propio $\mathbb{U}_m$), que son las potencias de a. Este subgrupo se denota por $< a >$, es finito y contiene a 1. Si $a^h \equiv 1 \pmod{m}$, siendo h el menor entero positivo (no siendo el 0) que cumple esto, entonces los elementos $\{a, a^2, ..., a^h\}$ son distintos y las potencias de a son iguales a uno de esos elementos. (Lo probaremos en próximos capítulos).

Definición 2.15. Sea $a \in \mathbb{U}_m$ y h es el menor entero positivo distinto a 0 de forma que $a^h \equiv 1 \pmod{m}$. Entonces, el subgrupo de $\mathbb{U}_m$ generado por estas potencias de a tiene exactamente h elementos. Llamamos a h **orden de a (mod m)**, y lo denotamos como $ord_m\ a$. Es el propio orden de $< a >$.

Ejemplo 2.16. Tomando $m = 11$, al ser primo, tenemos que $\mathbb{U}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Un generador del grupo es el elemento 2. $< 2 >= \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$, que es $\mathbb{U}_{11}$. Su orden (mod 11) es 10. Por otro lado, 4 no es generador de $\mathbb{U}_{11}$, pues $< 4 >= \{4, 5, 9, 3, 1\}$, que no es $\mathbb{U}_{11}$ completamente. En este caso, tenemos que su orden (mod 11) es 5.

El orden de a (mod m) esta relacionado con $\varphi(m)$ por el **teorema de Euler** (1.16), que nos dice que $a^{\varphi(m)} \equiv 1 \pmod{m}$ siempre que mcd(a, m)= 1, algo similar a lo que sucede con el orden de $a \in \mathbb{U}_m$. Tenemos lo siguiente:

Teorema 2.17. *mcd(a, m)=1* $\Rightarrow$ $ord_m\ a \mid \varphi(m)$.

Demostración. Por definición, $t = ord_m\ a$ es el entero positivo distinto de 0 menor que cumple $a^t \equiv 1 \pmod{m}$. Por otro lado, $\varphi(m) = tq + r$, $0 \leq r < t$, por lo que $1 \equiv a^{\varphi(m)} \equiv a^{tq+r} \equiv a^r \pmod{m}$. Así, $r = 0$ y $t \mid \varphi(m)$. □

Este último resultado nos dice que el orden de todo elemento $a \in \mathbb{U}_m$ es divisible por $\varphi(m)$. Esto tiene sentido hablando en base a teoría de grupos, pues $\varphi(m)$ es el cardinal de $\mathbb{U}_m$, por lo que el orden de todo subgrupo contenido en $\mathbb{U}_m$ tiene un cardinal que divide al cardinal del grupo. De hecho, esto es válido con cualquier entero positivo k de modo que $a^k \equiv 1 \pmod{m}$. Lo vemos en el siguiente resultado.

Teorema 2.18. *Sea* $a \in \mathbb{U}_m$, $ord_m\ a = t$. *Entonces* $a^n \equiv 1$ *(mod m)* $\Leftrightarrow$ $t \mid n$.

Demostración. Probamos ambas implicaciones:

"$\Leftarrow$"

Partimos de $t \mid n$, por lo que, para $j \in \mathbb{Z}$, $n = jt$. Como $a^t \equiv 1 \pmod{m}$, tenemos que $(a^t)^j \equiv 1^j \pmod{m}$, o lo que es lo mismo, $a^n \equiv 1 \pmod{m}$.

"$\Rightarrow$"

$n \in \mathbb{Z}^+ / \ a^n \equiv 1 \pmod{m}$. Por el algoritmo de división, $\exists q, r /\ n = qt + r$, con $0 \leq r < t$. Así, $a^n = a^{qt+r} = (a^t)^q a^r$. Por hipótesis, $a^n \equiv 1 \pmod{m}$ y $a^t \equiv 1 \pmod{m}$, por lo que $a^r \equiv 1 \pmod{m}$. Por $0 \leq r < t$, tenemos que $r = 0$, pues de no ser así, t no sería $ord_m\ a$, pues $r < t$. Por tanto, $n = qt$, y $t \mid n$. □

Veremos ahora un par de resultados interesantes en cuanto al orden de los elementos de $\mathbb{U}_m$, que nos serán útiles en el futuro.

Proposición 2.19. *Sean* $a, b, m \in \mathbb{Z}$, $m > 1$. *Entonces, si* $ab \equiv 1$ *(mod m) se cumple* $ord_m\ a = ord_m\ b$.

Demostración. Sean $ord_m\ a = h_1$ y $ord_m\ b = h_2$. Por definición de orden, tenemos que h_1 y h_2 son los menores enteros positivos de modo que $a^{h_1} \equiv 1 \pmod{m}$ y $b^{h_2} \equiv 1 \pmod{m}$.

En base a esto, tenemos: $ab \equiv 1 \pmod{m} \Rightarrow \left\{ \begin{array}{l} 1 \equiv (ab)^{h_1} \equiv a^{h_1} b^{h_1} \equiv b^{h_1} \pmod{m} \\ 1 \equiv (ab)^{h_2} \equiv a^{h_2} b^{h_2} \equiv a^{h_2} \pmod{m} \end{array} \right.$

$\left\{ \begin{array}{l} a^{h_1} \equiv 1 \equiv a^{h_2} \pmod{m} \text{ y } ord_m\ a = h_1 \Rightarrow h_1 \mid h_2 \\ b^{h_1} \equiv 1 \equiv b^{h_2} \pmod{m} \text{ y } ord_m\ b = h_2 \Rightarrow h_2 \mid h_1 \end{array} \right\}$

$\Rightarrow ord_m\ a = h_1 = h_2 = ord_m\ b.$ □

Proposición 2.20. $\left. \begin{array}{l} m \in \mathbb{Z},\ m > 1 \text{ } impar \\ ord_m\ a = 2t \end{array} \right\} \Rightarrow a^t \equiv -1 \text{ } (mod\ m).$

Demostración. $ord_m\ a = 2t \Rightarrow a^{2t} \equiv 1 \pmod{m} \Rightarrow (a^t)^2 \equiv 1 \pmod{m}$.

Por esto, tenemos que, o bien $a^t \equiv 1 \pmod{m}$, o bien $a^t \equiv -1 \pmod{m}$. Si estamos en el primer caso, al ser $t < 2t$ si $t \geq 1$. Por definición de orden, tenemos que $ord_m\ a \neq 2t$, pues tendríamos un entero positivo menor con el que a^t es congruente con 1 (mod m). Por tanto, tenemos que $a^t \equiv -1 \pmod{m}$. □

Observación 2.21. La proposición anterior no es válida si m es par.

Tomando $3 \in \mathbb{Z}_8$, tenemos que $3^2 = 9 \equiv 1 \pmod{8}$, pero 3 no es congruente con -1 (mod 8), pues $3 - (-1) = 3 + 1 = 4$, y $8 \nmid 4$.

Con esto, tenemos ya la definición del grupo de las unidades de $\mathbb{Z}_m$, (denominado $\mathbb{U}_m$), así como algunas propiedades de sus elementos y las órdenes de éstos. Estos resultados serán utilizados en posteriores capítulos, principalmente para hablar de raíces primitivas de un número $m \in \mathbb{Z}$, $m > 1$. Un elemento $a \in \mathbb{U}_m$ se dice que es raíz primitiva de m si su orden es el mismo que el del grupo de unidades $\mathbb{U}_m$, dicho de otro modo, si ese grupo de unidades se genera a partir de un elemento. Profundizaremos en esto en próximos capítulos.

Capítulo 3

Congruencias lineales.

En este capítulo estudiaremos las congruencias lineales para un módulo arbitrario, centrándonos sobre todo en la resolución de sistemas de congruencias de distintos módulos, con una variable, tanto siendo módulos coprimos dos a dos (en donde veremos el teorema chino de los restos), como con módulos arbitrarios.

Definición 3.1. En el primer capítulo, adelantamos en (1.7) que los elementos $x \in \mathbb{Z}$ que cumplen $f(x) \equiv 0 \pmod{m}$ ($m \in \mathbb{Z}$, $m > 1$) son los elementos de una clase de restos (mod m). Definimos en este caso **congruencia** como una ecuación en $\mathbb{Z}_m$. Tener en cuenta que el número de soluciones de $f(x) \equiv 0 \pmod{m}$ son las soluciones de $f(x) \equiv 0$ en $\mathbb{Z}_m$ (soluciones incongruentes en $\mathbb{Z}_m$).

3.1. Congruencias lineales. Definición y propiedades.

Partiendo de esto para una congruencia de grado arbitrario, nos centramos ahora en congruencias de grado 1.

Definición 3.2. Sea $m \in \mathbb{Z}$, $m > 1$. Se denomina **congruencia lineal** a una congruencia de grado 1, es decir, una congruencia $f(x) \equiv 0 \pmod{m}$ de forma que la congruencia se escribe de modo $ax \equiv b \pmod{m}$, $a, b \in \mathbb{Z}_m$.

Visto esto, tenemos que ver cuando una congruencia lineal es resoluble, pues partiendo de que en $\mathbb{Z}[x]$ no toda congruencia lineal es resoluble en $\mathbb{Z}$ (el anillo $\mathbb{Z}$ no tiene números racionales).

Teorema 3.3. *Sean a, b, $m \in \mathbb{Z}$, $m > 1$. $ax \equiv b \pmod{m}$ es resoluble $\Leftrightarrow d \mid b$, siendo $d = mcd(a, m)$. Además, $d \mid b \Rightarrow$ Existen d soluciones incongruentes (mod m).*

Demostración. Partiendo $ax \equiv b \pmod{m}$, esto es lo mismo que decir $ax - my = b$. Al ser una ecuación diofántica, esta es resoluble si, y sólo si, $d \mid b$, siendo $\text{mcd}(a, m) = d$. Por este motivo, partiendo de una solución x_0, y_0, otra solución será de forma $x = x_0 + t\frac{m}{d}$, $y = y_0 + t\frac{a}{d}$, siendo $t \in \mathbb{Z}$.

Veamos ahora que tenemos d soluciones distintas. Entre los distintos enteros que cumplen $x = x_0 + t\frac{m}{d}$, veamos qué sucede con $t = 0, 1, ..., d-1$. Tenemos los valores x_0, $x_0 + \frac{m}{d}$, ..., $x_0 + \frac{(d-1)m}{d}$, que son incongruentes (mod m) (pues forman un sistema completo de restos), y el resto de enteros son congruentes a uno de estos. En efecto. Supongamos que $\exists t_1, t_2 \in \mathbb{Z}$, $0 \leq t_1 < t_2 \leq d-1$ de modo que $x_0 + t_1\frac{m}{d} \equiv x_0 + t_2\frac{m}{d} \pmod{m}$. Entonces, tenemos $t_1\frac{m}{d} \equiv t_2\frac{m}{d} \pmod{m}$. Por tanto, como $\text{mcd}(\frac{m}{d}, m) = \frac{m}{d}$, tenemos que $t_1 \equiv t_2 \pmod{d}$, lo que nos dice que $d \mid t_2 - t_1$, cosa imposible por $0 < t_2 - t_1 < d$. Por ello, los valores anteriormente descritos son incongruentes entre sí y toda solución de forma $x_0 + t\frac{m}{d}$ es congruente a uno de estos enteros. Además, hay d soluciones. Por algoritmo de división, tomamos $t = qd + r$, $0 \leq r \leq d-1$.

Así, $x_0 + t\frac{m}{d} = x_0 + (qd+r)\frac{m}{d} = x_0 + mq + \frac{nr}{d} \equiv x_0 + r\frac{m}{d} \pmod{m}$, por lo que $x_0 + r\frac{m}{d}$ es solución. Como hay d valores posibles de r, tenemos d soluciones distintas. □

Un resultado inmediato de este teorema es que si $\text{mcd}(a, m) = 1$, entonces la congruencia $ax \equiv b \pmod{m}$ tiene una única solución (mod m). Esa solución, de hecho, será el inverso del elemento $a \in \mathbb{Z}_m$ en caso de que $b \equiv 1 \pmod{m}$.

Ejemplo 3.4. Veremos algunos ejemplos de congruencias con distinto número de soluciones.

1.- La congruencia $3x \equiv 4 \pmod{7}$ tiene una solución. En efecto, pues $\text{mcd}(3, 7) = 1$, y tenemos que la solución es $x \equiv 4 \cdot 3^{-1} \pmod{7}$, es decir, $x \equiv 6 \pmod{7}$ es la solución única de esta congruencia.

2.- La congruencia $15x \equiv 21 \pmod{33}$ tiene 3 soluciones. En efecto, como $\text{mcd}(15, 33) = 3$, tenemos entonces que la congruencia descrita equivale a la congruencia $5x \equiv 7 \pmod{11}$. Esta congruencia tiene una única solución al ser $\text{mcd}(5, 11) = 1$. Tenemos $x \equiv 7 \cdot 5^{-1} \pmod{11}$, por lo que $x \equiv 8 \pmod{11}$, y por el teorema anterior, tenemos que las soluciones de ña congruencia del inicio son $x \equiv \{8, 19, 30\} \pmod{33}$.

3.- La congruencia $12x \equiv 5 \pmod{14}$ no tiene solución, puesto que $\text{mcd}(12, 14) = 2$, pero $2 \nmid 5$. Se puede probar por fuerza bruta que no hay solución, cumpliéndose el teorema.

3.2. Sistemas de congruencias lineales. El teorema chino de los restos.

Definición 3.5. Sean a_i, b_i, $m_i \in \mathbb{Z}$, $m_i > 1$, $\forall i \in \{1, ..., r\}$. Un conjunto de congruencias con una variable x, de forma

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ a_r x \equiv b_r \pmod{m_r} \end{cases}$$

se denomina **sistema de congruencias lineales**.

Al igual que hicimos con una congruencia lineal, veremos como resolver un sistema de congruencias.

Observación 3.6. Para empezar, observar que toda congruencia de un sistema debe ser resoluble individualmente. Además, por el teorema anterior, podremos tener varias soluciones de cada congruencia del sistema. Entonces, si tenemos que $\forall i \in \{1, ..., r\}$, la congruencia $a_i x \equiv b_i \pmod{m_i}$ tiene solución, entonces el sistema anterior se puede reducir a varios sistemas, de la forma como se describe ahora:

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ x \equiv c_r \pmod{m_r} \end{cases}$$

siendo cada $c_i, i \in \{1, ..., r\}$ una solución posible de la congruencia i.

Para dar una solución del sistema, tomamos una solución de la primera congruencia y vamos llevándola a las siguientes congruencias, haciendo que sean compatibles con las siguientes. Se trata de ver la intersección de varias progresiones aritméticas.

Llegados a este punto, buscamos un método más rápido para encontrar estas soluciones. Podemos separar los casos posibles en dos: Los módulos m_i son coprimos dos a dos, o que haya módulos no coprimos entre sí. El primer caso es simple, pero muy importante, y obtenemos la solución mediante el teorema chino de los restos.

Teorema 3.7 (Teorema chino de los restos). *Sean $m_i \in \mathbb{Z}$, $m_i > 1$ $\forall i$ y sea $c_i \in \mathbb{Z}_{m_i}$. Si mcd(m_i, m_j)$= 1$, $1 \leq i < j \leq r$, entonces el sistema*

$$\begin{cases} x \equiv c_1 \ (mod\ m_1) \\ \quad . \\ \quad . \\ \quad . \\ x \equiv c_r \ (mod\ m_r) \end{cases}$$

tiene como solución completa una única clase de restos (mod $m_1...m_r$).

Demostración. Sea $m = m_1...m_r$. Con módulo y orden fijados, el sistema se define con el vector (r-pla) de constantes $\{c_1, ..., c_r\}$, siendo c_i clase de restos (mod m_i). Lo denotamos por $\overline{c_i} \in \mathbb{Z}_{m_i}$. Este vector $\{\overline{c_1}, ..., \overline{c_r}\}$ está en $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r}$. Dado un $x \in \mathbb{Z}$, tenemos que $\exists\{\overline{c_1}, ..., \overline{c_r}\}$ y es único, determinado por el sistema. Si el entero x cumple el sistema (es decir, es solución), entonces, $\forall x' \equiv x \pmod{m}$ lo cumple también, pues esto implica que $x' \equiv x \pmod{m_i}$ $\forall i \in \{1, ..., r\}$. Consideramos, entonces, $\overline{x} \in \mathbb{Z}_m$. A cada valor le corresponde un único vector en $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r}$, y tenemos un total de m clases de $\overline{x}$ distintas, con sus m vectores distintos. Por otro lado, cada vector va a determinar, como mucho, una clase $\overline{x} \in \mathbb{Z}_m$, pues si x y x' son soluciones del mismo sistema, $m_i \mid (x - x')$, con $i \in \{1, ..., r\}$, por lo que, por $m = m_1...m_r$, entonces $m \mid (x - x')$. Con esto, tenemos una biyección entre $\mathbb{Z}$ y $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r}$. Por tanto, tenemos

$$\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r} \longleftrightarrow \mathbb{Z}_m$$
$$\{\overline{c_1}, ..., \overline{c_r}\} \longleftrightarrow \overline{x}$$

□

Por el teorema chino de los restos hemos obtenido una biyección entre $\mathbb{Z}_m$ y $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r}$, si $m = m_1...m_r$ y los factores son coprimos dos a dos. Pero no sólo eso, sino que podemos hacer un isomorfismo de anillos. Antes de probar esto, tenemos que introducir la definición de suma directa.

Definición 3.8. Sean R_1, ...,R_r anillos. Se denomina **suma directa**, y se denota como $R = R_1 \oplus ... \oplus R_r$, al conjunto de vectores $R_1 \times ... \times R_r$ que cumplen lo siguiente: Siendo $\{a_1, ..., a_r\}$, $\{b_1, ..., b_r\} \in R$, entonces

- $\{a_1, ..., a_r\} = \{b_1, ..., b_r\} \Rightarrow a_1 = b_1$, ..., $a_r = b_r$.
- $\{a_1, ..., a_r\} + \{b_1, ..., b_r\} = \{a_1 + b_1, ..., a_r + b_r\}$.
- $\{a_1, ..., a_r\} \cdot \{b_1, ..., b_r\} = \{a_1 b_1, ..., a_r b_r\}$.

R es un anillo, con neutros $0 = \{0, ..., 0\}$ para la suma y $1 = \{1, ..., 1\}$ para el producto.

Definiendo esto, tenemos el resultado que nos da el isomorfismo de anillos adelantado antes de la definición de suma directa.

Teorema 3.9. *Sean* $m_1, ..., m_r \in \mathbb{Z}$, $m_1, ..., m_r > 1$, *y sea, además,* $m = m_1 \cdot ... \cdot m_r$, *y* $mcd(m_i, m_j) = 1\ \forall i \neq j$. *Entonces* $\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \ ... \ \oplus \mathbb{Z}_{m_r}$.

Demostración. Usamos la notación $(x)_m \in \mathbb{Z}_m$. La aplicación

$$\mathbb{Z} \longrightarrow \mathbb{Z}_m$$
$$x \longmapsto (x)_m$$

es un homomorfismo de anillos. Por tanto, tenemos que $\forall x, y \in \mathbb{Z}$, $x + y \longmapsto (x)_m + (y)_m$, y $xy \longmapsto (x)_m (y)_m$.

Por otro lado, sucede lo mismo para las aplicaciones

$$\mathbb{Z} \longrightarrow \mathbb{Z}_{m_i}$$
$$x \longmapsto (x)_{m_i}$$

Son también homomorfismos de anillos $\forall i \in \{1, ...r\}$. $\forall x, y \in \mathbb{Z}$ $x + y \longmapsto (x)_{m_i} + (y)_{m_i}$, y $xy \longmapsto (x)_{m_i} (y)_{m_i}$.

Se establece la correspondencia establecida por el teorema chino de los restos (3.7) entre $\mathbb{Z}_m$ y $\mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_r}$ entre $(x)_m \longleftrightarrow \{(x)_{m_1}, ..., (x)_{m_r}\}$ es una biyección. Por los homomorfismos anteriormente descritos, tenemos que la biyección anterior preserva suma y producto, por lo que será un isomorfismo. □

Sabiendo esto, podemos ver el valor de $x \in \mathbb{Z}_m$ que es solución del sistema de una variable con módulos coprimos dos a dos.

Observación 3.10. Sea el vector $\{\overline{c_1}, ..., \overline{c_r}\} \in \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_r}$. Entonces podemos poner $\{\overline{c_1}, ..., \overline{c_r}\} = \{\overline{c_1}, \overline{0}, ..., \overline{0}\} + ... + \{\overline{0}, ..., \overline{0}, \overline{c_r}\} = c_1\{\overline{1}, \overline{0}, ..., \overline{0}\} + \ ... \ + c_r\{\overline{0}, ..., \overline{0}, \overline{1}\} = c_1\overrightarrow{e_1} + ... + c_r\overrightarrow{e_r}$, siendo c_1, ..., $c_r \in \mathbb{Z}$ elementos de las clases de restos $\mathbb{Z}_{m_1}$, ..., $\mathbb{Z}_{m_r}$. Por lo tanto, este problema se reduce a encontrar la imagen en $\mathbb{Z}_m$ de cada vector de la base $\overrightarrow{e_1}$, ..., $\overrightarrow{e_r}$. Para $(y_i)_m \longleftrightarrow \overrightarrow{e_i}$, $i \in \{1, ..., r\}$, entonces, $x = c_1 y_1 + ... + c_r y_r$ cumple el sistema. Para los $\overrightarrow{e_i}$, el sistema pide que x, que en cada vector de la base se denota por y_i, sea múltiplo de todos los m_j con $i \neq j$. De este modo, tendríamos que $y_i = \frac{z_i m}{m_i}$, con $z_i \in \mathbb{Z}$, y se cumple $y_i \equiv 1 \pmod{m_i}$, o lo que es lo mismo, $\frac{m}{m_i} z_i \equiv 1 \pmod{m_i}$.

