UNIVERSIDAD DE SEVILLA

FACULTAD DE MATEMÁTICAS

DEPARTAMENTO DE ÁLGEBRA

DOBLE GRADO EN MATEMÁTICAS Y ESTADÍSTICA

LEYES DE RECIPROCIDAD (CUATRO DEMOSTRACIONES DE LA LEY DE RECIPROCIDAD CUADRÁTICA)

TRABAJO DE FIN DE GRADO

Autor: Eric Sevillano Castellano
Tutor: Dr. José María Tornero Sánchez

Sevilla-España
2017-2018

Eric Sevillano Castellano

LEYES DE RECIPROCIDAD

CUATRO DEMOSTRACIONES DE LA LEY DE RECIPROCIDAD CUADRÁTICA

UNIVERSIDAD DE SEVILLA

FACULTAD DE MATEMÁTICAS

DEPARTAMENTO DE ÁLGEBRA

Índice general

Resumen

A lo largo del siguiente trabajo vamos a profundizar en los contenidos impartidos en la asignatura **Estructuras Algebraicas** para explicar la *Ley de Reciprocidad Cuadrática* así como sus aplicaciones para la **Teoría Algebraica de Números**. Además existen otras *Leyes de Reciprocidad* como la *Leyes de Reciprocidad Cúbica, Bicuadrática, de Einsentein,...* entre otras, las cuales no estudiaremos en nuestro trabajo por falta de espacio.

- Durante el primer capítulo se explicarán conceptos acerca de la estructura de grupo de $U(\mathbb{Z}/\mathbb{Z}n)$ así como el concepto de *residuos de la n-ésima potencia* para averiguar para qué primos p se puede resolver la congruencia $x^n \equiv a \pmod{p}$ dado un a fijo.

En el resto de nuestro trabajo se dividirá en cuatro capítulos. En cada uno de ellos se dará una demostración la *Ley de Reciprocidad Cuadrática* (de las muchas que existen) usando en cada uno herramientas distintas:

- El segundo capítulo, además de enunciarla, hará uso de los residuos cuadráticos definiendo el concepto del *símbolo de Legendre* y posteriormente su generalización, el *símbolo de Jacobi*.
- En el tercer capítulo haremos uso del concepto de las *sumas cuadráticas de Gauss*, definiendo para ello los *números algebraicos* y los *enteros algebraicos* y estudiando las propiedades que cumplen, necesarias para llevar a cabo la demostración.
- El cuarto capítulo pasa a un enfoque completamente diferente usando para ello los *cuerpos finitos* así como sus propiedades y la existencia de un cuerpo con p^n elementos para todo p primo y para todo n natural.
- En el quinto y último capítulo de este trabajo volvemos a lo usado en el tercer capítulo y extendemos las *sumas de Gauss* a las conocidas como *sumas de Jacobi* para las cuales es necesario definir el concepto de *carácter multiplicativo*. Estas sumas, además de ser más potentes y complejas, tienen la ventaja de que se pueden usar para demostrar reciprocidades de orden superior.

El origen de este trabajo viene del proyecto como alumno interno del **Departamento de Álgebra** de la *Universidad de Sevilla* realizado en el curso académico anterior cuyo tema principal fue el *Algoritmo de Shanks*, el cual, aunque es probabilístico, es muy eficiente. Consiste en, dados un primo impar p y entero a, encontrar un número x (si existe) tal que $x^2 \equiv a \pmod{p}$. Para ello, primero calculamos el número impar q que cumple que $p - 1 = 2^e \cdot q$ y, por otro lado, elegimos aleatoriamente un número n tal que $\left(\frac{n}{p}\right) = -1$ (lo cual tiene una probabilidad cercana a $\frac{1}{2}$, por lo que se obtendrá algún n satisfactorio tras pocos intentos). Con esos datos, se inicia un proceso iterativo, el cual es finito, pudiendo acabar o bien dando un valor para x o bien diciendo que a no es un residuo cuadrático módulo p. En este trabajo se usaron las referencias bibliográficas [1], [2], [5] y [7]. Este proyecto, sin embargo, se basa en gran medida en la referencia [4] aunque se apoya también en las referencias [3] y [6].