$\forall i = \{1, ..., r\}$, el sistema para los $\overrightarrow{e_i}$ colapsa en $\frac{m}{m_i} z_i \equiv 1 \pmod{m_i}$, y buscando z_i. La ventaja de este procedimiento es que, al encontrar z_i, tenemos una representación explícita de las soluciones del sistema para el vector de constantes $\{c_1, ..., c_r\}$. Con esto, tendremos $x \equiv c_1 \frac{m}{m_1} z_1 + \ ... \ + c_r \frac{m}{m_r} z_r \pmod{m}$, por lo que $x \equiv c_i \pmod{m_i}$ $\forall i \in \{1, ..., r\}$.

Con esto, ya tenemos una forma de resolver este tipo de sistemas si los módulos son coprimos dos a dos. Veamos, después del siguiente ejemplo, qué sucede si esta condición se suprime, es decir, hay al menos dos módulos del sistema que no son coprimos.

Ejemplo 3.11. Solucionaremos el siguiente sistema:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod{21} \\ x \equiv 7 \pmod{25} \end{cases}$$

Los módulos son coprimos dos a dos (fácil de ver). Por (3.7), tenemos que existe una solución en módulo $m = m_1 m_2 m_3$. Por tanto, tenemos que buscar la solución en módulo $m = 4{\cdot}21{\cdot}25 = 2100$.

Tenemos que $x \equiv 3{\cdot}\frac{2100}{4}{\cdot}z_1 + 5{\cdot}\frac{2100}{21}{\cdot}z_2 + 7{\cdot}\frac{2100}{25}{\cdot}z_3$, siendo $\frac{2100}{m_i}z_i \equiv 1 \pmod{m_i}$, con $i \in \{1,2,3\}$, siendo los módulos los descritos en el sistema.

Buscamos los z_i.

$\frac{2100}{4}z_1 \equiv 1 \pmod 4 \Leftrightarrow 525z_1 \equiv 1 \pmod 4 \Leftrightarrow z_1 \equiv 1 \pmod 4$.

$\frac{2100}{21}z_2 \equiv 1 \pmod{21} \Leftrightarrow 100z_2 \equiv 1 \pmod{21} \Leftrightarrow 16z_2 \equiv 1 \pmod{21} \Leftrightarrow z_2 \equiv 4 \pmod{21}$.

$\frac{2100}{25}z_3 \equiv 1 \pmod{25} \Leftrightarrow 84z_3 \equiv 1 \pmod{25} \Leftrightarrow 9z_3 \equiv 1 \pmod{25} \Leftrightarrow z_3 \equiv 14 \pmod{25}$.

Por lo tanto, tenemos que $x \equiv 3{\cdot}525{\cdot}1 + 5{\cdot}100{\cdot}4 + 7{\cdot}84{\cdot}14 = 1575 + 2000 + 8232 = 11807 \equiv 1307 \pmod{2100}$, que es la solución del sistema de congruencias.

Observación 3.12. A diferencia del caso de módulos coprimos dos a dos, en este caso, el sistema podría ser inconsistente. Por ejemplo, si tomamos el sistema $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 6 \end{cases}$ esto es imposible, pues la primera congruencia nos dice que x es impar, mientras que la segunda exige que el valor de x sea par. Así, en este caso tendremos que tener en cuenta alguna condición extra que no nos causaba problema en el caso de módulos coprimos.

Supongamos, entonces, un sistema de congruencias de una variable x con módulos m_1, ..., $m_r \in \mathbb{Z}$, $m_i > 1$ $\forall i \in \{1, ..., r\}$ no necesariamente coprimos. Si tenemos que la congruencia i-ésima es válida, entonces $x = c_i + m_i y$, para algún $y \in \mathbb{Z}$. Suponemos ahora que la congruencia j-ésima también es válida. Esto significa que se cumple la congruencia $m_i y \equiv c_j - c_i \pmod{m_j}$. Así, tenemos que la resolución de esta congruencia es posible (por (3.3)) $\Leftrightarrow \text{mcd}(m_i, m_j) | (c_i - c_j)$. Con esto, tenemos el siguiente teorema para resolver estos sistemas de congruencias.

Teorema 3.13. *Una condición necesaria y suficiente para que el sistema* $\begin{cases} x \equiv c_1 \ (mod\ m_1) \\ \quad . \\ \quad . \\ \quad . \\ x \equiv c_r \ (mod\ m_r) \end{cases}$

tenga solución es que (mcd(m_i, m_j))| (c_i-c_j), con i,j $\in \{1, ..., r\}$, $i < j$, además de que cada congruencia sea resoluble por separado.

En otras palabras, cualquier colección finita de progresiones aritméticas tiene intersección no vacía si cada par de progresiones lo tiene. Con solución existente, la solución completa en $\mathbb{Z}$ es una clase de restos (mod mcm(m_1, ..., m_r)).

Demostración. Sea la congruencia $x \equiv c_i \pmod{m_i}$ válido. Entonces x es congruente con c_i en cualquier módulo que sea un factor primo de m_i. Nos centramos en un único factor primo p que haya en al menos dos m_i, y suponemos que $p^{e_i} \parallel m_i$ (la p-componente de m_i, la mayor potencia de p que divide a m_i) para cada i. Sea p^t la mayor potencia de p que encontremos en algún m_i. Sea $t = e_1$. $x \equiv c_1 \pmod{p^t}$, entonces $x \equiv c_i \pmod{p^{e_i}}$ se cumple si $c_1 \equiv c_i \pmod{p^{e_i}}$ para todo i que sea relevante. En ese caso, las otras congruencias se consideran redundantes y son omitidas. Tenemos que $p^{e_i} \parallel \text{mcd}(m_1, m_i)$, cumpliendo $c_1 \equiv c_i \pmod{p^{e_i}}$ para todo i que sea válido. Al quitar las congruencias redundantes, tenemos congruencias válidas para todo p primo que divida a mcm(m_1, ...,m_r), y esas congruencias, una para cada p, tienen módulo p^t, p-componente de mcm(m_1, ..., m_r). A partir de aquí, el teorema chino de los restos (3.7) nos da la demostración del teorema. □

Con esto, tenemos las condiciones bajo las cuales un sistema de congruencias de una variable tiene solución.

Ejemplo 3.14. Solucionaremos el sistema:

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv 4 \pmod{21} \\ x \equiv 18 \pmod{35} \end{cases}$$

Descomponemos los módulos en factores primos: $12 = 2^2 \cdot 3$, $21 = 3 \cdot 7$, $35 = 5 \cdot 7$.

Por ello, tenemos que mcd(12, 21)= 3, mcd(12, 35)= 1, mcd(21, 35)= 7. Por el teorema anterior, tenemos que ver $3 \mid (4-1)$, $1 \mid (18-1)$, $7 \mid (18-4)$. Esto es cierto, pues $3 \mid 3$, $1 \mid 17$, $7 \mid 14$. Con esto, tenemos que existe una solución x en módulo mcm(12, 21, 35)= 420. Para encontrar este x, eliminamos los valores redundantes. En este caso, obviaremos en el sistema la congruencia de módulo 21.

Por ello, tenemos que $x \equiv 1 \cdot \frac{420}{12} \cdot z_1 + 18 \cdot \frac{420}{35} \cdot z_2 \pmod{420}$.

$\frac{420}{12} z_1 \equiv 1 \pmod{12} \Leftrightarrow 35 z_1 \equiv 1 \pmod{12} \Leftrightarrow z_1 \equiv 11 \pmod{12}$.

$\frac{420}{35} z_2 \equiv 1 \pmod{35} \Leftrightarrow 12 z_2 \equiv 1 \pmod{35} \Leftrightarrow z_2 \equiv 3 \pmod{35}$.

Sabiendo esto, tenemos $x \equiv 1 \cdot 35 \cdot 11 + 18 \cdot 12 \cdot 3 = 385 + 648 = 1033 \equiv 193 \pmod{420}$.

Esto concluye el estudio de congruencias lineales en una variable.

Capítulo 4

Congruencias binómicas y restos n-potenciales.

En el capítulo anterior hemos visto como resolver congruencias lineales en una variable y sistemas de congruencias. En este capítulo hablaremos de congruencias binómicas de una variable y daremos la definición de resto n-potencial. Antes de empezar, veremos algunas propiedades de congruencias de grado $n > 1$. Estos resultados serán muy importantes para lo que veremos en futuros capítulos.

4.1. Soluciones de una congruencia de grado n con módulo primo.

Definición 4.1. Sea $f(x) = \overline{a}_0 x^n + \ldots + \overline{a}_{n-1}x + \overline{a}_n$, siendo $f \in \mathbb{Z}_m[x]$, y sea $\overline{a} \in \mathbb{Z}_m$. Tenemos que $f(\overline{a}) = \overline{a}_0\overline{a}^n + \ldots \overline{a}_{n-1} + \overline{a}_n$ está bien definido en $\mathbb{Z}_m$, siendo el valor de $f(x)$ en $x = \overline{a}$.

Si tenemos que $f(\overline{a}) = \overline{0}$, entonces $\overline{a}$ se denomina **cero de** $f(x)$, o **raíz de** $f(x) = 0$ **en** $\mathbb{Z}_m$, o bien **raíz de** $\overline{a}_0 x^n + \ldots + \overline{a}_{n-1}x + \overline{a}_n = 0 \pmod m$.

A partir de la definición de raíz, tenemos el siguiente resultado:

Teorema 4.2. *$\overline{a}$ raíz de $f(x) \equiv 0 \pmod m \Leftrightarrow (x - \overline{a}) \mid f(x)$ en $\mathbb{Z}_m$.*

Demostración. Tenemos que $f(x)$ en $\mathbb{Z}_m$ se descompone de forma $f(x) = (x-\overline{a})q(x)+r(x)$, con $r(x) = 0$ o $\partial r < \partial(x - \overline{a})$ (teorema de división). En este caso, $\partial(x - \overline{a}) = 1$, por lo que $r(x) = 0$ o constante. Como $f(\overline{a}) = 0 \Leftrightarrow r = 0 \Leftrightarrow (x - \overline{a}) \mid f(x)$. □

A partir de esto, podemos el número de soluciones posibles de una congruencia en un

dominio de factorización única, es decir, cuando el módulo en el que está la congruencia es primo (1.12).

Teorema 4.3 (Teorema de Lagrange)**.** *Sea $p \in \mathbb{Z}^+$, p primo, y $f(x) \in \mathbb{Z}_m[x]$, de grado $n \geq 1$. Entonces, $f(x) \equiv 0 \pmod{p}$ tiene, como mucho, n raíces.*

Demostración. Hacemos la demostración por inducción en n, grado de $f(x)$. Además, denotaremos los elementos de $\mathbb{Z}_p$ como a y no como veníamos haciendo, $\overline{a}$.

Con $n = 1$, tenemos $f(x) = a_1x + a_0$. Por ser $\partial f(x) = 1$, tenemos que a_1 no congruente con 0 (mod p). Así, mcd(a_1, p)= 1, por (3.3), la congruencia $a_1x \equiv -a_0 \pmod{p}$ tiene una solución única (mod p). Por tanto, el teorema es válido para $n = 1$.

Asumimos que es válido para polinomios de grado $\partial f(x) \leq k-1$. Veamos si es válido el caso de grado k. Tenemos que, o bien $f(x) \equiv 0 \pmod{p}$ sin soluciones (y terminaríamos), o tiene al menos una solución, $a \in \mathbb{Z}_p$. Dividiendo $f(x)$ por $x - a$, tenemos que $f(x) = (x - a)q(x) + r$, con $q(x)$ polinomio de grado $k - 1$ con coeficientes enteros, y $r \in \mathbb{Z}$. Sustituyendo $x = a$, tenemos $0 \equiv f(a) = (a - a)q(a) + r = r \pmod{p}$, por lo que $f(x) \equiv (x - a)q(x) \pmod{p}$.

Supongamos que $b \neq a$ en $\mathbb{Z}_p$ es otra solución incongruente de $f(x) \equiv 0 \pmod{p}$. Entonces $0 \equiv f(b) = (b - a)q(b) \pmod{p}$. Como b y a son distintos en $\mathbb{Z}_p$, tenemos que $q(b) \equiv 0 \pmod{p}$. Dicho de otro modo, toda solución de $f(x) \equiv 0 \pmod{p}$ diferente de a cumple $q(x) \equiv 0 \pmod{p}$. Por hipótesis de inducción, esta congruencia $q(x) \equiv 0 \pmod{p}$ tiene, como mucho, $k - 1$ soluciones incongruentes ($\partial q(x) = k - 1$). Con esto, $f(x) \equiv 0 \pmod{p}$ tiene, como mucho, k soluciones incongruentes (las $k - 1$ de $q(x)$ y a). □

Observación 4.4. El teorema de Lagrange (4.3) no es válido si m es compuesto. En efecto, supongamos $m = ab$ factorización no trivial de m. Entonces se tiene que $(x - a)(x - b) \equiv x^2 - (a + b)x + ab \equiv x^2 - (a + b)x \equiv x(x - a - b) \pmod{m}$, por lo que tendremos que $x^2 - (a + b)x \equiv 0 \pmod{m}$ tiene 4 raíces (casi siempre distintas): $x = \{0, a, b, a + b\}$. Veremos un poco más sobre esto más adelante.

Volviendo a centrarnos en módulos primos, en principio no hay nada que nos indique que $f(x) \equiv 0 \pmod{p}$ tiene $n = \partial f(x)$ raíces distintas, así como no sucede esto en $\mathbb{Z}$. Sin embargo, el siguiente resultado nos indica la cantidad de raíces del polinomio en $\mathbb{Z}_p$.

Teorema 4.5. *Sea $p \in \mathbb{Z}^+$, p primo, y $f(x) \in \mathbb{Z}_p$ de grado n. Una condición necesaria y suficiente para $f(x) \equiv 0 \pmod{p}$ tener n raíces distintas es que $f(x) \mid (x^p - x)$ en $\mathbb{Z}_p[x]$. Dicho de otro modo, el número de raíces distintas de $f(x) = 0$ en $\mathbb{Z}_p$ es el grado que tiene mcd$(f(x), x^p - x)$ en $\mathbb{Z}_p$.*

Demostración. Por el teorema de Fermat (1.15), $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$. Así, $x^p - x$ tiene p ceros, $\overline{0}$, $\overline{1}$, ..., $\overline{p-1}$. Por ser $\mathbb{Z}_p$ DFU (1.12), entonces $x^p - x = x(x-\overline{1})...(x-\overline{p-1})$. Esta segunda parte de la igualdad tiene los polinomios lineales en $\mathbb{Z}_p$. Si en $\mathbb{Z}_p[x]$ tenemos $f(x) = (x-\overline{r}_1)^{s_1} \ ... \ (x-\overline{r}_k)^{s_k} g(x)$, donde $\overline{r}_i$ distintas si $i \neq j$, $s_i \in \mathbb{Z}^+$ y $g(x)$ sin factores lineales. Por tanto, tenemos que $\text{mcd}(f(x), x^p - x) = (x-\overline{r}_1) \ ... \ (x-\overline{r}_k)$. Por tanto, tomando $k = n$, tenemos que $\text{mcd}(f(x), x^p - x) = f(x)$, es decir, $f(x) \mid (x^p - x)$. □

Observación 4.6. Tener en cuenta que $(x - r_i)^{s_i}$ por este teorema cuenta como una única raíz. Por tanto, tenemos que este teorema no separa $f(x)$ en factores lineales necesariamente cuando $f(x) \mid (x^p - x)$.

Lo que sí tenemos a partir de ese teorema es el siguiente resultado.

Corolario 4.7. *Sean d, $p \in \mathbb{Z}^+$, p primo. Tenemos que $d \mid (p-1) \Rightarrow x^d \equiv 1 \pmod{p}$ tiene d soluciones.*

Demostración. $d \mid (p-1) \Rightarrow p - 1 = dk$, $k \in \mathbb{Z}$. Entonces, $(x^{p-1} - 1) = (x^d - 1) f(x)$, donde $f(x) = x^{d(k-1)} + \ ... \ + x^d + 1$ tiene coeficientes enteros y es de grado $d(k-1) = p - 1 - d$. Por teorema de Lagrange (4.3), $f(x) \equiv 0 \pmod{p}$ tiene, como mucho, $p - 1 - d$ soluciones. Por otro lado, por teorema de Fermat (1.15), $x^{p-1} - 1 \equiv 0 \pmod{p}$ tendrá $p - 1$ soluciones incongruentes, que son 1, ..., $p - 1$.

Toda solución de forma $x \equiv a \pmod{p}$ de $x^{p-1} - 1 \equiv 0 \pmod{p}$ que no es solución de $f(x) \equiv 0 \pmod{p}$ cumple $x^d - 1 \equiv 0 \pmod{p}$. Para $0 \equiv a^{p-1} - 1 = (a^d - 1) f(a)$, con $p \nmid f(a) \Rightarrow p \mid (a^d - 1) \Rightarrow x^d - 1 \equiv 0 \pmod{p}$ tiene, al menos, $p - 1 - (p - 1 - d) = d$ soluciones. La última congruencia no puede tener más de d soluciones (4.3). Por lo tanto, habrá d soluciones de esta congruencia. □

Con esto, ya tenemos el número de soluciones de una congruencia de cualquier grado en un módulo primo. Además, con esto podemos demostrar que en el teorema de Wilson (1.18) es una equivalencia, es decir, p primo $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$.

Implicación recíproca en el teorema de Wilson. Tenemos $p \in \mathbb{Z}$ y partimos de $(p-1)! \equiv -1 \pmod{p}$, y veamos que p tiene que ser primo.

Supongamos que p no es primo, por lo que $\exists d \in \mathbb{Z}$ divisor de p, con $1 < d < p$. $d \leq p - 1$, por lo que d es uno de los factores de $(p-1)!$, por lo que $d \mid (p-1)!$. Por la congruencia, $p \mid (p-1)! + 1$, y como $d \mid p$, entonces $d \mid (p-1)! + 1$. Por tanto, tenemos que $d \mid 1$ (si un número divide a una suma con dos sumandos y uno de ellos es múltiplo de ese número, el otro también), pero esto es absurdo. Por tanto, p es primo. □

Observación 4.8. Siendo el módulo p primo impar, podemos resolver también congruencias cuadráticas de forma $ax^2+bx+c\equiv 0 \pmod{p}$. Suponemos $a\in\mathbb{Z}_p$ de modo que $a\nmid p$. Por ser p primo, entonces esto significa que a es coprimo con p, es decir, tiene inverso, y $2p$ también. Con todo esto, podemos ver que la fórmula habitual de resolución $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ tiene sentido con la condición de que b^2-4ac sea un cuadrado perfecto para que haya un valor de $\mathbb{Z}_p$ que, elevado a 2, dé ese valor b^2-4ac.

Ejemplo 4.9. Veamos $3x^2-5x+5\equiv 0 \pmod{7}$. En este caso, $a=3$, $b=-5\equiv 2 \pmod{7}$, $c=5$. Llevando esto a la fórmula, tenemos $x=\frac{-2\pm\sqrt{2^2-4\cdot 3\cdot 5}}{2\cdot 3}=\frac{-2\pm\sqrt{4-60}}{6}=\frac{-2\pm\sqrt{-56}}{6}$, y como $7\mid 56$, esto es $x=-2\cdot 6^{-1}=-2\cdot 6=-12\equiv 2 \pmod{7}$.

La desventaja de esto, por el momento, es ver qué números pueden ser cuadrados en módulo p. Esto será más sencillo con lo que veremos en los últimos capítulos.

4.2. Congruencia de grado n con módulo compuesto. Congruencias binómicas.

Para un módulo compuesto, $m\in\mathbb{Z}$, con una descomposición en factores primos $m=p_1^{e_1}...p_r^{e_r}$ $(e_i\in\mathbb{Z}^+\ \forall i\in\{1,...,r\})$. La congruencia $f(x)\equiv 0 \pmod{m}$ equivale a un sistema de congruencias
$$\begin{cases} f(x)\equiv 0 \pmod{p_1^{e_1}} \\ \quad . \\ \quad . \\ \quad . \\ f(x)\equiv 0 \pmod{p_r^{e_r}} \end{cases}$$
Resolviendo cada congruencia de forma individual (habiendo solución en cada una), tenemos un sistema de forma
$$\begin{cases} x\equiv a_11 \text{ o } a_12 \text{ o } ... \text{ o } a_{1s_1} \pmod{p_1^{e_1}}, \\ \quad . \\ \quad . \\ \quad . \\ x\equiv a_r1 \text{ o } a_r2 \text{ o } ... \text{ o } a_{rs_r} \pmod{p_r^{e_r}} \end{cases}$$
y evoluciona a $s_1...s_r$ sistemas distintos, eligiendo una solución distinta para cada congruencia. Por tanto, el estudio de soluciones de una congruencia (mod m) arbitraria se reduce al estudio de $f(x)\equiv 0 \pmod{p^e}$, p, $e\in\mathbb{Z}$, p primo y $e\geq 0$.

Observación 4.10. Sea la congruencia $f(x)\equiv 0 \pmod{p^e}$, p, $e\in\mathbb{Z}$, p primo, $e\geq 1$. Tenemos que, si $e=2$, estas soluciones son válidas cuando $e=1$, pero no al revés. Lo mismo sucede con e arbitrario y $e-1$. Esto se da porque una clase de restos (mod p^e) se separan en p clases de restos (mod p^{e+1}). Por tanto, podemos afirmar que las soluciones con exponente $e+1$ vienen siempre de soluciones con exponente e.

Buscamos, entonces, una solución para p^{e+1} a partir de las de p^e.

Definición 4.11. Supongamos que conocemos las soluciones de la congruencia $f(x) \equiv 0 \pmod{p^e}$, con $e \in \mathbb{Z}$, $e > 0$. Veremos cuales son válidas para $f(x) \equiv 0 \pmod{p^{e+1}}$. Siendo x_0 solución de $f(x) \equiv 0 \pmod{p^e}$, veamos si x_0 puede ser aproximación de una o más soluciones de $f(x) \equiv 0 \pmod{p^{e+1}}$. x_0 será $\overline{x}_0 \pmod{p^e}$, y tiene los $x_0 + tp^e$, $t \in \mathbb{Z}$, siendo la unión de p clases de restos $\pmod{p^{e+1}}$. Tenemos que ver si se puede tomar $t \in \mathbb{Z}$ de modo que $f(x_0 + tp^e) \equiv 0 \pmod{p^{e+1}}$. Sea $h = tp^e$, y sabemos que $f(x_0 + h) = f(x_0) + f'(x_0)h + \ldots + \frac{1}{n!}f^{(n)}(x_0)h^n$ (teorema de Taylor). Por la definición de h, tenemos que las potencias de h mayores a e son $0 \pmod{p^{e+1}}$. Así, $f(x_0 + tp^e) \equiv f(x_0) + f'(x_0)tp^e \pmod{p^{e+1}}$. Si $f(x_0 + tp^e) \equiv 0 \pmod{p^{e+1}}$, entonces tenemos que $tp^e f'(x_0) \equiv -f(x_0) \pmod{p^{e+1}}$. p^e es un factor común (por ser x_0 solución de la congruencia en módulo p^e), por lo que tenemos que $tf'(x_0) \equiv -\frac{f(x_0)}{p^e} \pmod{p}$. Tenemos entonces una congruencia lineal de t, con soluciones:

$$\begin{cases} 0, \text{ si } p \mid f'(x_0) \text{ pero } p^{e+1} \nmid f(x_0) \\ p, \text{ si } p \mid f'(x_0) \text{ y } p^{e+1} \mid f(x_0) \\ 1, \text{ si } p \nmid f'(x_0) \end{cases}$$

En el primer caso, x_0 no es solución de la congruencia en $\pmod{p^{e+1}}$, y x_0 se queda en el nivel p^e. En el segundo caso, x_0 es solución a nivel p^{e+1}, por lo que las p clases de restos en $\pmod{p^{e+1}}$ serán soluciones. Se dice en estos casos que x_0 es una **solución singular** de $f(x) \equiv 0 \pmod{p^e}$. Si estamos en el tercer caso, es decir, con $p \nmid f'(x_0)$, entonces x_0 es una **solución no singular** de $f(x_0) \equiv 0 \pmod{p^e}$, y da una única solución x_1 de la congruencia $f(x) \equiv 0 \pmod{p^{e+1}}$, dada por $x_1 \equiv x_0 - \frac{f(x_0)}{f'(x_0)} \pmod{p^{e+1}}$.

Ejemplo 4.12. Partimos de la congruencia $f(x) = x^3 + x^2 + x \equiv 0 \pmod{3}$. Tenemos dos soluciones para esta congruencia: $x \equiv \{0, 1\} \pmod{3}$. Por otro lado, tenemos que $f'(x) = 3x^2 + 2x + 1 \equiv 2x + 1 \pmod{3}$.

La solución $x \equiv 0 \pmod{3}$ es una solución no singular, pues $f'(0) = 1$ y, obviamente, $3 \nmid 1$. Por lo tanto, si llevamos esta congruencia al módulo $3^2 = 9$, vamos a tener una solución que parte de $x \equiv 0 \pmod{9}$. Tenemos que el valor que es solución de $f(x) \equiv 0 \pmod{9}$ es $x \equiv 0 - \frac{f(0)}{f'(0)} \pmod{9}$. Tenemos como resultado $x \equiv -\frac{0}{1} \equiv 0 \pmod{9}$ es la solución de la congruencia partiendo de esta solución no singular.

Por otro lado, $x \equiv 1 \pmod{3}$ es una solución singular de la congruencia $\pmod{3}$, pues $f'(1) = 6$ y $3 \mid 6$. Por otro lado, tenemos que esta solución $\pmod{3}$ no da ninguna solución a la congruencia $f(x) \equiv 0 \pmod{9}$, pues $9 \nmid 6$.

Por tanto, basta aplicar esto para solucionar $f(x) \equiv 0 \pmod{p^e}$, con $e > 1$. Tenemos, además, un resultado interesante para ver la cantidad de soluciones de una congruencia de forma $x^d - 1 \equiv 0 \pmod{p^e}$, que parte de lo siguiente.

Proposición 4.13. *Sea $f(x) \equiv 0$ (mod p) con s raíces distintas, todas no singulares. Entonces, esto es cierto para $f(x) \equiv 0$ (mod p^e), $\forall e \geq 1$.*

Demostración. Sean x_{01}, ..., x_{0s} raíces de $f(x) \equiv 0 \pmod{p}$. Estas son incongruentes entre sí, pues en caso contrario, se tomaría una de esas soluciones como representante de las soluciones congruentes. Por este motivo, basta con ver que pasa con una de las soluciones. Sea x_0 una solución. Como es solución no singular, entonces $p \nmid f'(x_0)$. Se tiene, entonces, una solución única de forma $x_1 \equiv x_0 - \frac{f(x_0)}{f'(x_0)} \pmod{p^2}$. Despejando, tenemos $f(x_0) \equiv (x_0 - x_1)f'(x_0) \pmod{p^2}$. Por p primo, $0 \equiv f(x_0) \equiv (x_0 - x_1)f'(x_0) \pmod{p}$, ya que, siendo $a \in \mathbb{Z}$, $p^2 \mid a \Rightarrow p \mid a$. Por tanto, tenemos $0 \equiv (x_0 - x_1)f'(x_0) \pmod{p}$. Como $p \nmid f'(x_0)$, entonces son coprimos, y al ser $\mathbb{Z}_p$ cuerpo por p primo, tenemos que el factor $x_0 - x_1 \equiv 0 \pmod{p}$, por lo cual $x_0 \equiv x_1 \pmod{p}$. Por ello, tenemos que $p \nmid f'(x_1)$, por lo que $f'(x_1)$ coprimo con p, por lo que $p^e \nmid f'(x_1)$ $\forall e \geq 1$. Por tanto, es cierto si $e = 1$.

Aplicamos hipótesis de inducción para probar para el resto de valores de e. $e = 1$ acabamos de probarlo. Suponemos cierto para $e = k$, $k \in \mathbb{Z}$. Veamos si es cierto para $e = k + 1$.

Al ser cierto para $e = k$, tenemos que $\exists x_{k-1}$ solución de $f(x) \equiv 0 \pmod{p^k}$, que es solución no singular. Por esto, $p^k \mid f'(x_{k-1})$. Tenemos una solución única de forma $x_k \equiv x_{k-1} - \frac{f(x_{k-1})}{f'(x_{k-1})} \pmod{p^{k+1}}$. De aquí, $f(x_{k-1}) \equiv f'(x_{k-1})(x_{k-1} - x_k) \pmod{p^{k+1}}$. De esto, tenemos $0 \equiv f(x_{k-1}) \equiv f'(x_{k-1})(x_{k_1} - x_k) \pmod{p^k}$, pues $p^k \mid a \Rightarrow p^{k-1} \mid a$ $\forall k > 1$. Más concretamente, $p \mid a$. De esto, $0 \equiv f'(x_{k-1})(x_{k-1} - x_k) \pmod{p^k}$. $p^k \mid f'(x_{k-1})$, por lo que $f'(x_{k-1})$ no es congruente a 0 (mod p^k). Por hipótesis de inducción, tenemos que se cumple entonces que $x_{k-1} - x_k \equiv 0 \pmod{p^k}$, por lo que $x_{k-1} \equiv x_k \pmod{p^k}$, por lo que $p^k \nmid f'(x_k) \equiv f'(x_{k-1}) \pmod{p^k}$, por lo que $p^k \nmid f'(x_k)$, y entonces x_k es solución no singular (mod p^{k+1}).

Por tanto, hay s raíces distintas em $f(x) \equiv 0 \pmod{p^e}$, $\forall e \geq 1$. □

Visto esto, entonces podemos demostrar el siguiente resultado de manera sencilla.

Proposición 4.14. *Sean d, $p \in \mathbb{Z}$, p primo. $d \mid (p-1) \Rightarrow x^d - 1 = 0$ con d raíces en $\mathbb{Z}_{p^e}$, con $e \geq 1$.*

Demostración. Por la proposición anterior (4.13), bastará ver que si $x^d - 1 \equiv 0 \pmod{p}$, con $d \mid (p-1)$, toda solución $x^d - 1 \equiv 0 \pmod{p}$ es no singular, y que esta congruencia tiene d raíces.

- Existen d raíces distintas de $x^d - 1 \equiv 0 \pmod{p}$.

  Esto se da por (4.7). Por tanto, tenemos d soluciones de la congruencia.

- Las raíces son no singulares.

  Suponemos x_0 solución singular de $x^d - 1 \equiv 0 \pmod{p}$, con $d \mid (p-1)$. Por ser solución singular, $p \mid f'(x_0)$, por lo que $f'(x_0) \equiv 0 \pmod{p}$. Siendo $f(x) = x^d - 1$, entonces $f'(x) = dx^{d-1} \equiv 0 \pmod{p}$. Por ser p primo y $d \mid (p-1)$, entonces mcd(d, p)$= 1$, por lo que d tiene inverso en $\mathbb{Z}_p$, por lo que las soluciones de $f'(x) \equiv 0 \pmod{p}$ son las mismas que las de $x^{d-1} \equiv 0 \pmod{p}$.

  Si $d = 1$, $x^{1-1} = 1$, que no es congruente con $0 \pmod{p}$. De otro modo, al ser p primo, entonces $\mathbb{Z}_p$ es cuerpo, por lo que $x^{d-1} \equiv 0 \pmod{p}$, y así $x \equiv 0 \pmod{p}$ es la única solución posible. Sin embargo, $x \equiv 0 \pmod{p}$ no puede ser solución de $x^d \equiv 1 \pmod{p}$, pues $0 \equiv 1 \pmod{p}$ imposible con $p > 1$. En consecuencia, las posibles raíces de $x^d \equiv 1 \pmod{p}$ tienen que ser no singulares.

□

Nos quedaría entonces ver como solucionar esa congruencia con un módulo primo. La cantidad de soluciones posibles ya la vimos en el apartado anterior, pero no cuales son éstas.

Si el primo p es pequeño, podemos encontrar las soluciones por fuerza bruta, probando los distintos valores de $\mathbb{Z}_p$. Sin embargo, esto es tedioso en caso de que el valor de p sea muy grande. Necesitaríamos un criterio para su resolución.

Sin poder entrar en casos generales, pues es muy complejo, podemos ver como saber ciertos casos específicos, que serán suficientes para nuestro estudio. Empezamos con el criterio de Euler para ver si un elemento de $\mathbb{Z}_p$ es un cuadrado.

Teorema 4.15 (Criterio de Euler)**.** *Sea $p \in \mathbb{Z}^+$ un primo impar. Si $p \mid a$, la congruencia $x^2 \equiv a \pmod{p}$ es resoluble (trivialmente). Si $p \nmid a$, $x^2 \equiv a \pmod{p}$ es resoluble o no dependiendo de si $a^{\frac{(p-1)}{2}} \equiv 1$ o $-1 \pmod{p}$, respectivamente.*

Demostración. Veremos el caso $p \nmid a$. En este caso, 0 no es raíz de $x^2 \equiv a \pmod{p}$, por lo que examinamos mcd($f(x)$, $x^{(p-1)}-1$) en $\mathbb{Z}_p[x]$. $x^{p-1}-1 = ((x^2)^{\frac{(p-1)}{2}} - a^{\frac{(p-1)}{2}}) + (a^{\frac{(p-1)}{2}} - 1)$, y como $x^2 - a$ divide al primero de los sumandos, por (4.5), tenemos que si $a^{\frac{(p-1)}{2}} - 1 = 0$ en $\mathbb{Z}_p$, entonces $x^2 - a = 0$ tiene dos raíces, y del otro modo, es decir, si $a^{\frac{(p-1)}{2}} = -1$, no tiene ninguna. En efecto, pues $0 = a^{p-1} - 1 = (a^{\frac{(p-1)}{2}} - 1)(a^{\frac{(p-1)}{2}} + 1)$. Como $\mathbb{Z}_p$ es dominio, uno de estos factores debe ser 0. □

Con este teorema, podemos adelantar la definición del símbolo de Legendre $(\frac{a}{p})$ que es igual a 0 si $p \mid a$, 1 si $p \nmid a$ y $x^2 \equiv a \pmod{p}$ resoluble (y se dice que a es resto cuadrático de p), o -1 si $p \nmid a$ y $x^2 \equiv a \pmod{p}$ no resoluble (y en este caso a es no resto cuadrático de p). Profundizaremos en esto más adelante.

Ejemplo 4.16. Tomemos de módulo $p = 11$. Veamos si 2 y 3 son restos cuadráticos para este módulo.

$a = 2$ Tenemos que $2^{\frac{(11-1)}{2}} \equiv 2^5 \equiv 32 \equiv -1 \pmod{11}$. Por (4.15), tenemos que 2 es no resto cuadrático de 11.

$a = 3$ Tenemos que $3^{\frac{(11-1)}{2}} \equiv 3^5 \equiv 243 \equiv 1 \pmod{11}$. Por (4.15), 3 es resto cuadrático de 11. En efecto, pues $3 \equiv 25 = 5^2 \pmod{11}$.

Antes de pasar al siguiente apartado, hablaremos de las congruencias $ax^2 + bx + c \equiv 0 \pmod{m}$, con m arbitrario. Veremos el caso más sencillo de este tipo de congruencias binómicas, pues verlos todos no da resultados muy interesantes. El caso más sencillo es en el que $\mcd(m, 2a) = 1$. De esta forma, tenemos que la congruencia es equivalente a $(2ax + b)^2 \equiv b^2 - 4ac \pmod{m}$. Con esto, ya podemos resolverlo.

Otro tipo de congruencias de forma $ax^2+bx+c \equiv 0 \pmod{m}$ que podríamos solucionar son aquellas de módulo m primo, que ya hemos analizado antes, y que proseguiremos en futuros capítulos.

4.3. Restos n-potenciales.

Definición 4.17. Sea $m \in \mathbb{Z}$, $m > 1$, y sea $a \in \mathbb{U}_m$. Se dice que a es un **resto n-potencial** de m si $x^n \equiv a \pmod{m}$ es resoluble, es decir, $x^n = a$ en $\mathbb{Z}_m$ y, por tanto, en $\mathbb{U}_m$. En caso de que $x^n \equiv a \pmod{m}$ no sea resoluble, se dice que a es **no resto n-potencial** de m. Por tanto, basta ver qué sucede en $\mathbb{U}_m$ si el elemento está en $\mathbb{U}_m$.

Observación 4.18. Los restos 2-potenciales se denominarán **restos cuadráticos**, y los restos 3-potenciales se denominarán **restos cúbicos**.

Ejemplo 4.19. Tomemos el módulo $m = 7$. Tenemos que 2 es un resto 4-potencial, pues $3^4 = 81 \equiv 4 \pmod{7}$. Por otro lado, 3 no es un resto 4-potencial, pues no hay elementos en $\mathbb{Z}_7$ que, al elevarlos a 4 dé 3.

Tenemos, entonces, la siguiente relación entre restos n-potenciales.

Teorema 4.20. *Sean a, b, $m \in \mathbb{Z}$, $m > 1$. Si a y b son restos n-potenciales de m, entonces las congruencias $x^n \equiv a \pmod{m}$ y $x^n \equiv b \pmod{m}$ tienen el mismo número de soluciones.*

Demostración. Sean x_1, ..., x_k las soluciones de $x^n \equiv a$, y supongamos que $y^n \equiv b \pmod{m}$. Entonces, $(yx_1x_j^{-1})^n \equiv b \pmod{m}$, con $j \in \{1, ..., k\}$, y claramente $yx_1x_j^{-1}$ no es congruente en módulo m a $yx_1x_l^{-1}$ si $j \neq l$. Por simetría, cada congruencia en el teorema tendrá tantas soluciones como la otra. □

Ejemplo 4.21. Volviendo al caso de $m = 7$, tenemos que 2 y 4 son restos 4-potenciales. $x^4 \equiv 2 \pmod 7$ tiene como soluciones $x \equiv \{2, 5\}$, dos soluciones. Por otro lado, $x^4 \equiv 4 \pmod 7$ tiene como soluciones $x \equiv \{3, 4\}$, también dos soluciones.

Es fácil ver que, siendo x_i y x_j soluciones de $x^n \equiv a \pmod m$, $x_i x_j^{-1}$ es solución de $u^n \equiv 1 \pmod m$. Tenemos con esto el siguiente teorema.

Teorema 4.22. *El conjunto de restos n-potenciales (mod m) forma un subgrupo $\mathbb{U}_m^{(n)}$ de $\mathbb{U}_m$. Además, toda solución de la congruencia $x^n \equiv a$ (mod m) es de forma ux, con x solución fijada de la congruencia y u recorre el conjunto de soluciones de la congruencia $u^n \equiv 1$ (mod m).*

La demostración del teorema es obvia a partir de (4.20).

Este teorema expresado en lenguaje algebraico se expresa de la siguiente manera: La aplicación

$$\begin{aligned} \mathbb{U}_m &\longrightarrow \mathbb{U}_m^{(n)} \\ x &\longmapsto x^n \end{aligned}$$

es un homomorfismo cuyo núcleo es el grupo de soluciones de $u^n \equiv 1 \pmod m$, y las soluciones de $x^n \equiv a$ forman una clase lateral del núcleo en $\mathbb{U}_m$.

Observación 4.23. En el estudio de restos n-potenciales nos restringiremos a los casos de módulos de potencias de primos (3.7).

Para este estudio, separamos el primo 2 del resto de primos, que serán los primos impares. Para estos últimos, tenemos un criterio para que a sea resto n-potencial, que es una generalización del criterio de Euler (4.15) que veremos en futuros capítulos. Centrándonos en el caso de $p = 2$, tenemos el siguiente resultado.

Teorema 4.24. *Sean a, $e \in \mathbb{Z}$, $e \geq 3$. Entonces, todo a impar es un resto n-potencial de 2^e si n es impar. Con n par, a es un resto n-potencial de $2^e \Leftrightarrow a \equiv 1$ (mod mcd(2^e, $4n$)). En cualquier caso, el número de restos n-potenciales (mod 2^e) es $\frac{2}{mcd(n,2)} \cdot \frac{2^{e-2}}{mcd(n,2^{e-2})}$.*

Demostración. Sea $d{=}(n, 2^{e-2})$. Utilizamos una representación única de forma que se cumpla $a \equiv (-1)^\alpha 5^\beta \pmod{2^e}$, $0 \leq \alpha < 2$, $0 \leq \beta < 2^{e-2}$.

Buscamos ξ, η enteros positivos de modo que $((-1)^\xi 5^\eta)^n \equiv a \pmod{2^e}$.

Esto es válido $\Leftrightarrow n\xi \equiv \alpha \pmod 2$ y $n\eta \equiv \beta \pmod{2^{e-2}}$. La primera congruencia es resoluble $\Leftrightarrow \mathrm{mcd}(n, 2) | \alpha$, y tenemos $\mathrm{mcd}(n, 2)$ soluciones de $\xi \pmod 2$. La segunda es resoluble $\Leftrightarrow d \mid \beta$, que se cumple $\Leftrightarrow (5^\beta)^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$ o, por definición de β, $a^{\frac{2^{e-2}}{d}} \equiv (-1)^{\alpha \frac{2^{e-2}}{d}} \pmod{2^e}$.

Pero el exponente en -1 es siempre par si $\mathrm{mcd}(n,\,2)|\,\alpha$, pues en el caso $\alpha = 1$ implica que $d = 1$ (si $\alpha = 0$, $a^0 = 1$). Con esto, obtenemos una condición necesaria y suficiente para a resto n-potencial de 2^e: $\mathrm{mcd}(n,\,2)|\,\alpha$ y $a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$.