Por otro lado, esta memoria forma parte de uno más grande que tratará sobre las *Leyes de Reciprocidad de órdenes superiores* y que se realizó como proyecto de becario de colaboración y alumno interno para el **Departamento de Álgebra** de la *Universidad de Sevilla* para el curso académico actual. Ambos formarán un trabajo completo y extenso sobre las *Leyes de Reciprocidad*.

Dicho proyecto complementario se dividirá en dos capítulos explicando en cada uno las *Leyes de Reciprocidad Cúbica y Bicuadrática*, respectivamente:

- En el primer capítulo definiremos al *anillo* $\mathbb{Z}[\omega]$ haciendo uso de las raíces cúbicas de la unidad y del *símbolo residual cúbico* (análogo a los *símbolo de Legendre y Jacobi* visto en capítulos anteriores). Realizaremos dos demostraciones: una análoga a la del tercer capítulo y la otra a la del quinto capítulo, haciendo uso de las *sumas de Gauss y de Jacobi cúbicas* para demostrar la *Ley de Reciprocidad Cúbica*.
- El segundo capítulo se centrará en la *Ley de Reciprocidad Bicuadrática* debiendo definir, análogamente al apartado anterior, el *anillo* $\mathbb{Z}[i]$, también conocidos como *enteros gaussianos* además del correspondiente *símbolo residual cuártico* para poder llegar a la demostración satisfactoriamente.

Abstract

Along this project we are going to delve into the concepts introduced in the course **Algebraic Structures** in order to explain the *Law of Quadratic Reciprocity* as well as its applications in **Algebraic Number Theory**. Furthermore, there are others *Laws of Reciprocity* as the *Cubic, Biquadratic, Einsentein Reciprocity Law* among others, which will not be treated in this project due to lack of space.

- At the first chapter we are going to explain the structure of $U(\mathbb{Z}/\mathbb{Z}n)$ as well as the notion of *nth power residues* in order to solve for which primes p the congruence $x^n \equiv a \pmod{p}$ is solvable for some fixed $a \in \mathbb{Z}$.

The rest of our project will split up in four chapters. In each of them we will give a proof of the *Law of Quadratic Reciprocity* (among all those that exist) using differents tools in each of them:

- The second chapter makes use of the quadratic residues defining the concept of the *Legendre symbol* and its generalization, the *Jacobi symbol*.
- At the third chapter we make use of the notion of *quadratic Gauss sums*, defining concepts such as *algebraic numbers* and *algebraic integers*.
- The fourth chapter changes to a completely different point of view using *finite fields*. We prove the existence of a field of p^n elements for all primes p and for all natural n.
- At the fifth and last chapter of this project we return to the third chapter's topics, and we extend the *Gauss sums* to the well-known *Jacobi sums*, for which is necessary to define the concept of *multiplicative character*. Not only these sums are more powerful and trickier, but they have the advantage that they can be really useful to show reciprocities of higher order.

The origin of this disertation comes from the project as intern student for the **Department of Algebra** of the *University of Sevilla* in the former academic year whose subject was *Shanks' Algorithm*, which is very efficient even though it is probabilistic,. It consists of, given an odd prime p and an integer a, finding a number x (if it exists) such that $x^2 \equiv a \pmod{p}$. For that, first we have to calculate a odd number q such that $p - 1 = 2^e \cdot q$ and, additionally, we choose randomly a number n such that $\left(\frac{n}{p}\right) = -1$ (whose probability is almost $\frac{1}{2}$, so we can find one after a few tries). With these data, we initialize an iterative process, which is finite, because it gives a value for x or saying that a is a non-residue quadratic modulo p. In this project we used the bibliographic references [1], [2], [5] and [7]. The current project, however, is mainly based on the reference [4] although it is supported also on the references [3] and [6].

On the other hand, this memoir is part of another bigger one which addresses the *Laws of Reciprocity of higher orders* which was undertaken as an intern student for the **Department of Algebra** of the *University of Sevilla* for the current academic year. Both take part of complete and extensive project about *Laws of Reciprocity*.

That complementary work is composed of two chapters, explaining the *Law of Cubic and Biquadratic Reciprocity*, respectively:

- At the first chapter we define the *ring* $\mathbb{Z}[\omega]$ making use of the cubic roots of the unity and the *cubic residue symbol* (analogous to the *Legendre and Jacobi symbol* we have seen in previous chapters). It contains two proofs: one similar to the one we have seen in the third and fifth chapters of the main project, making use of the *cubic Gauss and Jacobi sums* in order to prove the *Law of Cubic Reciprocity*.
- The second chapter we focus on the *Law of Biquadratic Reciprocity*, for which we have to define the *ring* $\mathbb{Z}[i]$ which is well-known as the *Gaussian integers*, in addition to the corresponding *quartic residue symbol* in order to achieve the proof satisfactorily.

Conceptos y propiedades básicas

Antes de empezar este trabajo es necesario enunciar algunos teoremas muy recurrentes a lo largo de todo el trabajo así como establecer algunas notaciones.

Notación 1 *Sean a, b, m enteros tales que a es congruente con b módulo m. La representación que usaremos en el trabajo para ello es la siguiente:*

$$a \equiv b \ \ (m).$$

Teorema 0.1 (Teorema Chino del Resto) *Sea $m \in \mathbb{Z}_{>0}$ y supongamos que $m = m_1 m_2 \cdots m_t$ y $\gcd(m_i, m_j) = 1$, para todo $i \neq j$. Sean b_1, b_2, $\ldots$, b_t enteros y consideremos el sistema de congruencias:*

$$\begin{cases} x \equiv & b_1 \ \ (m_1) \\ x \equiv & b_2 \ \ (m_2) \\ & \vdots \\ x \equiv & b_t \ \ (m_t) \end{cases}$$

Este sistema tiene siempre solución en $\mathbb{Z}$ y cualquier par de soluciones difiere en un múltiplo de m.

También existe una versión del mismo para anillos (que es la que nos será realmente útil en nuestro trabajo) que se puede enunciar brevemente como sigue:

$$\mathbb{Z}/\mathbb{Z}m \approx \mathbb{Z}/\mathbb{Z}m_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}m_t$$

Teorema 0.2 (Pequeño Teorema de Fermat) *Sea p un número primo y $a > 0$ un número natural. Entonces se tiene que:*

$$a^p \equiv a \ \ (p).$$

Equivalentemente, sea p un número primo y $a > 0$ un número natural tal que $\gcd(a, p) = 1$. Entonces se tiene que:

$$a^{p-1} \equiv 1 \ \ (p).$$

Teorema 0.3 (Fórmula de Inversión de Möbius) *Sea f una función de compleja definida sobre $\mathbb{Z}_{>0}$ y μ la función de Möbius definida en $\mathbb{Z}_{>0}$, cuyos valores son los siguientes:*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ contiene algún cuadrado} \\ (-1)^l & \text{si } n = p_1 p_2 \cdots p_l \text{ donde los } p_i \text{ son primos distintos y positivos} \end{cases}$$

Sea $F(n) = \sum_{d|n} f(d)$. Entonces se tiene que

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Corolario 0.1 *Sabiendo que $\phi(n)$ es la función que nos dice la cantidad de números naturales menores que n que son coprimos con n se tiene que*

$$\phi(d) = \sum_{c|d} \mu(c)\frac{d}{c}.$$

Teorema 0.4 (Teorema de Dirichlet para sucesiones aritméticas) *Sean a, $d \in \mathbb{Z}$ tales que $\gcd(a, d) = 1$. Entonces la progresión aritmética definida por $a_n = a+nd$ contiene infinitos números primos.*