Si n es impar, entonces $\mathrm{mcd}(n,\,2) = 1$ y $d = 1$, por lo que lo anterior es válido por ser a impar. Supongamos entonces que $2^\nu \parallel n$, con $\nu > 0$. Entonces, $d = 2^{min\{e-2,\nu\}}$. En este caso, $\mathrm{mcd}(n,\,2)|\,\alpha$ válido $\Leftrightarrow \alpha = 0$. Así, $a \equiv 5^\beta \pmod{2^e}$, es decir, $a \in <5>$. Equivalentemente, $a \equiv 1 \pmod 4$. Por tanto, tenemos que $a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$ se transforma en $a \equiv 1 \pmod{2^e}$ si $e \leq \nu + 2$, y $a^{e-2-\nu} \equiv 1 \pmod{2^e}$ si $e \geq \nu + 2$.

Supongamos $e \geq \nu + 2$. En este caso, si se cumple $a \equiv 1 \pmod 4$ y $a^{2^{e-2-\nu}} \equiv 1 \pmod{2^e}$, entonces a es resto n-potencial de 2^e, por lo que es resto n-potencial de $2^{\nu+2}$. Por ello, esto es válido para $e = \nu + 2$. Por otro lado, tenemos que $a \equiv 1 \pmod{2^{\nu+2}}$, por lo que $a^{2^{e-2-\nu}} \equiv 1 \pmod{2^e}$ para $e > \nu+2$. Por esto, tenemos que $a^{e-2-\nu} \equiv 1 \pmod{2^e}$, $e \geq \nu+2$ $\Leftrightarrow a \equiv 1 \pmod{2^{\nu+2}}$, que, combinado con $a \equiv 1 \pmod{2^e}$, $e \leq \nu + 2$, nos da que $a \equiv 1 \pmod{2^{min\{e,\nu+2\}}}$. Pero esto es equivalente a $a \equiv 1 \pmod{\mathrm{mcd}(2^e,\,4n)}$.

Para el número de soluciones, tener en cuenta que, cuando $n\nu \equiv \beta \pmod{2^{e-2}}$ es resoluble, tiene d soluciones $\pmod{2^{e-2}}$. Por esto, hay un total de $\mathrm{mcd}(n,\,2)\cdot d$ pares de $\{\xi,\,\nu\}$ exponentes que nos dan distintos valores de $x \equiv (-1)^\xi 5^\nu \pmod{2^e}$, para el cual $x^n \equiv a \pmod{2^e}$ cuando a es resto n-potencial. Como el grupo $\mathbb{U}_{2^e}$ tiene 2^{e-1} elementos, la cantidad de restos n-potenciales será $\frac{2^{e-1}}{mcd(n,2)d}$, que es igual a $\frac{2}{mcd(n,2)}\cdot\frac{2^{e-2}}{mcd(n,2^{e-2})}$. □

Observación 4.25. El teorema es válido también si $e = 2$.

Ya tenemos entonces no sólo cuantos, sino también cuales son los restos n-potenciales en módulo 2^e con $e \geq 3$. Para módulos de otra forma, veremos qué sucede en el próximo capítulo.

Capítulo 5

Raíces primitivas.

Al finalizar el capítulo 2 adelantamos la definición de orden de un elemento del grupo $\mathbb{U}_m$, y dimos algunas propiedades interesantes. En este capítulo nos centraremos en las raíces primitivas de un grupo de unidades. Antes de profundizar en este concepto, veremos algunas propiedades útiles de órdenes de elementos de un grupo.

5.1. Propiedades de orden de elementos de $\mathbb{U}_m$.

Recordemos que la definición de orden de $a \in \mathbb{U}_m$ es la de $t \in \mathbb{Z}$, $t > 0$, siendo el mínimo t de modo que $a^t \equiv 1 \pmod{m}$, siendo $m \in \mathbb{Z}$, $m > 1$. Con esto, tenemos las siguientes propiedades, válidas con cualquier módulo.

Teorema 5.1. *Sean t, m, $n \in \mathbb{Z}$, t, $n > 0$, $m > 1$, y sea $a \in \mathbb{U}_m$ con $ord_m\ a = t$. Entonces, $ord_m\ (a^n) = \frac{t}{mcd(t,n)}$.*

Demostración. Sea d=mcd(n, t). Escribimos $n = n_1 d$, $t = t_1 d$, y mcd(n_1, t_1)= 1. Claramente, $(a^n)^{t_1} = (a^{n_1 d})^{\frac{t}{d}} = a^{n_1 t} = (a^t)^{n_1} \equiv 1 \pmod{m}$. **(1)**

Sea $ord_m(a^n) = r$. Por ello, $r \mid t_1$. Por otro lado, $ord_m\ a = t$, lo que nos dice que $a^{nr} \equiv (a^n)^r \equiv 1 \pmod{m}$, por lo que $t \mid nr$ (2.18), y en este caso, o $t_1 d \mid n_1 dr$ o $t_1 \mid n_1 r$. Como mcd(t_1, n_1)= 1, la primera parte sería igual a $t_1 \mid r$. Combinando esto con **(1)**, tenemos entonces que $r = t_1 = \frac{t}{d} = \frac{t}{mcd(n,t)}$. □

Ejemplo 5.2. Sea $m = 15$ y tomemos $t = 2$. Es fácil ver que $ord_{15}\ 2 = 4$. Por otro lado, tenemos que $8 = 2^3$ será, según el teorema, de orden $ord_{15}\ 8 = 2^3 = \frac{4}{mcd(4,3)} = 4$. Y es cierto, pues $8^4 = 4096 \equiv 1 \pmod{15}$ y $8^2 \equiv 4 \pmod{15}$, $8^3 \equiv 2 \pmod{15}$. Por otro lado, $4 = 2^2$ tendrá de orden $ord_{15}\ 4 = 2^2 = \frac{4}{mcd(4,2)} = 2$, lo que es cierto.

Teorema 5.3. *Sean $a \in \mathbb{U}_m$, $ord_m\ a = t$. Entonces, $a^i \equiv a^j \pmod{m} \Leftrightarrow i \equiv j \pmod{t}$.*

Demostración. Probaremos ambas implicaciones.

"$\Rightarrow$"

Partimos de $a^i \equiv a^j \pmod{m}$, y supongamos $i > j$. $a \in \mathbb{U}_m \Rightarrow a$ coprimo a m. Con esto, podemos cancelar una potencia de a para obtener $a^{i-j} \equiv 1 \pmod{m}$. Por (2.18), la última congruencia es válida con $t \mid (i-j)$, es decir, $i \equiv j \pmod{t}$.

"$\Leftarrow$"

Partimos de $i \equiv j \pmod{t}$, por lo que $i = j + qt$, con $q \in \mathbb{Z}$. Por definición de t, tendremos que $a^t \equiv 1 \pmod{m}$. De esto, $a^i \equiv a^{j+qk} \equiv a^j (a^t)^q \equiv a^j \pmod{m}$. □

Esto último nos demuestra que los elementos del grupo $< a > \subset \mathbb{U}_m$ son incongruentes entre sí, pues al tomar $1 \leq i \leq j \leq m$, entonces $i \equiv j \pmod{t}$, que sólo será válido si $i = j$.

Veremos, ahora, una propiedad que es válida para módulos primos, y será importante para futuros resultados tanto con módulos primos como compuestos.

Teorema 5.4. *Sea $p \in \mathbb{Z}$ un primo positivo. Sea $t \in \mathbb{Z}$. Entonces puede darse:*

1.– $t \nmid (p-1) \Rightarrow \nexists x \in \mathbb{Z} /\ ord_p\ x = t$.

2.– $t \mid (p-1) \Rightarrow$ *hay o bien* 0 *o bien* $\varphi(t)$ *elementos en* $\mathbb{U}_m$ *de orden* t.

Demostración. Probaremos ambas frases por separado.

1.- Sea $a \in \mathbb{U}_m$. Por teoría de grupos, $ord_m\ a \mid \varphi(m)$ (2.17), por lo que, al ser p primo, $\varphi(p) = (p-1)$, así, este resultado es cierto.

2.- Sea, ahora $t \mid (p-1)$ y $ord_m\ a = t$. Entonces, la congruencia $x^t \equiv 1 \pmod{p}$ tiene soluciones distintas $x \equiv a$, a^2, ..., a^t (4.3). Todo elemento de orden t es congruente a una de esas soluciones posibles para x. Por (5.1), tenemos que $ord_p\ (a^n) = t \Leftrightarrow$ mcd$(n, t) = 1$, con $1 \leq n \leq t$, por lo que hay $\varphi(t)$ elementos en $\mathbb{U}_m$.

□

Ejemplo 5.5. Sea $m = 13$. m es primo, por lo que $\mathbb{U}_{13}$ tiene $13 - 1 = 12$ elementos. Por lo tanto, si tomamos $t = 5$, no va a haber ningún elemento de $\mathbb{U}_{13}$ de orden 5 (pues $5 \nmid 12$). Por otro lado, con $t = 4$ tendríamos que comprobar si hay elementos con este orden, pues $4 \mid 12$. Tenemos que $5^4 = 625 \equiv 1 \pmod{13}$. Por lo tanto, tenemos que va a haber $\varphi(4) = 2$ elementos con este orden. En efecto, pues $ord_{13}\ 8 = 4$.

Con todo esto, empezaremos entonces el estudio de raíces primitivas.

5.2. Raíces primitivas en módulos primos y potencias de primos.

Definición 5.6. Sea $a \in \mathbb{U}_m$, $m \in \mathbb{Z}$, $m > 1$. Sabemos que, por definición de la función φ de Euler, que $\mathbb{U}_m$ tiene en total $\varphi(m)$ elementos. Así, el elemento $a \in \mathbb{U}_m$ es una **raíz primitiva del entero** m si $ord_m\ a = \varphi(m)$. Otras formas de ver esta definición son:

- $a^{\varphi(m)} \equiv 1 \pmod{m}$, pero a^k no congruente a 1 (mod m) $\forall k < \varphi(m)$, $k \in \mathbb{Z}^+$.
- El subgrupo $\mathbb{U}_m$ de $\mathbb{Z}_m$ es igual al grupo $< a >$, con a raíz primitiva de m.

Ejemplo 5.7. El conjunto $\mathbb{U}_7$ tiene como generador el elemento 3. En efecto, pues $< 3 >= \{3, 2, 6, 4, 5, 1\} = \mathbb{U}_7$. Por lo tanto, decimos que 3 es raíz primitiva de 7.

Con esto, tenemos que el grupo $\mathbb{U}_m$ tendría la estructura más simple posible, pues estaría generada por un elemento que sea raíz primitiva de $\mathbb{U}_m$. Además, ese $a \in \mathbb{U}_m$ no tiene por qué ser único. Esto lo veremos más tarde.

Vamos a ver si todos los números $m \in \mathbb{Z}$, $m > 1$ tienen raíces primitivas. Empezaremos con los números primos.

Teorema 5.8. *Sean $p \in \mathbb{Z}$ un número primo y $t \mid (p-1)$. Entonces $\exists \varphi(t)$ elementos en $\mathbb{U}_p$ de modo que $ord_p\ a = t$. En particular, $\mathbb{U}_p$ es cíclico y tiene $\varphi(p-1)$ raíces primitivas de p.*

Demostración. $\forall t$ divisor de $p-1$, sea $\psi(t)$ el número del teorema. $\forall a \in \mathbb{U}_p$ hay un orden único, y tenemos un total de $p-1$ elementos, tenemos que $\sum_{t|(p-1)} \psi(t) = p-1$.

Por otro lado, $\sum_{t|(p-1)} \varphi(t) = p-1$. Por (5.4), tenemos que $\psi(t)$ es 0 o $\varphi(t)$ $\forall t$. Por lo tanto, se compatibilizan solamente si $\psi(t) = \varphi(t)$ $\forall t$, con lo que tenemos el resultado. □

Destacaremos, en este caso, que si p es primo, entonces tenemos una cantidad de $\varphi(p-1)$ raíces primitivas del primo p.

Veamos ahora qué sucede con módulos que son potencias de números primos. Se tomará $m \in \mathbb{Z}$, $m = p^n$, con p primo y $n > 1$. Tenemos que separar los casos $p = 2$ y p impar. Veremos primero el siguiente resultado.

Teorema 5.9. *Sean a, p, $z \in \mathbb{Z}$, p primo impar y $p \nmid a$. Sea $ord_p\ a = t$ y $p^z \parallel a^t - 1$. Con $p > 2$ o $z > 1$, entonces $t_n = ord_{p^n}\ a = \begin{cases} t & si\ n \leq z \\ tp^{n-z} & si\ n \geq z \end{cases}$*

Demostración. Separamos en dos partes, dependiendo del valor de n.

a) $n \leq z \Rightarrow a^t \equiv 1 \pmod{p^n} \Rightarrow t_n \mid t$. Pero como $a^{t_n} \equiv 1 \pmod{p^n}$, por $p^n \mid (a^{t_n} - 1) \Rightarrow p \mid (a^{t_n} - 1)$, tenemos que $a^{t_n} \equiv 1 \pmod{p}$, por lo que $t \mid t_n$. En consecuencia, $t_n = t$.

b) Por definición, $z > 0$. Sea $n > z$, y pongamos $a^t = 1 + up^z$, con $p \nmid u$. Entonces, para $k = z$ y $u_k = u$, tenemos $a^{tp^{k-z}} = 1 + u_k p^k$, con $p \nmid u_k$.

$\forall k \geq z$ que mantiene la relación, tomando la p-ésima potencia en ambos lados, tenemos $a^{tp^{k-z+1}} = 1 + \binom{p}{1} u_k p^k + \ldots + \binom{p}{p-1} (u_k p^k)^{p-1} + (u_k p^k)^p$.

Claramente, $\binom{p}{s} = \frac{p(p-1)\ldots(p-s+1)}{s!}$, con $0 < s < p$ son divisibles por p, pues está p en el numerador en cada caso. Por tanto, las p-componentes de los términos siguientes al primero en la segunda parte son p^{k+1}, p^{2k+1}, ..., $p^{(p-1)k+1}$, p^{kp}.

Los exponentes, excepto el primero, son mayores a $k + 1$. Esto es obvio para todos los exponentes menos para kp. Pero siendo $kp > k + 1$, tenemos $k(p - 1) > 1$, que viene dado por $p > 2$ y $k \geq z > 1$. Por lo tanto, $\exists v_k \in \mathbb{Z}$ de modo que $a^{tp^{k-z+1}} = 1 + p^{k+1}(u_k + pv_k) = 1 + p^{k+1} u_{k+1}$, con $p \nmid u_{k+1}$. En consecuencia, $a^{tp^{k-z}} = 1 + u_k p^k$ es válido $\forall k \geq z$ por inducción.

En particular, $a^{tp^{k-z}} = 1 + u_k p^k$, por lo que $t_n \mid tp^{n-z}$. Sea $t_n = t' p^{n-r}$, con $t' \mid t$ y $r \geq z$. Ahora bien, como $a^{tn} \equiv 1 \pmod{p^n}$, entonces $a^{tn} \equiv 1 \pmod{p}$ (visto antes). Por tanto, $t \mid t_n$, como $\mathrm{mcd}(t, p) = 1$, tenemos que $t \mid t'$, y con esto, tenemos que $t = t'$. De este modo, $a^{tp^{n-r}} \equiv 1 \pmod{p^n}$, y como $a^{tp^{k-z}} = 1 + u_k p^k$, entonces $r \leq z$. Por consiguiente, $r = z$ y $t_n = tp^{n-z}$.

□

Ejemplo 5.10. Tomando $m = 25 = 5^2$ y tomemos el elemento $2 \in \mathbb{U}_{25}$. $ord_{25}\ 2 = 20$. Por ello, por el teorema tenemos que, con $5^3 = 125$, entonces $ord_{125}\ 2 = 20 \cdot 5^{3-2} = 20 \cdot 5 = 100$.

Por tanto, tenemos un teorema que nos da las raíces primitivas de p^n, con p y n enteros, p primo.

Construcción de raíces primitivas de potencias de primos impares. Sea $g \in \mathbb{Z}$ una raíz primitiva de p, y supongamos $z = 1$, siendo $z \in \mathbb{Z}^+$ el exponente de p que es p-componente de $g^{p-1} - 1$. Sea n el exponente descrito anteriormente. Con $n \geq 1$, tenemos por el teorema que $ord_{p^n}\ g = (p-1)p^{n-1} = \varphi(p^n)$, por lo que g es raíz primitiva de p^n. Por otro lado, si tenemos $z > 1$, tomando $g_1 = g + p$, que es raíz primitiva de p ($g_1 \equiv g \pmod{p}$). Sea $p^{z_1} \parallel g_1^{p-1} - 1$. Tenemos entonces que $g_1^{p-1} - 1 = (g+p)^{p-1} - 1 = g^{p-1} + (p-1)g^{p-2}p - 1 \equiv (p-1)g^{p-2}p$, pero esto no es congruente con 0 $(\mathrm{mod}\ p^2)$, por lo que $z_1 = 1$ y g_1 es raíz primitiva de p^n $\forall n \geq 1$. □

Por consiguiente, podemos afirmar que **toda potencia positiva de un número primo tiene una raíz primitiva**.

Llegamos ahora al caso en el que $p = 2$. Tenemos que, con $p = 2$, que el teorema (5.9) falla tomando también $z = 1$. Por ejemplo, $3 \equiv 1 \pmod 2$ es raíz primitiva de 2 con $z = 1$, pero 3 no es raíz primitiva de $8 = 2^3$. De hecho, no hay raíces primitivas de 8, ya que $\varphi(8) = 4$, pero $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, por lo que el orden máximo de los elementos de $\mathbb{U}_8$ tiene que ser $2 \neq 4$.

Por otro lado, si tomamos en $t_n = ord_{p^n}\ a = \begin{cases} t & \text{si } n \leq z \\ tp^{n-z} & \text{si } n \geq z \end{cases}$ los valores de $a = 5$, $t = 1$ y $z = 2$, tenemos que $ord_{2^n}\ 5 = 2^{n-2} = \frac{1}{2}\varphi(2^n)$. A partir de esto, tenemos un teorema interesante cuando $p = 2$.

Teorema 5.11. *Tanto 2 como 2^2 tienen a -1 como raíz primitiva. $\forall n \geq 3$, 2^n no tiene raíces primitivas. Por otro lado, las potencias 5, 5^2, ..., $5^{2^{n-2}}$ son la mitad de un sistema de restos reducido (mod 2^n), al ser estos enteros congruentes con 1 (mod 4). Las clases restantes se representan como -5, -5^2, ..., $-5^{2^{n-2}}$. Dicho de otro modo, $\mathbb{U}_{2^n}$ no es cíclico, pero tiene dos generadores, $\overline{-1}$, y $\overline{5}$ de órdenes 2 y $\frac{1}{2}\varphi(2^n)$.*

Demostración. 2 y 2^2 tienen a -1 como raíz primitiva es trivial: $-1 \equiv 1 \pmod 2$, que siempre tiene orden $1 = \varphi(2)$, $-1 \equiv 3 \pmod 4$ y $3^2 \equiv 1 \pmod 4$, con orden $2 = \varphi(4)$.

Para el resto de exponentes, como $\forall a$ impar, $a^2 \equiv 1 \pmod 8$, entonces la congruencia $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ es correcta con $k = 3$, y con $k \geq 3$ tenemos $a^{2^{k-1}} = (1 + 2^k u)^2 = 1 + 2^{k+1}(u + 2^{k-1}u^2) \equiv 1 \pmod{2^{k+1}}$, con $u \in \mathbb{Z}$. Así, tenemos que la congruencia vale $\forall k \geq 3$. Por lo tanto, siempre tendremos $(ord_{2^k}\ a) \mid 2^{k-2}$. Por definición, $\varphi(2^n) = 2^{n-1}$, por lo que no hay raíces primitivas.

La tercera frase viene de $ord_{2^n}\ 5 = 2^{n-2} = \frac{1}{2}\varphi(2^n)$, y de que las potencias de 5 son congruentes con 1 (mod 4). Esto, junto con el hecho de que de que hay exactamente 2^{n-2} enteros positivos menores a 2^n congruentes con 1 (mod 4), nos da el resultado. De forma análoga, tenemos que los elementos -5, ..., $-5^{2^{n-2}}$ son distintos (mod 2^n) al serlo 5, ..., $5^{2^{n-2}}$, y esos elementos son congruentes a -1 (mod 4). Por tanto, deben ser congruentes en algún grado a 3, 7, ..., $2^n - 1$. □

Con esto, sabemos que no todos los números enteros tienen raíces primitivas. Además, tenemos una pequeña introducción de como es la estructura del grupo de unidades cuando el módulo es un número sin raíces primitivas.

Antes de continuar, daremos una generalización de lo usado en el inicio de la demostración anterior.

Proposición 5.12. *Sean p, $n \in \mathbb{Z}$, siendo p primo y n positivo. Si $a \equiv b \pmod{p^n}$, entonces $a^{p^k} \equiv b^{p^k} \pmod{p^{n+k}}$, con k entero positivo.*

Demostración. $a \equiv b \pmod{p^n} \Rightarrow a = b + p^n u$, siendo $u \in \mathbb{Z}$.