Definición 0.1 *Sean a, $n \in \mathbb{Z}$ y $\gcd(a, n) = 1$. Diremos que el orden de a módulo n es el orden de $\overline{a} = a + \mathbb{Z}n$ en el grupo $U(\mathbb{Z}/\mathbb{Z}n)$.*

Definición 0.2 *Sea R un dominio de integridad. Se dice que es un Dominio Euclídeo si hay una función λ que va de los elementos no nulos de R al conjunto $\{0, 1, 2, 3, \dots, \}$ tal que si a, $b \in R$, $b \neq 0$, $\exists c$, $d \in R$ con las propiedades:*

1. *$a = cb + d$.*
2. *$d = 0$ o bien $\lambda(d) < \lambda(b)$.*

Definición 0.3 *Todo dominio euclídeo es un dominio de ideales principales y en particular verifica la identidad de Bézout.*

Definición 0.4 *Un cuerpo K es una extensión del cuerpo k si k es un subcuerpo de K. En dicho caso se notará K/k.*

Definición 0.5 *Sea k un cuerpo y K un extensión de k. A la dimensión de K como k-espacio vectorial la llamaremos grado de la extensión, la cual notaremos de la forma:*

$$[K : k] = dim_k\ K$$

Cuando ésta es finita se dirá que la extensión K/k es una extensión finita.

Capítulo 1

Introducción

Asumimos todos los conceptos y propiedades básicas aprendidas en la asignatura de **Estructuras Algebraicas**, y vamos a definir otros necesarios para poder explicar adecuadamente el tema principal de nuestro trabajo.

1.1. Raíces primitivas y estructura de grupo de $U(\mathbb{Z}/\mathbb{Z}n)$

Si $n = \prod_{i=1}^{l} p_i^{a_i}$, sabemos por el **Teorema Chino del Resto** (0.1) que

$$U(\mathbb{Z}/\mathbb{Z}n) \approx U(\mathbb{Z}/\mathbb{Z}p_1^{a_1}) \times \cdots \times U(\mathbb{Z}/\mathbb{Z}p_l^{a_l}).$$

Por lo tanto, para determinar la estructura de $U(\mathbb{Z}/\mathbb{Z}n)$ es suficiente considerar el caso de $U(\mathbb{Z}/\mathbb{Z}p^a)$ con p primo. Empezaremos considerando el caso $U(\mathbb{Z}/\mathbb{Z}p)$.

Dado que $\mathbb{Z}/\mathbb{Z}p$ es un cuerpo, nos será útil el siguiente lema:

Lema 1.1 *Sea $f(x) \neq 0 \in k[x]$ donde k es un cuerpo. Supongamos que $deg(f) = n$, entonces f tiene a lo sumo n raíces distintas.*

Corolario 1.1 *Sean $f(x), g(x) \in k[x]$ y $deg(f) = deg(g) = n$. Si $f(\alpha_i) = g(\alpha_i)$ para $n+1$ valores distintos $\alpha_1, \ldots, \alpha_{n+1}$. Entonces, $f(x) = g(x)$.*

Demostración:

Aplicar el **Lema 1.1** para el polinomio $f(x) - g(x)$. □

Proposición 1.1.1

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \ \ (p)$$

Demostración:

Si $\overline{a}$ denota la clase residual de a en $\mathbb{Z}/\mathbb{Z}p$, una forma equivalente de expresar esta proposición es

$$x^{p-1} - \overline{1} = (x-\overline{1})(x-\overline{2})\ldots(x-(\overline{p-1}))$$

en $\mathbb{Z}/\mathbb{Z}p[x]$. Sea

$$f(x) = (x^{p-1} - \overline{1}) - (x-\overline{1})(x-\overline{2})\ldots(x-(\overline{p-1})).$$

Entonces $f(x)$ tiene grado menor que $p-1$ (dado que el término líder se cancela) y tiene $p-1$ raíces $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ (por el **Pequeño Teorema de Fermat** (0.2)) por lo que $f = 0$. □

Corolario 1.2 *En las condiciones anteriores:*

$$(p-1)! \equiv -1 \ \ (p)$$

Demostración:

Esta demostración se consigue sustituyendo $x = 0$ en la **Proposición 1.1.1**. □

Este resultado es conocido como Teorema de Wilson. Es fácil probar que si $n > 4$ no es primo entonces $(n-1)! \equiv 0 \ \ (n)$.

Por lo tanto, la congruencia $(n-1)! \equiv -1 \ \ (n)$ es característica de los primos. Usaremos el Teorema de Wilson más adelante cuando hablemos de los residuos cuadráticos.

Proposición 1.1.2 *Si $d \mid (p-1)$, entonces $x^d \equiv 1 \ \ (p)$ tiene exactamente d soluciones.*

Demostración:

Sea $dd' = p-1$. En $\mathbb{Z}[x]$ se tiene la siguiente expresión:

$$\frac{x^{p-1}-1}{x^d-1} = \frac{(x^d)^{d'}-1}{x^d-1} = (x^d)^{d'-1} + (x^d)^{d'-2} + \cdots + x^d + 1 = g(x)$$

Por tanto,

$$x^{p-1} - 1 = (x^d - 1)g(x) \text{ en } \mathbb{Z}[x]$$

y

$$x^{p-1} - \overline{1} = (x^d - \overline{1})\overline{g}(x) \text{ en } \mathbb{Z}/\mathbb{Z}p[x]$$

Si $x^d - \overline{1}$ tuviera menos de d raíces por el **Lema 1.1** se tiene que el término de la derecha tendría menos de $p-1$ raíces. Sin embargo, el término de la izquierda tiene $p-1$ raíces: $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ por lo que $x^d \equiv 1 \ \ (p)$ tiene exactamente d raíces como queríamos probar. □

Teorema 1.1 *$U(\mathbb{Z}/\mathbb{Z}p)$ es un grupo cíclico.*

Demostración:

Para $d \mid (p-1)$ sea $\psi(d)$ el número de elementos de $U(\mathbb{Z}/\mathbb{Z}p)$ de orden d. Por la **Proposición 1.1.2** vemos que los elementos de $U(\mathbb{Z}/\mathbb{Z}p)$ que satisfacen $x^d \equiv 1 \ \ (p)$ forman un grupo de orden d. Por lo tanto, $\sum_{c|d} \psi(c) = d$. Aplicando la **Fórmula de Inversión de Möbius** (0.3) y su **corolario** (0.1), se obtiene

$$\psi(d) = \phi(d).$$

En particular, $\psi(p-1) = \phi(p-1)$, el cual es mayor que 1 si $p > 2$. Como el caso $p = 2$ es trivial, hemos probado que la existencia de un elemento (en realidad $\phi(d)$ elementos) de orden $p-1$ en todos los casos. □

A continuación se proporcionarán dos nuevas demostraciones de **Teorema 1.1** aunque antes debemos dar algunas definiciones adicionales.

Definición 1.1 *Un entero a es llamado una raíz primitiva módulo p si $\overline{a}$ genera el grupo $U(\mathbb{Z}/\mathbb{Z}p)$. Equivalentemente, a es una raíz primitiva módulo p si $p-1$ es el menor entero positivo tal que $a^{p-1} \equiv 1 \ \ (p)$.*

Como ejemplo, 2 es una raíz primitiva módulo 5, dado que los menores residuos positivos de 2, 2^2, 2^3 y 2^4 son 2, 4, 3 y 1 respectivamente. Por tanto, $4 = 5-1$ es el menor entero positivo tal que $2^n \equiv 1 \ \ (5)$.

Para $p = 7$, 2 no es una raíz primitiva dado que $2^3 \equiv 1 \ \ (7)$ pero 3 sí lo es porque 3, 3^2, 3^3, 3^4, 3^5 y 3^6 son congruentes con 3, 2, 6, 4, 5 y 1 módulo 7 respectivamente.