Entonces tenemos que $a^p = (b+p^n u)^p = b^p + \binom{p}{1} b^{p-1} p^n u + ... + \binom{p}{p-1} b (p^n u)^{p-1} + (p^n u)^p = b^p + b^{p-1} p^{n+1} u + ... + b p^{n(p-1)+1} u + p^{np} u^p = b^p + p^{n+1}(b^{p-1} u + ... b p^{n(p-2)} u^{p-1} + p^{n(p-1)-1} u^p) \equiv b^p \pmod{p^{n+1}}$. Esto es válido con un n arbitrario, por lo que será válido $\forall k$, lo que da el resultado. □

5.3. Raíces primitivas con descomposición en varios primos.

Llegamos entonces a ver qué es lo que sucede si tenemos un módulo que se descompone en varios primos. Tenemos el siguiente resultado.

Teorema 5.13. $\left.\begin{array}{l} mcd(m,\, n) = 1 \\ m > 2,\, n > 2 \end{array}\right\} \Rightarrow mn \in \mathbb{Z}$ *sin raíces primitivas.*

Demostración. Sea $a \in \mathbb{Z}$ de modo que $\text{mcd}(a,\, mn) = 1$, por lo que $\text{mcd}(a,\, m) = 1$ y $\text{mcd}(a,\, n) = 1$. (2.5). Sean, entonces $h = \text{mcm}(\varphi(m),\, \varphi(n))$, y $d = \text{mcd}(\varphi(m),\, \varphi(n))$. Los elementos $\varphi(m)$ y $\varphi(n)$ son pares si $m,\, n > 2$ (φ función multiplicativa y $\varphi(2^n) = 2^{n-1}$ y $\varphi(p^n) = (p-1)p^{n-1}$ con p primo impar, por lo que $p-1$ par). Por esto, $d \geq 2$, por lo que $h = \frac{\varphi(m)\varphi(n)}{d} \leq \frac{\varphi(mn)}{2}$. Por (1.16), $a^{\varphi(m)} \equiv 1 \pmod{m}$. Elevando a la potencia $\frac{\varphi(n)}{d}$, $a^h \equiv (a^{\varphi(m)})^{\frac{\varphi(n)}{d}} \equiv 1^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{m}$. De forma análoga, tenemos que se cumple $a^h \equiv 1 \pmod{n}$. Uniendo esto a la hipótesis de que $\text{mcd}(m,\, n) = 1$, tenemos en consecuencia que $a^h \equiv 1 \pmod{mn}$. En consecuencia, tenemos que el orden de cualquier entero coprimo a mn no va a ser mayor a $\frac{\varphi(mn)}{2}$, que es menor a $\varphi(mn)$, orden de $\mathbb{U}_{mn}$. Por tanto, no hay raíces primitivas de mn. □

Por tanto, tenemos que si un número $a \in \mathbb{Z}$ se puede escribir como producto de dos números $m,\, n \in \mathbb{Z}$, ambos mayores que 2 y coprimos, entonces a no tiene raíces primitivas.

Tenemos confirmado, entonces, que los números 2, 4 y p^k, con p primo impar y $k \in \mathbb{Z}$, con $k \geq 1$ tienen raíces primitivas. Los únicos enteros positivos que no se han descrito ni aquí ni antes son los enteros de la forma $2p^k$, con $k \in \mathbb{Z}$, $k \geq 1$.

Teorema 5.14. *Los enteros de la forma $2p^k$, con p primo y $k \geq 1$ tienen raíces primitivas.*

Demostración. Este resultado es un corolario del caso de módulo p^k, con p primo y $k \in \mathbb{Z}$ mayor o igual a 1.

Sea g raíz primitiva de p^k, y asumimos que g es impar, pues de ser par, tenemos que $g + p^k$ es impar y raíz primitiva de p^k. Por esto, tenemos que $\text{mcd}(g,\, 2p^k) = 1$. Sea n el

orden de g en (mod $2p^k$). Tenemos que n divide $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$. Por ello, $g^n \equiv 1 \pmod{2p^k}$ implica que $g^n \equiv 1 \pmod{p^k}$, por lo que $\varphi(p^k) \mid n$. Por lo tanto, tenemos que $n = \varphi(2p^k)$, por lo que g es raíz primitiva de $2p^n$. □

Con todos estos resultados, podemos dar el siguiente teorema.

Teorema 5.15. *Los enteros con raíces primitivas son aquellos de una de las siguientes formas:* 2, 4, p^n *o* $2p^n$, *siendo* $p \in \mathbb{Z}$ *impar primo y* $n \in \mathbb{Z}$, *con* $n > 1$.

Con estos resultados hemos conseguido ver qué enteros son los que tienen raíces primitivas, pero no nos dan un algoritmo para saber cuales. Sin embargo, es sencillo ver que la única raíz primitiva de 2 es 1, y que 3 es la única raíz primitiva de 4. También tenemos un método de ver las raíces primitivas de una potencia positiva de un primo impar (5.9). Nos queda entonces ver como buscar las raíces primitivas de un número primo impar. En este caso, tenemos un problema finito que puede ser resuelto por prueba y error. Reducimos 2, 2^2, 2^3, etc., a sus menores restos positivos (los elementos $a \in \mathbb{Z}$, $0 \leq a < p$ de modo que $2^n \equiv a \pmod{p}$, con n entero), para ver $ord_p\ 2$. Si este orden es menor a $p-1$ (orden de $\mathbb{U}$), elegimos un entero a no congruente a una potencia de 2 (pues por (5.1) el orden de una potencia de una unidad (mod p) será menor o igual al orden del elemento, por lo que no podrá ser $p-1$), y vemos su orden. Seguimos hasta encontrar un elemento del orden buscado. De todas formas, podemos hacer esta búsqueda más eficiente.

Búsqueda raíz primitiva de un entero primo. Sean $a, b \in \mathbb{U}_p$, $t, u \in \mathbb{Z}$. Si tenemos

$$\left.\begin{array}{l} ord_p\ a = t \\ ord_p\ b = u \\ \text{mcd}(t, u) = 1 \end{array}\right\} \text{entonces } \exists v \in \mathbb{Z} \text{ de modo que } v = ord_p\ ab = tu. \text{ Claramente,}$$

$(ab)^{tu} \equiv 1 \pmod{p} \Rightarrow v \mid tu$.

Sea ahora $v = t_1u_1$, con $t_1 \mid t$ y $u_1 \mid u$. En este caso, $ord_p a^u = t$ (por t y u coprimos), y tenemos que $1 \equiv (ab)^{t_1u} \equiv (a^u)^{t_1} \pmod{p}$, por lo que $t \mid t_1$. De modo análogo, tenemos que $u \mid u_1$. Modificando lo que corresponda, tenemos que los elementos a, b de $\mathbb{U}_m$ con órdenes arbitrarios t y u tienen como producto un elemento de orden mcm(t, u). □

De este modo, podemos dar una nueva prueba de que los enteros primos tienen raíces primitivas. Supongamos q un entero primo de modo que $q^f \parallel p-1$, siendo $f > 0$. Por (4.7), las congruencias $x^{q^{f-1}} \equiv 1 \pmod{p}$ y $y^{q^f} \equiv 1 \pmod{p}$ tienen q^{f-1} y q^f soluciones respectivamente, y un $y \neq x$ con orden $q^f \pmod{p}$. Para cada q que divida a $p-1$, tomamos un y y multiplicamos estos y entre sí juntos, entonces este producto es una raíz primitiva de p.

Así, en vez de ir probando las potencias de a para ver su orden, usaremos el siguiente resultado.

Teorema 5.16. *Sean $p \in \mathbb{Z}$ primo y $a \in \mathbb{U}_p$. Si $p \nmid a$ y $\forall q$ divisor primo de $p-1$ se cumple que $a^{\frac{p-1}{q}}$ no congruente con 1 (mod p), entonces a es una raíz primitiva de p.*

Así, tenemos una forma más rápida para buscar raíces primitivas de un entero p primo impar.

5.4. Estructura del grupo $\mathbb{U}_m$.

Por ahora, sea $m \in \mathbb{Z}$ con descomposición en primos $m = p_1^{e_1} \ ... \ p_r^{e_r}$. Tenemos un isomorfismo entre $\mathbb{Z}_m$ y $\mathbb{Z}_{p_1^{e_1}} \oplus ... \oplus \mathbb{Z}_{p_r^{e_r}}$ (3.9), con lo que tenemos una biyección entre $(x)_m$ y $\{(x)_{p_1^{e_1}}, ..., (x)_{p_r^{e_r}}\}$. Sabemos claramente que si $x \in \mathbb{Z}$, entonces $(x)_m \in \mathbb{U}_m$ (que significa x coprimo con m) equivale a que $(x)_{p_i^{e_i}} \in \mathbb{U}_{p_i^{e_i}}$, con $1 \leq i \leq r$. Por lo tanto, podemos describir el grupo $\mathbb{U}_m$ de la siguiente forma.

Teorema 5.17. *Si $m \in \mathbb{Z}$ se descompone en factores primos de forma $m = p_1^{e_1}...p_r^{e_r}$, con p_i primos distintos entre sí y e_i enteros positivos, entonces $\mathbb{U}_m$ es isomorfo a $\mathbb{U}_{p_1^{e_1}} \times ... \times \mathbb{U}_{p_r^{e_r}}$, grupo de las r-plas con producto dentro de la misma componente.*

Podemos verlo de otro modo, usando lo visto para los factores $\mathbb{U}_{p^e}$. Con $p = 2$ tenemos un caso excepcional, por lo que cambiaremos un poco la notación. Denotaremos por $< a >$ al grupo cíclico generado por el elemento a de un grupo en específico.

Teorema 5.18. *Sea $m \in \mathbb{Z}$, $m > 1$ con descomposición en factores primos $m = 2^e p_1^{e_1}...p_r^{e_r}$, con e, $r \geq 0$ y si $r > 0$, p_1, ..., p_r son primos impares distintos y e_1, ..., e_r positivos. Sean g_1, ..., g_r raíces primitivas de p_1, ..., p_r, con $r > 0$. Entonces $\mathbb{U}_m$ es isomorfo al producto de grupos multiplicativos cíclicos siguiente:*

$< (-1)_{2^2} > \times < (5)_{2^e} > \times < (g_1)_{p_1^{e_1}} > \times ... \times < (g_r)_{p_r^{e_r}} >$, *donde los dos primeros factores se omiten con $e = 0$ o 1, y el segundo factor se omite también si $e = 2$.*

Esto puede ser expresado de otro modo, diciendo que $\forall a \in \mathbb{Z}$, existe una colección de exponentes $[\eta, \varepsilon, \varepsilon_1, ..., \varepsilon_r]$ de modo que

$$\begin{cases} a \equiv (-1)^\eta 5^\varepsilon \pmod{2^e},\ 0 \leq \eta < 2,\ 0 \leq \varepsilon < \frac{1}{2}\varphi(2^e), \\ a \equiv g_1^{\varepsilon_1} \pmod{p_1^{e_1}},\ 0 \leq \varepsilon_1 < \varphi(p_1^{e_1}), \\ \vdots \\ a \equiv g_r^{\varepsilon_r} \pmod{p_r^{e_r}},\ 0 \leq \varepsilon_r < \varphi(p_r^{e_r}) \end{cases}$$

con las mismas omisiones que en el caso del teorema.

Esto nos abre el paso al siguiente capítulo, que dedicaremos a la teoría de índices.

Capítulo 6

Índices.

En el capítulo anterior se habla del isomorfismo de grupos entre $\mathbb{U}_m$ y el producto de grupos cíclicos definido como $< (-1)_{2^2} > \times < (5)_{2^e} > \times < (g_1)_{p_1^{e_1}} > \times ... \times < (g_r)_{p_r^{e_r}} >$, siendo g_i raíz primitiva de $p_i^{e_i}$, con $1 \leq i \leq r$, y con los dos primeros factores que se pueden omitir. También tenemos una correspondencia de exponentes para este mismo grupo. Lo analizaremos.

6.1. Índices. Propiedades.

Sea $m \in \mathbb{Z}$ fijado. Asumimos $r > 0$ número de primos impares distintos en los que se descompone m y $8 \mid m$. Estas condiciones se toman por ser el caso en el cual no se omiten factores del producto isomorfo a $\mathbb{U}_m$. Así, todas las congruencias sucederán en el sistema de congruencias $\begin{cases} a \equiv (-1)^{\eta} 5^{\varepsilon} \pmod{2^e},\ 0 \leq \eta < 2,\ 0 \leq \varepsilon < \frac{1}{2}\varphi(2^e), \\ a \equiv g_i^{e_i} \pmod{p_i^{e_i}},\ 0 \leq \varepsilon_i \leq \varphi(p_i^{e_i}),\ \forall i \in \{1, ..., r\}. \end{cases}$ y teniendo los primos p_1, ..., p_r con orden fijado.

Sean g_1, ..., g_r raíces primitivas fijadas. Por el teorema para raíces primitivas fijadas, tenemos una biyección entre $a \in \mathbb{U}_m$ y una $(r+1)$-pla $\{\eta, \varepsilon, \varepsilon_1, ..., \varepsilon_r\}$, donde $\eta \in \mathbb{Z}_2$, $\varepsilon \in \mathbb{Z}_{2^{e-2}}$ y $\varepsilon_i \in \mathbb{Z}_{\varphi(p_i^{e_i})}$, con $1 \leq i \leq r$.

Tenemos, además que si $a \leftrightarrow \{\eta, \varepsilon, \varepsilon_1, ..., \varepsilon_r\}$ y $a' \leftrightarrow \{\eta', \varepsilon', \varepsilon_1', ..., \varepsilon_r'\}$, entonces tenemos $aa' \leftrightarrow \{\eta + \eta', \varepsilon + \varepsilon', \varepsilon_1 + \varepsilon_1', ..., \varepsilon_r + \varepsilon_r'\}$. Dicho de otro modo, esta correspondencia define un isomorfismo de grupos entre $\mathbb{U}_m$ y el producto de grupos aditivos cíclicos definido como $\mathbb{Z}_2 \times \mathbb{Z}_{\varphi(2^e)/2} \times \mathbb{Z}_{\varphi(p_1^{e_1})} \times ... \times \mathbb{Z}_{\varphi(p_r^{e_r})}$, con orden indicado en los subíndices.

Definición 6.1. El vector de exponentes definido en la correspondencia anterior se denomina **vector de índices** de a. Dadas las raíces primitivas g_1, ..., g_r de las potencias de primos correspondientes, ese vector de índices es único en el producto de grupos anterior.

Ejemplo 6.2. Tomando $m = 21 = 3{\cdot}7$. La única raíz primitiva de 3 es 2, mientras que 7 tiene como raíces primitivas 3 y 5. Tomando 3, el vector de índices del número $4 \in \mathbb{U}_{21}$ con respecto a estas raíces primitivas es $\{0, 4\}$. Por otro lado, el de $17 \in \mathbb{U}_{21}$ será $\{1, 1\}$.

Durante el resto de este capítulo, denotaremos por q a aquellos módulos para los cuales $\mathbb{U}_q$ es cíclico, dicho de otro modo, tienen una raíz primitiva, que llamaremos g.

Definición 6.3. Sea $\mathbb{U}_q$ con raíces primitivas. Para este módulo q, el vector de índices de a sólo tiene un elemento, al ser $< g >= \mathbb{U}_q$. Este elemento es denominado **índice** de $a \in \mathbb{U}_q$. Lo denotaremos como $ind\ a$.

Observación 6.4. Esta relación con a y su índice con respecto a la raíz primitiva g es análoga a la relación de un elemento $x \in \mathbb{R}^+$ con la función logaritmo (log).

Ejemplo 6.5. Sea $q = 18$. Sus raíces primitivas son 5 y 11. Con respecto a 5, tenemos que el índice de $7 \in \mathbb{U}_{18}$ es 2, mientras que el de $17 \in \mathbb{U}_{18}$ es 3.

Tenemos que $1 \leq ind\ a \leq \varphi(q)$, también que $g^{ind\ a} \equiv a \pmod{q}$, siendo g una raíz primitiva de q. De aquí, obtenemos entonces las siguientes relaciones.

Teorema 6.6. *Sea q con raíz primitiva g, y siendo $ind\ a$ el índice del elemento $a \in \mathbb{U}_q$ con respecto a g. Entonces se cumple:*

a) $ind\ (ab) \equiv ind\ a + ind\ b\ (mod\ \varphi(q))$

b) $ind\ a^k \equiv k\ ind\ a\ (mod\ \varphi(q))$, *con* $k > 0$.

c) $ind\ 1 \equiv 0\ (mod\ \varphi(q))$, $ind\ g \equiv 1\ (mod\ \varphi(q))$.

Demostración. Probaremos los distintos apartados:

a) Por definición de índice, $g^{ind\ a} \equiv a \pmod{q}$, $g^{ind\ b} \equiv b \pmod{q}$. Multiplicando, tenemos $g^{ind\ a + ind\ b} \equiv ab \pmod{q}$. Pero $g^{ind\ (ab)} \equiv ab \pmod{q}$, por lo que las congruencias anteriores nos dan $g^{ind\ a + ind\ b} \equiv g^{ind\ (ab)} \pmod{q}$. Podríamos tener que $ind\ a + ind\ b > \varphi(q)$, lo cual no sería un problema por (5.3). En efecto, pues esa última ecuación equivale a que sus exponentes son congruentes (mod $\varphi(q)$), es decir, $ind\ a + ind\ b \equiv ind\ (ab) \pmod{\varphi(q)}$.

b) Tenemos que $g^{ind\ a^k} \equiv a^k \pmod{q}$. Por otro lado, tenemos que $g^{k\ ind\ a} = (g^{ind\ a})^k \equiv a^k \pmod{q}$, por lo que $g^{ind\ a^k} \equiv g^{k\ ind\ a} \pmod{q}$. Por lo tanto, tenemos que $ind\ a^k \equiv k\ ind\ a \pmod{\varphi(q)}$.

c) Trivial por definición de raíz primitiva y (5.3).

□

Por lo tanto, estas propiedades nos dan una opción de resolución más simple de las ecuaciones de forma $ax^n \equiv b \pmod{q}$, siempre que esta congruencia tenga solución. Por tanto, lo siguiente a estudiar es saber qué índice tiene cada elemento de $\mathbb{U}_q$ con respecto a la raíz primitiva g. Para esto, podemos hacerlo probando cada exponente en la raíz primitiva g, o bien con tablas de índices. Trabajaremos como crear estas tablas en el siguiente apartado.

6.2. Tablas de índices.

En este apartado veremos como hacer las tablas de índices de un módulo $q \in \mathbb{Z}$ que admita raíces primitivas. Las tablas se hacen con respecto a una de estas raíces primitivas, y los índices varían dependiendo de la raíz primitiva escogida. Esto lo vemos en los siguientes ejemplos.

Ejemplo 6.7. Raíces primitivas y tabla de índices con respecto a una de éstas para el módulo $q = 41$.

El módulo $q = 41$ es primo. Por ello, tenemos que $\varphi(41) = 40$. El grupo $\mathbb{U}_{41}$ tiene 40 elementos (los elementos de $\mathbb{Z}_{41}$ sin el 0). Por (2.17), $ord_{41}\ a \mid 40\ \forall a \in \mathbb{U}_{41}$. (5.8) nos da que hay un total de $\varphi(40) = 16$ raíces primitivas. Por (5.1), las raíces primitivas son aquellos elementos de $\mathbb{U}_{41}$ que no son cuadrados ni potencias quintas, al descomponerse $40 = 2^3 \cdot 5$ en factores primos.

Vemos, en primer lugar, qué elementos de $\mathbb{U}_{41}$ son cuadrados de otros. Utilizando la igualdad $(n+1)^2 = n^2 + (2n+1)$ y teniendo en cuenta que $x^2 \equiv (41-x)^2 \pmod{41}$ (pues $(41-x)^2 = 41^2 - 82x + x^2 \equiv x^2 \pmod{41}$), calculamos hasta $n = 20$. Ordenándolos, tenemos que los restos cuadráticos en módulo 41 son los siguientes:

$\{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\}$.

Tenemos un total de 20 restos cuadráticos, y nos quedan 20 elementos, de los cuales sabemos que 16 son raíces primitivas. Los 4 restantes son restos 5-potenciales. Veremos cuales de estos elementos lo son. En $\mathbb{Z}_{41}$, tenemos:

$3^5 = 38 = 7^5 = 13^5$, $6^5 = 27 = 14^5$, $11^5 = 3 = 12^5$, $15^5 = 14$.

Por ello, estas raíces 5-potenciales son $\{3, 14, 27, 38\}$.

Así, tenemos que $\{6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35\}$ son raíces primitivas de $q = 41$.

Procedemos ahora a la construcción de la tabla de índices a partir de una raíz primitiva de 41. Tomemos $g = 6$. Las siguientes potencias se van haciendo de forma recursiva del siguiente modo: $g^{n+1} \equiv g \cdot g^n \pmod{41}$. Obtenemos la siguiente tabla:

a	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	40
ind a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	35	5	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7	1
ind a	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40

Una vez tenemos la tabla, la resolución de congruencias del estilo $ax^n \equiv b \pmod{q}$ es más simple en caso de ser resoluble. Volviendo al ejemplo anterior, tenemos que resolver $16x \equiv 37 \pmod{41}$ equivale a resolver $ind\ 16 + ind\ x \equiv ind\ 37 \pmod{40}$. Sustituyendo los índices con $g = 6$, tenemos que $ind\ x \equiv 32 - 24 = 8 \pmod{40}$. Tenemos que $ind\ x = 8$. El elemento $a \in \mathbb{U}_{41}$ que tiene este índice es $x \equiv 10 \pmod{41}$.

Para $3x^2 \equiv 17 \pmod{41}$, tenemos $2ind\ x \equiv ind\ 17 - ind\ 3 \equiv 33 - 15 = 18 \pmod{40}$. Por tanto, tenemos que $ind\ x \equiv 9$ ó $29 \pmod{40}$, por lo que los valores posibles de x son 19 ó 22 (mod 41).

También es posible que la congruencia no sea resoluble. Con $3x^2 \equiv 10 \pmod{41}$, tenemos $2ind\ x \equiv ind\ 10 - ind\ 3 \equiv 8 - 15 = -7 \equiv 33 \pmod{40}$. Como 2 y 40 no son coprimos (pues 40 es múltiplo de 2), y al no ser entero $\frac{33}{2}$, entonces la congruencia no tiene solución.

Observación 6.8. El valor del índice de los elementos de $a \in \mathbb{U}_q$ depende de la raíz primitiva g escogida.

Si en el ejemplo tomamos $g = 7$, la tabla de índices es:

a	7	8	15	23	38	20	17	37	13	9	22	31	12	2	14	16	30	5	35	40
ind a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	34	33	26	18	3	21	24	4	28	32	19	10	29	39	27	25	11	36	6	1
ind a	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40

En este caso, la congruencia $16x \equiv 37 \pmod{41}$ equivale a $ind\ 16 + ind\ x \equiv ind\ 37 \pmod{40} \Leftrightarrow ind\ x \equiv 8 - 16 = -8 \equiv 32 \pmod{40}$, lo que indica que $x \equiv 10$. El resultado es el mismo, pero no los índices.

Además, las congruencias no resolubles siguen sin poder resolverse. $3x^2 \equiv 10 \pmod{41} \Leftrightarrow 2ind\ x \equiv ind\ 10 - ind\ 3 \equiv 32 - 25 = 7 \pmod{40}$, y tenemos el mismo inconveniente que había con $g = 6$.

Si bien podríamos diferenciar el índice dependiendo de la raíz primitiva utilizada usando $ind_g\ a$, sólo usaremos esta notación cuando pueda haber confusiones. En general, utilizaremos $ind\ a$.

Ejemplo 6.9. Raíces primitivas y tabla de índices con respecto a una de éstas para el módulo $q = 37$.

37 es primo, por lo que $\mathbb{U}_{37}$ tiene $\varphi(37) = 36$ elementos (los elementos de $\mathbb{Z}_{37}$ menos el 0). Tenemos que $ord_{37}\ a \mid 36$, y sabemos que habrá $\varphi(36) = 12$ raíces primitivas. (5.1) nos dice que estas raíces primitivas son elementos de $\mathbb{U}_{37}$ que no sean restos cuadráticos ni restos cúbicos. Usando $(n+1)^2 = n^2 + (2n+1)$, tenemos la siguiente lista de restos cuadráticos: $\{1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36\}$. Tenemos un total de 18 restos cuadráticos, y nos quedan otros 18 elementos en $\mathbb{U}_{37}$. Como sabemos que hay 12 raíces primitivas, entonces 6 de esos elementos restantes tienen que ser restos cúbicos. Llegamos a lo siguiente en $\mathbb{Z}_{37}$:

$2^3 = 8 = 15^3$, $5^3 = 14 = 13^3$, $6^3 = 31 = 8^3$, $14^3 = 6$, $17^3 = 29$, $18^3 = 23$.

Por esto, los restos cúbicos son $\{6, 8, 14, 23, 29, 31\}$,lo que resulta en las siguientes raíces primitivas: $\{2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35\}$.

Haremos ahora la tabla de índices de $\mathbb{U}_{37}$ para la raíz primitiva $g = 2$. Por recursividad, $g^{n+1} \equiv g \cdot g^n \pmod{37}$. Tenemos la tabla siguiente:

a	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36
ind a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1
ind a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

Con esto tenemos otro ejemplo de tabla de índices con módulo primo impar. Pero ya sabemos que estos números no son los únicos que tienen raíces primitivas. Hacer tablas para los números 2 y 4 no nos da nada, pues tienen una cantidad manejable de unidades, y las potencias superiores no tienen raíces primitivas (5.11). Veremos entonces los casos que nos faltan.

Antes de esto, necesitamos un resultado previo. Con un módulo primo p ya hemos demostrado que el número de raíces primitivas es $\varphi(\varphi(p))$. Veamos que esto se da con todo número q que admite raíces primitivas.

Teorema 6.10. *Sea $q \in \mathbb{Z}$ un número con raíces primitivas. Entonces, $\exists\varphi(\varphi(q))$ raíces primitivas.*

Demostración. Sea $a \in \mathbb{U}_q$ raíz primitiva de q. (5.1) nos indica que una potencia de una raíz primitiva es raíz primitiva si $\text{mcd}(\varphi(q), t) = 1$, siendo t el exponente al que está elevada la raíz primitiva a. Por lo tanto, esto sucede con una cantidad $\varphi(\varphi(q))$, y habrá esta cantidad de raíces primitivas de q. □

Con esto, podemos adentrarnos en la construcción de tablas de índices para cualquier módulo que tenga raíces primitivas.

Ejemplo 6.11. Raíces primitivas y tabla de índices con respecto a una de éstas para el módulo $q = 81$.

$81 = 3^4$, potencia del primo 3. Por tanto, hay raíces primitivas. Por (2.10), tenemos que hay $\varphi(81) = 2{\cdot}3^3 = 54$ elementos en $\mathbb{U}_{81}$. Por teoría de grupos, tenemos que $ord_{81}a \mid 54$ $\forall a \in \mathbb{U}_{81}$.

81 es una potencia del primo 3, por lo que los elementos de $\mathbb{U}_{81}$ son aquellos elementos de $\mathbb{Z}_{81}$ que no son múltiplos de 3. Además, por el teorema anterior (6.10), tenemos que habrá un total de $\varphi(\varphi(81)) = \varphi(54) = 18$ raíces primitivas. Por ser $54 = 2{\cdot}3^3$, las raíces primitivas de este grupo serán los elementos que no sean restos cuadráticos ni restos cúbicos.

Los restos cuadráticos de las unidades son $\{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76, 79\}$. Tenemos 27 restos cuadráticos. Destacar el hecho de que todos estos elementos son de la forma $3k + 1$, con $k \in \mathbb{Z}_{27}$.

Los 27 elementos restantes se separan en 18 raíces primitivas y 9 restos cúbicos que veremos ahora. En $\mathbb{Z}_{81}$, tenemos lo siguiente:

$2^3 = 8$, $5^3 = 44$, $8^3 = 26$, $11^3 = 35$, $14^3 = 71$, $17^3 = 53$, $20^3 = 62$, $23^3 = 17$, $26^3 = 80$.

Por tanto, los restos cúbicos son $\{8, 17, 26, 35, 44, 53, 62, 71, 80\}$. Como hicimos antes, destacamos que todos son de la forma $9k + 8$, $k \in \mathbb{Z}_9$.

El conjunto de raíces primitivas de este grupo es el siguiente: $\{2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77\}$.

Tomemos ahora la raíz primitiva $g = 2$. Obtenemos la siguiente tabla:

a	2	4	8	16	32	64	47	13	26	52	23	46	11	22	44	7	14	28
ind a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a	56	31	62	43	5	10	20	40	80	79	77	73	65	49	17	34	68	55
ind a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
a	29	58	35	70	59	37	74	67	53	25	50	19	38	76	71	61	41	1
ind a	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54

Veremos, a continuación, el caso en el que $q = 2p^k$, con p primo y k positivo.

Ejemplo 6.12. Tenemos $q = 26 = 2{\cdot}13$. $\mathbb{U}_{26}$ tiene un total de $\varphi(26) = \varphi(2)\varphi(13) = 1{\cdot}12 = 12$ elementos por (2.10). Son los elementos de $\mathbb{Z}_{26}$ que no son pares ni el 13. Además, $\forall a \in \mathbb{U}_{26}$, $ord_{26}\ a \mid 12$. Por (6.10), sabemos que hay $\varphi(12) = 4$ raíces primitivas de 26, y como $12 = 2^2{\cdot}3$, las raíces primitivas de 26 son los elementos de $\mathbb{U}_{26}$ que no son restos cuadráticos ni restos cúbicos.

La lista de restos cuadráticos de las unidades (mod 26) ordenada es $\{1, 3, 9, 17, 23, 25\}$.

Nos quedan entonces 6 elementos, que se separan en 4 raíces primitivas y 2 restos cúbicos. Obtenemos lo siguiente en $\mathbb{Z}_{26}$:

$5^3 = 21$, $7^3 = 5$. Con esto tenemos que las raíces cúbicas (mod 26) son $\{5, 21\}$.

Por tanto, tenemos que $\{7, 11, 15, 19\}$ son las raíces primitivas de 26. Tomemos ahora $g = 7$. Tenemos la siguiente tabla:

a	7	23	5	9	11	25	19	3	21	17	15	1
ind a	1	2	3	4	5	6	7	8	9	10	11	12

Ejemplo 6.13. Tenemos $q = 18 = 2{\cdot}3^2$. $\mathbb{U}_{18}$ tiene un total de $\varphi(18) = \varphi(2)\varphi(9) = 1{\cdot}6 = 6$ elementos por (2.10). Son los elementos de $\mathbb{Z}_{18}$ que no son pares ni divisibles entre 3. Además, $\forall a \in \mathbb{U}_{18}$, $ord_{18}\ a \mid 6$. Por (6.10), sabemos que hay $\varphi(6) = 2$ raíces primitivas de 18,y como $6 = 2{\cdot}3$, las raíces primitivas de 18 son los elementos de $\mathbb{U}_{18}$ que no son restos cuadráticos ni restos cúbicos.

La lista de restos cuadráticos de las unidades (mod 18) ordenada es $\{1, 7, 13\}$.

Nos quedan entonces 3 elementos, que se separan en 2 raíces primitivas y 1 resto cúbico. Obtenemos lo siguiente en $\mathbb{Z}_{18}$:

$5^3 = 17 = 11^3 = 17^3$. Con esto tenemos que la raíz cúbica (mod 18) es 17.

Por tanto, tenemos que $\{5, 11\}$ son las raíces primitivas de 18.

Tomamos, ahora, $g = 5$. La tabla de índices es la siguiente:

a	5	7	17	13	11	1
ind a	1	2	3	4	5	6

Entonces, ya hemos visto algunas tablas de índices para números que admiten raíces primitivas. Podemos extrapolar esto a módulos sin raíces primitivas. La diferencia en este caso está en que ahora tendremos una tabla de vectores de índices, partiendo del sistema de congruencias de (5.18), tenemos el vector de índices con el que empezamos el capítulo $\{\eta, \varepsilon, \varepsilon_1, ..., \varepsilon_r\}$. Este vector depende de las raíces primitivas elegidas para los factores primos, así como del orden de estos.

Ejemplo 6.14. Tabla de vectores de índices $m = 40$.

Tenemos $m = 40 = 2^3{\cdot}5$. Por (6.1), tenemos que $\mathbb{U}_{40}$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_{\varphi(2^3)/2} \times \mathbb{Z}_{\varphi(5)}$. Este conjunto es $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$. La cantidad de elementos en $\mathbb{U}_{40}$ es $\varphi(40) = \varphi(2^3){\cdot}\varphi(5) = 4{\cdot}4 = 16$. Son los elementos de $\mathbb{Z}_{40}$ que no son pares ni divisibles entre 5. Tomando $g = 2$ raíz primitiva de 5 (la otra posible es 3, 1 y 4 son raíces cuadráticas (mod 5)). La tabla de índices en (mod 5) es

a	2	4	3	1
ind a	1	2	3	4

Partiendo de esto, tenemos lo siguiente:

a	1	3	7	9	11	13	17	19
$\eta \in \mathbb{Z}_2$	0	1	1	0	1	0	0	1
$\varepsilon \in \mathbb{Z}_2$	0	1	0	0	1	1	0	1
$\varepsilon_1 \in \mathbb{Z}_4$	0	3	1	2	0	3	1	2
Vector	(0,0,0)	(1,1,3)	(1,0,1)	(0,0,2)	(1,1,0)	(0,1,3)	(0,0,1)	(1,1,2)
a	21	23	27	29	31	33	37	39
$\eta \in \mathbb{Z}_2$	0	1	1	0	1	0	0	1
$\varepsilon \in \mathbb{Z}_2$	1	0	1	1	0	0	1	0
$\varepsilon_1 \in \mathbb{Z}_4$	0	3	1	2	0	3	1	2
Vector	(0,1,0)	(1,0,3)	(1,1,1)	(0,1,2)	(1,0,0)	(0,0,3)	(0,1,1)	(1,0,2)

Observación 6.15. Las propiedades en (6.6) pueden extrapolarse a los vectores. Volviendo al ejemplo anterior, tenemos, por ejemplo, que $3{\cdot}17 \equiv 11 \pmod{40}$, y al sumar los vectores asociados, tenemos $(1,1,3)+(0,0,1) = (1,1,0)$ (en el producto de anillos descrito en el ejemplo), que es el vector asociado a 11. Por otro lado, tenemos que $7^2 \equiv 9 \pmod{40}$, y $2{\cdot}(1,0,1) = (0,0,2)$.

Con esto, podemos resolver sencillamente las congruencias de forma $ax^n \equiv b \pmod{m}$ siendo a, $b \in \mathbb{U}_m$ y $n \in \mathbb{Z}$, $n \geq 1$, siempre que esta sea resoluble. Para los otros elementos de $\mathbb{Z}_m$, no podemos utilizar los índices para su resolución. Habría que ver si ba^{-1}, que no es una unidad (aunque a sí lo es), es un cuadrado de los elementos no unidades de $\mathbb{Z}_m$.

Por ejemplo, volviendo al ejemplo anterior, usando esa tabla de vectores de índices, podemos ver si $13x^3 \equiv 21 \pmod{40}$ o $13x^2 \equiv 21 \pmod{40}$ son resolubles.

Para $13x^3 \equiv 21 \pmod{40}$, sustituyendo por vectores de índices en el producto de grupos definido $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, tenemos $(0,1,3) + 3vector\ x = (0,1,0) \Leftrightarrow$

$3vector\ x = (0,1,0) - (0,1,3) = (0,0,-3) = (0,0,1)$. Como $3 \in \mathbb{U}_4$, entonces tiene inverso, por lo que tenemos que $vector\ x = 3^{-1}(0,0,1) = 3(0,0,1) = (0,0,3)$. Por ello, $x \equiv 33 \pmod{40}$, siendo $vector\ x$ el vector de índices asociado a x.

Para $13x^2 \equiv 21 \pmod{40}$, tenemos $(0,1,3) + 2vector\ x = (0,1,0) \Leftrightarrow 2vector\ x = (0,0,1)$. Como 2 no coprimo con 4, no tiene inverso, y como 2 no divide a 1, entonces no es resoluble.

Con esto, tenemos una manera más simple para la resolución de congruencias de forma $ax^n \equiv b \pmod{m}$.

6.3. Resultados derivados de las propiedades de índices.

Procedemos a presentar unos resultados importantes que se prueban gracias a lo que sabemos de índices. El que vamos a presentar ahora es una generalización del criterio de

Euler (4.15), así como de (4.7).

Teorema 6.16. *Sea $q \in \mathbb{Z}$ número con raíces primitivas y supongamos $a \in \mathbb{U}_q$. a es un resto n-potencial de $q \Leftrightarrow a^{\frac{\varphi(q)}{d}} \equiv 1$ (mod q), con d =mcd(n, $\varphi(q)$).*

El número de restos n-potenciales de q es $\frac{\varphi(q)}{d}$, y cada uno de ellos es el resto n-potencial de exactamente d enteros (mod q).

Demostración. Tomando índices en $x^n \equiv a \pmod q$, tenemos $n\ ind\ x \equiv ind\ a \pmod{\varphi(q)}$, que es resoluble si, y sólo si, $\mathrm{mcd}(n, \varphi(q))|\ ind\ a$. Esto es lo mismo que decir que $ind\ a \equiv 0 \pmod d$, por lo que se tiene $\frac{\varphi(q)}{d}\ ind\ a \equiv 0 \pmod{\varphi(q)}$, por lo que $a^{\frac{\varphi(q)}{d}} \equiv 1 \pmod q$.

Finalmente, si g es raíz primitiva de q, entonces los $\frac{\varphi(q)}{d}$ números g^d, g^{2d}, ..., $g^{(\frac{\varphi(q)}{d})d}$ son distintos (mod q), cumpliendo la congruencia del teorema. Tenemos, entonces, $\frac{\varphi(q)}{d}$ soluciones. Por (4.20), estas son las soluciones posibles. □

Por otro lado, podemos utilizar la teoría de índices para resolver congruencias de la forma $ax^2 + bx + c \equiv 0 \pmod p$.

Resolución de congruencias cuadráticas con índices. Sea $Ax^2 + Bx + C \equiv 0 \pmod p$, p primo impar y $p \nmid A$. Entonces A tiene inverso. Llegamos a lo siguiente: $x^2 + bx + c \equiv 0 \pmod p$, siendo $b = BA^{-1}$ y $c = CA^{-1}$. Los valores de b y c pueden ser 0 si B o C son 0; o podemos calcularlos por índices ($ind\ b = ind\ B - ind\ A$ en $\mathbb{Z}_{p-1}$, y con c análogo).

Aplicamos la fórmula a la nueva congruencia: $x = \frac{-b \pm \sqrt{b^2-4c}}{2}$. Como p es primo, $\mathbb{Z}_p$ es cuerpo y todo elemento menos el 0 tiene inverso, por lo que 2 tiene inverso. Podemos calcular $b^2 \pmod p$ con $2ind\ b \pmod{(p-1)}$. Por otro lado, $4c \pmod p$ se calcula como $ind\ 4 + ind\ c \pmod{(p-1)}$. Ya calculado esto, calculamos $\Delta = b^2 - 4c$. Así, llevamos el valor $\sqrt{\Delta} \pmod p$ a $\frac{1}{2}\ ind\ \Delta \pmod{(p-1)}$. Por ser p impar, $p-1$ es par, por lo que 2 y $p-1$ no son coprimos. Por tanto, lo anterior sólo tiene sentido si $ind\ \Delta$ es par. Si no, es irresoluble.

Si es resoluble, $(-b \pm \sqrt{\Delta})/2$ tiene sentido (mod p), y podemos resolverlo por índices. □

Con esto no necesitamos saber nada más que si $ind\ \Delta$ es par para ver si es resoluble o no, sin necesidad de resultados avanzados, cosa que no sucedía sin índices. Esos resultados a los que hacemos alusión serán estudiados a partir del siguiente capítulo.

Capítulo 7

Restos cuadráticos y el símbolo de Legendre.

A lo largo de los siguientes capítulos estudiaremos la forma de ver de manera rápida si un elemento de $\mathbb{Z}_m$, con $m \in \mathbb{Z}$, $m > 1$ es un cuadrado de otro elemento de ese conjunto. Primero profundizaremos en la definición de resto cuadrático y daremos algún resultado con respecto a estos elementos.

7.1. Restos cuadráticos.

Definición 7.1. Sea $m \in \mathbb{Z}$, $m > 1$, y sea $a \in \mathbb{U}_m$. Se dice que a es un **resto cuadrático de** m si la congruencia $x^2 \equiv a \pmod{m}$ es resoluble. Es, como ya se dijo en capítulos anteriores, el caso de resto n-potencial con $n = 2$. En caso de que no sea resoluble, entonces a es un **no resto cuadrático** de m.

Es sencillo ver que si $a \in \mathbb{Z}$ es resto cuadrático en módulo m y $b \equiv a \pmod{m}$, entonces b es resto cuadrático (pues ambos se representan por el mismo elemento $x \in \mathbb{Z}_m$).

Ejemplo 7.2. Tenemos que $4 \in \mathbb{Z}_{13}$ es un resto cuadrático de 13, pues $2^2 \equiv 4 \pmod{13}$. Sin embargo, $5 \in \mathbb{Z}_{13}$ no es resto cuadrático de 13. Por otro lado, tenemos que $4 \equiv 17 \pmod{13}$, por lo que 17 será también un resto cuadrático de 13.

Veremos, a continuación, un par de teoremas que nos indicarán que las cuestiones referidas a restos cuadráticos de módulo compuesto se pueden reducir al caso de módulo primo.

Observación 7.3. El número primo 2 juega un papel distinto al resto de primos, por hecho de que toda solución (mod 2) va a ser singular, pues $f(x) = x^2 - a$, por lo que $f'(x) = 2x$, y $2 \mid f'(x)$ $\forall x$ cosa que no pasa con otros primos.

Teorema 7.4. *Sea $m \in \mathbb{Z}$, $m > 1$. Un elemento $a \in \mathbb{U}_m$ es un resto cuadrático de m $\Leftrightarrow$ Existe un resto cuadrático de todos los primos impares que forman $m = 2^e p_1^{e_1} ... p_r^{e_r}$, y* $\begin{cases} a \equiv 1 (mod\ 4) & si\ 2^2 \parallel m, \\ a \equiv 1 (mod\ 8) & si\ 8 \mid m. \end{cases}$

Demostración. Sea $m = 2^e p_1^{e_1} ... p_r^{e_r}$. Entonces la congruencia $x^2 \equiv a \pmod{m}$ equivale a

$$\begin{cases} x^2 \equiv a \pmod{2^e}, \\ x^2 \equiv a \pmod{p_1^{e_1}}, \\ \qquad . \\ \qquad . \\ \qquad . \\ x^2 \equiv a \pmod{p_r^{e_r}} \end{cases}$$

Claramente, si a es resto cuadrático de $p_i^{e_i}$, con $1 \leq i \leq r$, entonces es resto cuadrático del propio primo. Por otro lado, si a resto cuadrático de un primo impar p, entonces $a^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}$ por (6.16), por lo que $a^{p^{e-1}\frac{(p-1)}{2}} \equiv 1 \pmod{p^e}$ (5.12), por lo que a es resto cuadrático de p^e. Como en el caso con módulo 4, 1 es resto y -1 no. Para el caso 2^e, con $e \geq 3$, (4.24), para $n = 2$ nos da que $a \equiv 1 \pmod{8}$ es una condición necesaria y suficiente para que a sea un resto. □

Con esta demostración, tenemos una forma de ver la cantidad de soluciones de la congruencia $x^2 \equiv a \pmod{m}$. (6.16) nos dice que hay dos soluciones con $m = p^e$, con p primo impar. Para el caso de $x^2 \equiv a \pmod{2^e}$, tenemos e soluciones si $e = \{1, 2\}$. Si $e \geq 3$, tenemos que (4.24) nos da una existencia de 2^{e-3} restos. Así, (4.20) nos dice que $x^2 \equiv a \pmod{2^e}$ tiene un total de $\frac{\varphi(2^e)}{2^{e-3}} = 4$ soluciones en caso de ser resoluble. Obtenemos, así, el siguiente resultado:

Teorema 7.5. $\left.\begin{array}{c} a \in \mathbb{U}_m \\ x^2 \equiv a\ (mod\ m)\ resoluble \end{array}\right\} \Rightarrow \exists\ 2^{r+u}$ *soluciones, siendo r la cantidad de primos impares distintos que hay y $u = \{0, 1, 2\}$, dependiendo de si $4 \nmid m$, $2^2 \parallel m$, o $8 \mid m$, respectivamente.*

Ejemplo 7.6. Veamos el número de soluciones posibles para $x^2 \equiv 9 \pmod{20}$. Según el teorema anterior, al saber que $3^2 \equiv 9 \pmod{20}$, tenemos que la congruencia es resoluble y, según el teorema anterior, esta congruencia tendrá $2^{1+1} = 2^2 = 4$ soluciones distintas, pues $20 = 2^2 \cdot 5$ tiene un primo impar 5 y $4 \parallel 20$. Una solución es 3 como ya hemos visto. Comprobando los distintos elementos de $\mathbb{Z}_{20}$, tenemos que todas las soluciones de la congruencia son $\{3, 7, 13, 17\}$, un total de 4 soluciones, tal como predecía el teorema.

Con esto, hemos avanzado en el estudio de raíces cuadráticas: hemos visto la cantidad de soluciones que habrá en una congruencia cuadrática en módulo m, con $m \in \mathbb{Z}$ $m > 1$.

Nos falta ver como saber si un elemento es resto cuadrático en módulo m, cosa que veremos a partir de ahora.

7.2. El símbolo de Legendre.

Ya hemos visto que los restos cuadráticos de potencias del primo 2 se pueden dar explícitamente, y que los restos cuadráticos de las potencias de un primo impar son aquellos que lo son para el propio primo. Por tanto, podemos centrarnos en investigar los restos cuadráticos de módulos primos impares.

Definición 7.7. Sea $p \in \mathbb{Z}$, p primo impar positivo y $a \in \mathbb{Z}_p$. Entonces se define el **símbolo de Legendre** $(\frac{a}{p})$ de la siguiente forma: $(\frac{a}{p}) = \begin{cases} 1, & \text{si } a \text{ es un resto cuadrático de } p, \\ -1, & \text{si } a \text{ es un no resto cuadrático de } p, \\ 0, & \text{si } p \mid a. \end{cases}$

Teorema 7.8. *Con las condiciones de la definición de símbolo de Legendre, siendo $a \in \mathbb{Z}$, arbitrario, entonces $a^{\frac{(p-1)}{2}} \equiv (\frac{a}{p})$ (mod p). Esto da una forma "rápida" de ver si un entero es un resto cuadrático de un primo impar o no, y dando, así, el valor de esta función para ese número con el módulo p.*

Ejemplo 7.9. Volviendo al primer ejemplo, el de restos cuadráticos en módulo 13, ya hemos visto que 4 es resto cuadrático de 13, pero 5 no. Tenemos entonces que $(\frac{4}{13}) = 1$ y $(\frac{5}{13}) = -1$. Esto se cumple por el criterio de Euler. En efecto, pues tenemos $4^{\frac{13-1}{2}} = 4^6 = 4096 \equiv 1 \pmod{13}$, y $1 = (\frac{4}{13})$, por lo que se cumple. Por otro lado, $5^{\frac{5}{13}} = 5^6 = 15625 \equiv -1 \pmod{13}$, y $-1 = (\frac{5}{13})$.

Veamos algunas propiedades de esta función.

Teorema 7.10. *El símbolo de Legendre $(\frac{a}{p})$ cumple:*

a) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. *Esto nos dice que el producto de dos restos cuadráticos o de dos no restos cuadráticos es un resto cuadrático, mientras que el producto de un resto cuadrático con un no resto cuadrático será un no resto cuadrático. Esto, además, nos dice que el símbolo de Legendre es una función multiplicativa.*

b) $a \equiv b \pmod{p} \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$.

c) $(\frac{a^2}{p}) = 1$ *si* $p \nmid a$.

d) $(\frac{-1}{p}) = (-1)^{\frac{(p-1)}{2}}$. *Así,* -1 *es resto cuadrático de* p *si* $p \equiv 1 \pmod{4}$, *pero no si* $p \equiv -1 \pmod{4}$.

Demostración. Probamos los distintos apartados, usando (7.8):

a) $(\frac{ab}{p}) \equiv (ab)^{\frac{(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}}\ b^{\frac{(p-1)}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \pmod p$. Otra forma de verlo es la siguiente: El símbolo de Legendre vale ± 1 si el elemento es coprimo con p. Si $(\frac{ab}{p}) \neq (\frac{a}{p})(\frac{b}{p})$, entonces $1 \equiv -1 \pmod p$, o lo que es lo mismo, $2 \equiv 0 \pmod p$, por lo que $p \mid 2$, lo que es absurdo por $p > 2$. Por lo que lo escrito es cierto.

b) $a \equiv b \pmod p \Rightarrow \begin{cases} x^2 \equiv a \pmod p \\ x^2 \equiv b \pmod p \end{cases}$ con las mismas soluciones. Por lo tanto, $x^2 \equiv a \pmod p$ y $x^2 \equiv b \pmod p$ serán ambos resolubles o ambos no resolubles. Por ello, $(\frac{a}{p}) = (\frac{b}{p})$.

c) Tenemos que a satisface $x^2 \equiv a^2 \pmod p$, por lo que $(\frac{a^2}{p}) = 1$.

d) Tomamos $a = -1$, y sabemos que $(\frac{-1}{p})$ y $(-1)^{\frac{(p-1)}{2}}$ son 1 o -1. Por lo tanto, $(\frac{-1}{p}) \equiv (-1)^{\frac{(p-1)}{2}} \pmod p$, por lo que, al ser p primo impar, $p > 2$, y entonces $(\frac{-1}{p}) = (-1)^{\frac{(p-1)}{2}}$.

□

Entonces, podemos asumir que a es un primo positivo, y tomar el símbolo de Legendre $(\frac{a}{p})$ con a y p primos. Con esto, tenemos el siguiente resultado que, aunque usaremos con a primo, es válido $\forall a/\ p \nmid a$.

Teorema 7.11 (Lema de Gauss)**.** *Si μ es la cantidad de elementos de a, $2a$, ..., $\frac{1}{2}(p-1)a$, cuyos menores restos en valor absoluto (mod p) son negativos (es decir, entre -1 y $p-1$, tomamos -1, siendo $p > 2$), entonces $(\frac{a}{p}) = (-1)^{\mu}$.*

Demostración. Reemplazamos los elementos a, $2a$, ..., $\frac{1}{2}(p-1)a$ por sus restos menores en valor absoluto (mod p). Denotamos los positivos como r_1, r_2, ...; y los negativos como $-r'_1$, $-r'_2$, ... No hay dos r_i iguales, ni dos r'_i iguales. Además, si $m_1 a \equiv r_i \pmod p$ y $m_2 a \equiv -r'_j$ y $r_i = r'_j$, entonces $a(m_1 + m_2) \equiv 0 \pmod p$, por lo que tenemos $m_1 + m_2 \equiv 0 \pmod p$ (por $a \in \mathbb{U}_p$), lo que es imposible por $0 < m < \frac{p}{2}$. Por lo tanto, los $\frac{(p-1)}{2}$ números r_i, r'_i son enteros distintos entre 1 y $\frac{(p-1)}{2}$, esos números están en algún orden. Por tanto, $a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a \equiv (-1)^{\mu}(\frac{p-1}{2})! \pmod p$, y por tanto $a^{\frac{(p-1)}{2}} \equiv (-1)^{\mu} \pmod p$. Como además $a^{\frac{(p-1)}{2}} \equiv (\frac{a}{p}) \pmod p$, entonces $(\frac{a}{p}) \equiv (-1)^{\mu} \pmod p$, por lo que $(\frac{a}{p}) = (-1)^{\mu}$. □

Ejemplo 7.12. Una vez más, volvemos a partir de $4, 5 \in \mathbb{Z}_{13}$.

En el caso $a = 4$, tenemos los valores 4, 8, 12, 16, 20 y 24 con el lema de Gauss. Reduciendo a módulo 13, a sus menores restos en valor absoluto, tenemos 4, -5, -1, 3,

-6, -2. Tenemos 4 elementos en ese conjunto que son negativos en módulo 13. Por ello, $\mu = 4$ y $(-1)^\mu = (-1)^4 = 1 = (\frac{4}{13})$.

Si $a = 5$, tenemos 5, 10, 15, 20, 25 y 30, que reducidos a sus menores restos en valor absoluto en módulo 13, tenemos 5, -3, 2, -6, -1, 4. En este caso, $\mu = 3$ y tenemos $(-1)^\mu = (-1)^3 = -1 = (\frac{5}{13})$.

Este lema nos ayuda a caracterizar los primos de los cuales un entero a es resto cuadrático. Si tomamos $a = 2$, tenemos el siguiente teorema.

Teorema 7.13. *Sea p primo impar. Entonces* $(\frac{2}{p}) = \begin{cases} 1 \text{ si } \pm 1 \pmod 8 \\ -1 \text{ si } \pm 3 \pmod 8 \end{cases}$

Demostración. Por el lema de Gauss (7.11), tenemos que $(\frac{2}{p}) = (-1)^\mu$, siendo μ el número de elementos en $S = \{1{\cdot}2, 2{\cdot}2, ..., 2{\cdot}\frac{p-1}{2}\}$ que, al dividirlos entre p, sus restos son mayores a $\frac{p}{2}$. En el conjunto S, todos sus elementos son menores a p. Basta, por tanto, con ver qué sucede con los números que pasan de $\frac{p}{2}$. $\forall k \in \{1, ..., \frac{p-1}{2}\}$, tenemos que $2k < \frac{p}{2}$, lo que equivale a que $4k < p$. Sea [ ] la función entero. Tenemos un total de $[\frac{p}{4}]$ enteros menores a $\frac{p}{2}$ en S, por lo que $\mu = \frac{p-1}{2} - [\frac{p}{4}]$ son enteros mayores a $\frac{p}{2}$. Podemos reducir entonces a un total de cuatro posibilidades, siendo p primo impar de una de las siguientes formas:

$p = 8k + 1$: Entonces $\mu = 4k - [\frac{8k+1}{4}] = 4k - [2k + \frac{1}{4}] = 4k - 2k = 2k$.

$p = 8k + 3$: Entonces $\mu = 4k + 1 - [\frac{8k+3}{4}] = 4k - [2k + \frac{3}{4}] = 4k + 1 - 2k = 2k + 1$.

$p = 8k + 5$: Entonces $\mu = 4k + 2 - [\frac{8k+5}{4}] = 4k - [2k + 1 + \frac{1}{4}] = 4k + 2 - 2k - 1 = 2k + 1$.

$p = 8k + 7$: Entonces $\mu = 4k + 3 - [\frac{8k+7}{4}] = 4k - [2k + 1 + \frac{3}{4}] = 4k + 3 - 2k - 1 = 2k + 2$.

Por lo tanto, tenemos que si $p = 8k \pm 1$ ($8k + 7$ es lo mismo que $8(k + 1) - 1$, $k \in \mathbb{Z}$), entonces el elemento μ es par, por lo que $(\frac{2}{p}) = 1$, mientras que si $p = 8k \pm 3$, ($8k + 5$ es lo mismo que $8(k + 1) - 3$, $k \in \mathbb{Z}$), entonces μ es impar y $(\frac{2}{p}) = -1$. □

Tenemos, entonces, una forma rápida de ver si 2 es un resto cuadrático del primo impar p, de la siguiente forma:

Corolario 7.14. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

Demostración. Separamos los primos impares como arriba:

$p = 8k \pm 1$ Tenemos que $\frac{p^2-1}{8} = \frac{(8k\pm1)^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$, que es un entero par (por ser k entero). Por tanto, $(-1)^{\frac{p^2-1}{8}} = 1 = (\frac{2}{p})$.

$p = 8k \pm 3$ En este caso, $\frac{p^2-1}{8} = \frac{(8k\pm3)^2-1}{8} = \frac{64k^2\pm48k+8}{8} = 8k^2 \pm 6k + 1$, entero impar, con lo que tenemos $(-1)^{\frac{p^2-1}{8}} = -1 = (\frac{2}{p})$.

□

Por este resultado, tenemos entonces las siguientes propiedades de ± 2 en el conjunto de $\mathbb{Z}_p$.

Teorema 7.15. *Sea $p \in \mathbb{Z}$ un primo impar, y $2p+1$ otro primo impar. Entonces, $(-1)^{\frac{(p-1)}{2}} \cdot 2$ es raíz primitiva del primo $2p+1$.*

Demostración. Sea $q = 2p + 1$. Distinguimos dos casos:

$p \equiv 1 \pmod 4$ Entonces $(-1)^{\frac{p-1}{2}} \cdot 2 = 2$. $\varphi(q) = q - 1 = 2p$. Por tanto, el orden de 2 (mod q) es uno de los números 1, 2, p o $2p$. Por (7.8), tenemos $(\frac{2}{p}) \equiv 2^{\frac{q-1}{2}} = 2^p \pmod q$. En este caso, tenemos $q \equiv 3 \pmod 8$, es decir, $(\frac{2}{q}) = -1$ por teorema anterior, tenemos que $2^p \equiv -1 \pmod q$, por lo que 2 no puede tener orden p (mod q). Tampoco puede ser 1 o 2, pues $2^2 \equiv 1 \pmod q$ implica que $q \mid 3$, cosa imposible al ser $q \geq 7$ por definición de q. Por lo tanto, $ord_q\ 2 = 2p$, lo que hace que 2 sea raíz primitiva de q.

$p \equiv 3 \pmod 4$ $(-1)^{\frac{p-1}{2}} \cdot 2 = -2$, y $(-2)^p \equiv (\frac{-2}{q}) = (\frac{-1}{q})(\frac{2}{q}) \pmod q$. Tenemos en este caso que $q \equiv 7 \pmod 8$, tenemos que $(\frac{-1}{q}) = -1$ (7.10), por lo que $(\frac{2}{q}) = 1$, lo que implica que $(-2)^p \equiv 1 \pmod q$. Con esto, obtenemos un razonamiento análogo para ver que $ord_q\ (-2) = 2p$, por lo que -2 es raíz primitiva de q.

□

Observación 7.16. De esto, obtenemos que, si p y $4p+1$ son primos, entonces 2 es raíz primitiva de $4p+1$. Esto significa que 2 es raíz primitiva de infinitos primos de esta forma, como veremos a continuación.

Teorema 7.17 (Teorema de Euclides)**.** *Existe una cantidad infinita de números primos.*

Demostración. Supongamos que sólo existe una cantidad finita de primos p_1, ..., p_n, y tomemos el número $P = p_1...p_n + 1$. Por ser $P > 1$, entonces este número se puede dividir por un primo, llamémoslo p. Por ser p_1, ..., p_n los únicos primos, entonces p es igual a alguno de estos primos. Pero ese primo p también tiene que dividir $p_1...p_n$. Por ello, $p \mid p_1...p_n$, y $p \mid P$. Por lo tanto, $p \mid (P - p_1...p_n)$, por lo que $p \mid 1$, lo cual es absurdo al ser $p > 1$ por ser primo. En consecuencia, tiene que haber una cantidad infinita de números primos. □

Teorema 7.18. *Existen infinitos primos de forma $4k+1$.*

Demostración. Como hicimos antes, lo veremos por contradicción. Sean p_1, ...,p_n la cantidad de primos de esta forma, y sea $N = (2p_1...p_n)^2 + 1$. Por ser N impar, existe un primo impar p que divide a N. Dicho de otro modo, $(2p_1...p_n)^2 \equiv -1 \pmod{p}$. En términos del símbolo de Legendre, $(\frac{-1}{p}) = 1$, lo que es válido sólo con $p = 4k + 1$, con $k \in \mathbb{Z}$, y será uno de los descritos arriba. Por lo tanto, $p \mid N - (2p_1...p_n)^2$. Llegamos a que $p \mid 1$, lo que es una contradicción al ser todo número primo mayor a 1. Por lo tanto, hay una cantidad infinita de primos de la forma $4k + 1$. □

Acabaremos dando un adelanto del próximo capítulo con la siguiente tabla de valores del símbolo de Legendre $(\frac{p}{q})$ para primos impares p, $q \leq 23$. Obtenemos la siguiente tabla:

q↓ p→	3	5	7	11	13	17	19	23
3	0	-1	1	-1	1	-1	1	-1
5	-1	0	-1	1	-1	-1	1	-1
7	-1	-1	0	1	-1	-1	-1	1
11	1	1	-1	0	-1	-1	-1	1
13	1	-1	-1	-1	0	1	-1	1
17	-1	-1	-1	-1	1	0	1	-1
19	-1	1	-1	1	-1	1	0	1
23	1	-1	-1	-1	1	-1	-1	0

Clasificando estos números (mod 4), tenemos que

$\{5, 13, 17\} \in (1)_4$,

$\{3, 7, 11, 19, 23\} \in (3)_4$.

Podemos observar, por un lado, que si uno de los elementos de $(1)_4$ está involucrado, entonces $(\frac{p}{q}) = (\frac{q}{p})$. Se nota en el hecho de que la fila y la columna correspondiente a cada uno de estos elementos es igual, cosa que no pasa con los otros primos. De hecho, tomando 3 y 7, tenemos que $(\frac{3}{7}) = -1$, pero $(\frac{7}{3}) = 1$. Esto pasa siempre que p, $q \in (3)_4$. Por tanto, en este caso $(\frac{p}{q}) = -(\frac{q}{p})$. Esto lo acabamos de ver con p, $q \leq 23$. La razón por la cual se cumple esto la veremos en el siguiente capítulo, donde, además, la generalizaremos con cualquier par de primos impares p y q, con lo que tendremos, unido a lo que ya hemos descrito en este capítulo, una manera sencilla para ver qué números son restos cuadráticos de un módulo primo dado.

Capítulo 8

Ley de reciprocidad cuadrática.

En el capítulo anterior hemos dado algunos resultados del valor del símbolo de Legendre (mod p) para elementos $q \in \mathbb{Z}$ que sean primos (separando los impares del primo 2). Si describimos ahora el valor de $(\frac{a}{p})$ con $a \in \mathbb{Z}$ arbitrario, tenemos que (7.10) nos dice que el símbolo de Legendre es una función multiplicativa, y que sabemos como se definen $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ y $(\frac{a^2}{p}) = 1$ si $p \nmid a$ y $(\frac{a^2}{p}) = 0$ si $p \mid a$, nos queda evaluar el valor de $(\frac{q}{p})$ con $q \neq p$ primos impares.

8.1. La ley de reciprocidad cuadrática.

Al acabar el capítulo anterior vimos qué sucedía con primos ≤ 23. Esto se refleja y generaliza en el siguiente teorema.

Teorema 8.1 (Ley de reciprocidad cuadrática)**.** *Sean p, $q \in \mathbb{Z}$ primos impares positivos distintos. Entonces, tenemos* $\begin{cases} (\frac{p}{q}) = (\frac{q}{p}) \text{ si } p \text{ o } q \equiv 1 \pmod 4 \\ (\frac{p}{q}) = -(\frac{q}{p}) \text{ si } p, q \equiv -1 \pmod 4 \end{cases}$

Dicho de otro modo, $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Demostración. Por el lema de Gauss (7.11), tenemos dos enteros μ, ν de modo que $(\frac{q}{p}) = (-1)^{\mu}$, $(\frac{p}{q}) = (-1)^{\nu}$. Estos números son las cantidades de múltiplos que son los menores restos en valor absoluto de los conjuntos q, $2q$, ..., $(\frac{p-1}{2})q$ (mod p), y p, $2p$, ..., $(\frac{q-1}{2})p$ (mod q) que son negativos. Nos quedaría probar, entonces, que $\mu + \nu \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$.

Tomemos xq uno de esos múltiplos de q, siendo $x \in \mathbb{Z}$, $1 \leq x \leq \frac{(p-1)}{2}$. Eligiendo un y de modo que $-\frac{p}{2} < qx - py < \frac{p}{2}$, entonces $qx - py$ es el menor resto en valor absoluto de qx (mod p). De esta inecuación, encontramos que y está en un intervalo de longitud 1 de la siguiente forma: $\frac{qx}{p} - \frac{1}{2} < y < \frac{qx}{p} + \frac{1}{2}$.

De esta forma, tenemos un y único y no negativo; y en el caso de que sea $y = 0$, tendríamos que $qx - py = qx > 0$, y μ no contribuye nada. Además, tenemos que con $x \leq \frac{(p-1)}{2}$ se cumple $\frac{qx}{p} + \frac{1}{2} \leq \frac{q}{2} - \frac{q}{2p} + \frac{1}{2} < \frac{q+1}{2}$, por lo que podemos, sin pérdida de generalidad, restringir y al intervalo $0 < y \leq \frac{(q-1)}{2}$.

Por tanto, μ denota la cantidad de combinaciones de x e y de modo que los conjuntos $\mathcal{P} = \{1, 2, ..., \frac{p-1}{2}\}$ y $\mathcal{Q} = \{1, 2, ..., \frac{q-1}{2}\}$ cumplen $0 > qx - py > -\frac{p}{2}$. De forma análoga, tenemos que ν es la cantidad de pares $x \in \mathcal{P}$ e $y \in \mathcal{Q}$ para los cuales $0 > py - qx > -\frac{q}{2}$. Para cualquier otro par $x \in \mathcal{P}$, $y \in \mathcal{Q}$ que cumplan $py - qx > \frac{p}{2}$ o $py - qx < -\frac{q}{2}$, supongamos que hay λ casos del primero y ρ del segundo. Por lo tanto, tenemos que $\frac{p-1}{2} \cdot \frac{q-1}{2} = \mu + \nu + \lambda + \rho$.

Como $x \in \mathcal{P}$, $y \in \mathcal{Q}$, entonces los números $x' = \frac{p+1}{2} - x$ e $y' = \frac{q+1}{2} - y$ se mueven en los mismos conjuntos que x e y, pero en orden contrario. Si $py - qx > \frac{p}{2}$, entonces $py' - qx' = p(\frac{q+1}{2} - y) - q(\frac{p+1}{2} - x) = \frac{p-q}{2} - (py - qx) < \frac{p-q}{2} - \frac{p}{2} = -\frac{q}{2}$.Análogamente, si $py - qx < -\frac{q}{2}$, tenemos que $py' - qx' > \frac{p}{2}$. Por tanto, tenemos que $\lambda = \rho$, y, en consecuencia, $\frac{p-1}{2} \cdot \frac{q-1}{2} = \mu + \nu + 2\lambda \equiv \mu + \nu \pmod 2$. □

Corolario 8.2. *Si p, q primos impares distintos, entonces*

$$(\tfrac{p}{q})(\tfrac{q}{p}) = \begin{cases} 1 \text{ si } p \equiv 1 \pmod 4 \text{ o } q \equiv 1 \pmod 4 \\ -1 \text{ si } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Demostración. $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$ par $\Leftrightarrow$ p o q es de forma $4k+1$. Por otro lado, si ambos son de forma $4k+3$, entonces $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$ impar. □

Con esto, siendo p, $q \in \mathbb{Z}$ primos impares distintos, y sabiendo que $(\frac{q}{p})^2 = 1$, entonces que tenemos que $(\frac{p}{q}) = \begin{cases} (\frac{q}{p}) \text{ si } p \equiv 1 \pmod 4 \text{ o } q \equiv 1 \pmod 4 \\ -(\frac{q}{p}) \text{ si } p \equiv q \equiv 3 \pmod 4. \end{cases}$

Tomando, ahora, la ley de reciprocidad cuadrática vista antes, junto con las propiedades del símbolo de Legendre (7.10), entonces es fácil ver el valor de $(\frac{q}{p})$, con p primo, que nos dirá si q es resto cuadrático de p.

Ejemplo 8.3. Veamos si 2819 es un resto cuadrático de 4177. Ambos son primos, y $4177 \equiv 1 \pmod 4$. Por tanto, tenemos $(\frac{2819}{4177}) = (\frac{4177}{2819}) = (\frac{1358}{2819}) = (\frac{2 \cdot 7 \cdot 97}{2819}) = (\frac{2}{2819})(\frac{7}{2819})(\frac{97}{2819}) = -1 \cdot -(\frac{2819}{7})(\frac{2819}{97}) = (\frac{5}{7})(\frac{6}{97}) = (\frac{2}{5})(\frac{1}{3}) = -1$, por lo que 2819 no es resto cuadrático de 4177.

Además de esto, la ley de reciprocidad cuadrática se puede utilizar también para determinar los primos p de los cuales un primo dado q es un resto cuadrático. Esto se observa en el siguiente teorema.

Teorema 8.4. *Sea $q \in \mathbb{Z}$ un primo impar positivo fijado, y sea $p \in \mathbb{Z}$ primo impar positivo distinto de q. Todo primo p tiene una representación de dos formas*

$p = 4qk \pm a$ con $k \in \mathbb{Z}$ y $0 < a < 4q$ con $a \equiv 1$ (mod 4). (1)

Si esto es válido, entonces

$(\frac{q}{p}) = (\frac{a}{q})$. *(2)*

Así, los p para los cuales $(\frac{q}{p}) = 1$ son aquellos $p \equiv \pm a$ (mod 4q) $\forall a$ que cumpla $0 < a < 4q$, $a \equiv 1$ *(mod 4) y* $(\frac{a}{q}) = 1$. *(3)*

Los a que cumplen esto último vienen dados por el menor resto positivo (mod 4q) de los cuadrados impares 1^2, 3^2, ..., $(q-2)^2$.

Demostración. Por el teorema de división, $\exists^o k'$, a' de manera que $p = 4qk' + a'$, cumpliendo $1 \leq a' < 4q$, y siendo a' impar. Si $a' \equiv 1 \pmod 4$, entonces (1) vale con el signo $+$, y siendo $k = k'$, $a = a'$. En el caso $a' \equiv -1 \pmod 4$, entonces es válido con el signo $-$ y siendo $k = k' + 1$ y $a = 4q - a'$. Cualquier otro valor de k, además de k' y $k' + 1$ debe dar $|a| > 4q$.

Para (2), supongamos primero que lo anterior es cierto con el signo $+$. En este caso, $p \equiv 1 \pmod 4$ y $p \equiv a \pmod q$, por lo que $(\frac{q}{p}) = (\frac{p}{q}) = (\frac{a}{q})$. Si se cumple con el signo $-$, $p \equiv -1 \pmod 4$ y $p \equiv -a \pmod q$, por lo que $q \equiv -1 \pmod 4$, y entonces $(\frac{q}{p}) = -(\frac{p}{q}) = -(\frac{-a}{q}) = (\frac{a}{q})$, o bien $q \equiv 1 \pmod 4$ y $(\frac{q}{p}) = (\frac{p}{q}) = (\frac{-a}{q}) = (\frac{a}{q})$.

Para terminar, tenemos que si $(\frac{a}{q}) = 1$, se cumple que $\exists b$ de modo que $a \equiv b^2 \pmod q$ y $1 \leq b \leq q - 1$, de donde tenemos que $a \equiv (q-b)^2 \pmod q$ y $1 \leq q - b \leq q - 1$. Sea b' el entero impar entre b y $q - b$ (al ser q primo impar, esto es cierto). Tenemos que $a \equiv b'^2 \pmod q$, $1 \leq b' \leq q - 2$, y b' impar por lo visto antes. En ese caso, $a \equiv 1 \equiv b'^2 \pmod 4$, por lo que $a \equiv b'^2 \pmod{4q}$. □

Ilustraremos esto con los siguientes ejemplos.

Ejemplo 8.5. Tomemos $q = 3$. El único entero a que cumple $0 < a < 4 \cdot 3 = 12$, cumpliendo $a \equiv 1 \pmod 4$ y $(\frac{a}{3}) = 1$ es $a = 1$. Por tanto, 3 será un resto cuadrático de los primos $12k \pm 1$. Todo otro número impar es de forma $12k \pm 3$, que no son primos (todos son divisibles entre 3) o $12k \pm 5$. Por lo tanto, tenemos que $(\frac{3}{p})$ se determina de este modo, y tenemos, entonces, que se cumple $(\frac{3}{p}) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \pmod{12} \\ -1 \text{ si } p \equiv \pm 5 \pmod{12} \end{cases}$

Ejemplo 8.6. Tenemos algo semejante con $q = 17$. Tenemos los cuadrados impares 1^2, 3^2, 5^2, 7^2, 9^2, 11^2, 13^2, 15^2. $4q = 4 \cdot 17 = 68$, que es el módulo al que reducimos estos números. Tenemos, entonces, los siguientes números: $1, 9, 25, 49, 13, 53, 33, 21$. Por lo tanto, cumpliendo $a \equiv 1 \pmod 4$, tenemos que 17 va ser resto cuadrático de los primos de forma $68k \pm 1, 9, 13, 21, 25, 33, 49, 53$; y un no resto cuadrático de los primos de forma $68k \pm 5, 29, 37, 41, 45, 57, 61, 65$.

El propio 17 es el único primo de la forma $68k \pm 17$.

Vistos estos ejemplos, podemos dar una explicación general de lo que sucede.

Observación 8.7. Tenemos en general que, de las $2q$ progresiones de tipo $4qk \pm a$, exactamente $q-1 = \frac{1}{2}\varphi(4q)$ contienen sólo primos de los cuales q es un resto cuadrático, otras $q-1$ contienen sólo primos de los cuales q no es resto cuadrático, y 2 (tanto $4qk \pm q$ o $4qk \pm 3q$, dependiendo de si $q \equiv 1$ o $3 \pmod 4$) no tienen primos distintos al propio q.

Ejemplo 8.8. Tomemos en esta ocasión $q = 5$. Tenemos que $4 \cdot 5 = 20$, que será de donde partamos para ver los primos de los que 5 es resto cuadrático. Tenemos que $1^2 = 1$ y $3^2 = 9$, que no hace falta reducir en módulo 20. Por lo tanto, tenemos que 5 es resto cuadrático de los primos de forma $20k \pm 1$, 9; mientras que no lo será con los primos de forma $20k \pm 13$, 17. Notar que, con $20k \pm 5$, el propio $q = 5$ es el único primo en la progresión.

Por otro lado, determinar los primos de los cuales un número compuesto es un resto cuadrático resulta más complicado. La condición necesaria es que el producto de símbolos de Legendre de los distintos factores que forman al número compuesto en cuestión den como resultado 1.

Ejemplo 8.9. Buscaremos los primos p de los cuales 6 es un resto cuadrático, es decir, los primos p que cumplen $(\frac{6}{p}) = 1$. En este caso, necesita cumplirse que $(\frac{2}{p}) = (\frac{3}{p}) = 1$ o bien que $(\frac{2}{p}) = (\frac{3}{p}) = -1$. Por lo tanto, necesitamos que se cumplan a la vez

$$p \equiv \pm 1 \pmod 8,\ p \equiv \pm 1 \pmod{12}$$

o bien

$$p \equiv \pm 3 \pmod 8,\ p \equiv \pm 5 \pmod{12}$$

siendo válidas todas las combinaciones de signos.

Tenemos, entonces, los siguientes pares simultáneos posibles

$p \equiv 1 \pmod 8$	$p \equiv -1 \pmod 8$	$p \equiv 1 \pmod 8$	$p \equiv -1 \pmod 8$
$p \equiv 1 \pmod{12}$	$p \equiv -1 \pmod{12}$	$p \equiv -1 \pmod{12}$	$p \equiv 1 \pmod{12}$
$p \equiv 3 \pmod 8$	$p \equiv -3 \pmod 8$	$p \equiv 3 \pmod 8$	$p \equiv -3 \pmod 8$
$p \equiv 5 \pmod{12}$	$p \equiv -5 \pmod{12}$	$p \equiv -5 \pmod{12}$	$p \equiv 5 \pmod{12}$

Cuatro de estos pares son inconsistentes, mientras que los otros tienen como soluciones $p \equiv \pm 1, \pm 5 \pmod{24}$. En estos casos, $(\frac{6}{p}) = 1$. Por otro lado, si $p \equiv \pm 7, \pm 11 \pmod{24}$, entonces $(\frac{6}{p}) = -1$. Con esto tenemos la solución, pues al ser $\varphi(24) = 8$, sólo 8 clases de restos (mod 24) contienen números primos.

8.2. Congruencias cuadráticas con módulos compuestos

Con el valor del símbolo de Legendre antes descrito, tenemos cuando $a \in \mathbb{Z}_p$ es un resto cuadrático con un módulo p primo impar. Partiendo de esto, podemos analizar, con este símbolo, cuando un valor $a \in \mathbb{Z}_m$ es resto cuadrático de $m \in \mathbb{Z}$ módulo compuesto. Veremos primero el caso de $m = p^n$, $n \geq 1$.

Teorema 8.10. *Sea p un número primo impar y sea $a \in \mathbb{Z}$ tal que mcd(a, p)= 1. Entonces, $x^2 \equiv a \pmod{p^n}$, $n \geq 1$ tiene solución $\Leftrightarrow (\frac{a}{p}) = 1$.*

Demostración. Demostraremos las dos implicaciones:

"$\Rightarrow$"

$x^2 \equiv a \pmod{p^n}$ con solución $\Rightarrow x^2 \equiv a \pmod{p}$ con solución (pues $p^n \mid x^2 - a$ implica que $p \mid x^2 - a$). Por lo tanto, $(\frac{a}{p}) = 1$.

"$\Leftarrow$"

Sea $(\frac{a}{p}) = 1$. Probaremos que $x^2 \equiv a \pmod{p^n}$ es resoluble por inducción. Si $n = 1$, no hay que probar nada (Por hipótesis, se cumple). Supongamos que es válido para $n = k \geq 1$, por lo que $x^2 \equiv a \pmod{p^k}$ admite solución x_0. En este caso, $x_0^2 = a + bp^k$, con $b \in \mathbb{Z}$. Para pasar de k a $k + 1$, usaremos x_0 y b para dar solución de $x^2 \equiv a \pmod{p^{k+1}}$. Resolvemos $2x_0 y \equiv -b \pmod{p}$, obteniendo solución $y_0 \pmod{p}$ única (mcd$(2x_0, p)$= 1). Elevando al cuadrado, tenemos entonces que $(x_0 + y_0 p^k)^2 = x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k} = a + (b + 2x_0 y_0)p^k + y_0^2 p^{2k}$. Pero $p \mid b + 2x_0 y_0$, de lo que tenemos que $x_1^2 \equiv (x_0 + y_0 p^k)^2 \equiv a \pmod{p^{k+1}}$. Así, $x^2 \equiv a \pmod{p^n}$ con solución siendo $n = k + 1$. Por inducción, esto vale $\forall n \in \mathbb{Z}^+$. □

Ya sabemos, entonces, que todos los restos cuadráticos de una potencia de un número primo impar son restos cuadráticos del propio número. Veamos, ahora, qué sucede con el primo restante, $p = 2$. Tenemos el siguiente resultado:

Teorema 8.11. *Sea $a \in \mathbb{Z}$ impar. Tenemos:*

a) $x^2 \equiv a \pmod{2}$ siempre es resoluble.

b) $x^2 \equiv a \pmod{4}$ con solución $\Leftrightarrow a \equiv 1 \pmod{4}$.

c) $x^2 \equiv a \pmod{2^n}$, con $n \geq 3$, tiene solución $\Leftrightarrow a \equiv 1 \pmod{8}$.

Demostración. Probamos los distintos apartados:

a) Trivial, pues $\forall a$ impar, $a \equiv 1 \pmod{2}$.

b) Partimos de que todo cuadrado de un entero impar es congruente con 1 (mod 4). Por ello, $x^2 \equiv a \pmod 4$ resoluble con $a = 4k + 1$, con $k \in \mathbb{Z}$. En este caso hay dos soluciones (mod 4): $x = 1$ y $x = 3$.

c) $n \geq 3$. Partimos del hecho de que todo entero impar elevado al cuadrado es congruente a 1 (mod 8), y se ve que $x^2 \equiv a \pmod{2^n}$ resoluble si $8k + 1 = a$. Para la otra implicación, basta con aplicar (5.12) para ver que hay una solución $x_1 \pmod{2^{n+1}}$ a partir de la solución $x_0 \pmod{2^n}$. Por tanto, esto es válido para todo $n \geq 3$.

□

Tenemos, entonces, que podemos adaptar (7.4) para el símbolo de Legendre.

Teorema 8.12. *Sea $m = 2^{k_0} p_1^{k_1} ... p_r^{k_r}$ factorización en primos de $m > 1$, y sea $a \in \mathbb{Z}$ de modo que mcd(a, m)= 1. Entonces, $x^2 \equiv a \pmod m$ resoluble si, y sólo si, $(\frac{a}{p_i}) = 1$, siendo $i \in \{1, ..., r\}$ y $a \equiv 1 \pmod 4$ si $4 \parallel m$, o $a \equiv 1 \pmod 8$ si $8 \mid m$.*

Notar que todos estos resultados son, como vimos en capítulos anteriores, para los elementos $a \in \mathbb{U}_m$, con $m > 1$. Es este grupo el que se separa en restos cuadráticos y no restos cuadráticos.

Al trabajar con el conjunto de unidades (mod m), podemos ver que las raíces primitivas no pueden ser raíces cuadráticas, ni al revés. Por tanto, las raíces cuadráticas (mod m) son un conjunto de las unidades disjunto al conjunto de raíces primitivas. Por ello, si un elemento $a \in \mathbb{U}_m$ es raíz primitiva de m, entonces $(\frac{a}{p}) = -1$, pero no sucede al revés. Por ejemplo, tenemos que 2 es raíz primitiva de 13, y también es cierto que $(\frac{2}{13}) = (-1)^{\frac{13^2-1}{8}} = (-1)^{21} = -1$. Por otro lado, sabemos que $(\frac{11}{13}) = (\frac{13}{11}) = (\frac{2}{11}) = (-1)^{15} = -1$, pero no es una raíz primitiva de 13, pues $7^3 \equiv 11 \pmod{13}$, por lo que $< 11 > \neq \mathbb{U}_{13}$.

Lista de símbolos

$>$	mayor que
$\geq$	mayor o igual que
$<$	menor que
$\leq$	menor o igual que
$=$	igual
$\neq$	distinto
$\in$	pertenece
$\subset$	contenido en
$\mid$	divide a
$\nmid$	no divide a
$\equiv$	congruente
$\Leftrightarrow$	equivalente; si y sólo si
$\Rightarrow$	implicación a la derecha
$\Leftarrow$	implicación a la izquierda
$\cdot$	producto
$\forall$	para todo
mcm	mínimo común múltiplo
mcd	máximo común divisor
!	factorial
$\exists$	existe
$\nexists$	no existe
$^{\text{o}}$	único
φ	función de Euler
$\sum$	sumatorio
$< a >$	subgrupo multiplicativo generado por $a \in \mathbb{U}_m$
ord_m	orden en módulo m
/	tal que

$\|$	p-componente
∂	grado del polinomio
$\surd$	raíz cuadrada
f	polinomio
f'	derivada
$(\frac{a}{p})$	símbolo de Legendre
$\binom{p}{s}$	combinatorio: $\binom{p}{s} = \frac{p!}{s!(p-s)!}$
ind_g	índice de un elemento con respecto a la raíz primitiva g
log	logaritmo
$[\ ]$	función entero
$\mathbb{Z}$	anillo de enteros
$\mathbb{Z}_m$	grupo aditivo de clases (mod m)
$\mathbb{Z}^+$	enteros positivos
$\mathbb{Z}_m^*$	elementos de $\mathbb{Z}_m$ sin el 0
$\mathbb{U}_m$	conjunto de unidades (mod m)
$\mathbb{Z}[x]$	anillo de polinomios con coeficientes enteros
$\mathbb{Z}_m[x]$	anillo de polinomios con coeficientes en $\mathbb{Z}_m$
$\mathbb{U}_m^{(n)}$	grupo de restos n-potenciales de $\mathbb{U}_m$
$\times$	producto directo
$\oplus$	suma directa

Glosario

Bibliografía

[1] LeVeque, William J., *Fundamentals Of Number Theory*, Addison-Wesley, 1977.

[2] Burton, David M., *Elementary Number Theory*, 6th ed., McGraw-Hill , 2007.

[3] Adams, William W. and Goldstein, Larry J., *Introduction To Number Theory*, Prentice-Hall, 1976.

[4] Baker, Alan, *A Concise Introduction to the Theory of Numbers*, Cambrige University Press, 1984.