Aunque el **Teorema 1.1** muestra la existencia de raíces primitivas para un primo p dado, no hay una forma fácil de encontrar una. En los casos en los que p sea pequeño se puede probar por ensayo y error. Para mayores p sin embargo este proceso se hace inmanejable.

La famosa conjetura de E. Artin establece que si $a > 1$ no es un cuadrado, existen infinitos primos para los cuales a es una raíz primitiva, la cual se ha demostrado suponiendo cierta la *Hipótesis Generalizada de Riemann (GRH)*. Si no la usamos en cambio dicha conjetura no ha sido demostrada para ningún entero a día de hoy.

Ahora vamos a explicar brevemente otras dos demostraciones del **Teorema 1.1**.

Demostración 2:

Sea $p-1 = q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t}$ la descomposición en primos de $p-1$. Consideremos las congruencias:

(1) $x^{q_i^{e_i-1}} \equiv 1 \ \ (p)$

(2) $x^{q_i^{e_i}} \equiv 1 \ \ (p)$

Cada solución de la congruencia **(1)** es una solución de la congruencia **(2)**, dado que

$$x^{q_i^{e_i}} = (x^{q_i^{e_i-1}})^{q_i}.$$

Es más, la congruencia **(2)** tiene más soluciones que la congruencia **(1)**. Sea g_i una solución de la congruencia **(2)** que no lo sea de la congruencia **(1)** y definamos $g = g_1 g_2 \cdots g_t$. Se tiene que $\overline{g_i}$ genera un subgrupo de $U(\mathbb{Z}/\mathbb{Z}p)$ de orden $q_i^{e_i}$. De ahí se deduce que $\overline{g}$ genera un subgrupo de $U(\mathbb{Z}/\mathbb{Z}p)$ de orden $q_1^{e_1} q_2^{e_2} \ldots q_t^{e_t} = p-1$. Por tanto, g es una raíz primitiva y $U(\mathbb{Z}/\mathbb{Z}p)$ es cíclico. □

Demostración 3:

Finalmente, usando la Teoría de Grupos podemos ver que $\psi(d) \leq \phi(d)$ para todo $d \mid (p-1)$. Pero tiene que

$$\sum_{d|(p-1)} \psi(d) = \sum_{d|(p-1)} \phi(d) = p-1.$$

De esto se sigue que $\psi(d) = \phi(d)$ para todo $d \mid (p-1)$. En particular, $\psi(p-1) = \phi(p-1)$. Para $p > 2$, $\phi(p-1) > 1$, lo que implica que $\phi(p-1) > 1$ y esto nos prueba el teorema. □

La noción de raíz primitiva puede generalizarse de la siguiente manera.

Definición 1.2 *Sean a, $n \in \mathbb{Z}$. Se dice que a es una raíz primitiva módulo n si la clase residual de $\overline{a} = a + \mathbb{Z}n$ genera $U(\mathbb{Z}/\mathbb{Z}n)$. Esto es equivalente a que a y n sean coprimos y que $\phi(n)$ sea el menor entero positivo tal que $a^{\phi(n)} \equiv 1 \ \ (n)$.*

En general, no es verdad que $U(\mathbb{Z}/\mathbb{Z}n)$ sea cíclico. Por ejemplo, los elementos de $U(\mathbb{Z}/\mathbb{Z}8)$ son $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$ y $\overline{1}^2 = \overline{1}$, $\overline{3}^2 = \overline{1}$, $\overline{5}^2 = \overline{1}$, $\overline{7}^2 = \overline{1}$ por lo que no hay elementos de orden $4 = \phi(8)$. De esto se sigue que no todo entero tiene raíces primtivas. Vamos a determinar cuáles sí las tienen.

Lema 1.2 *Si p es un primo y $1 < k < p$ entonces el coeficiente binomial $\binom{p}{k}$ es divisible entre p.*

Demostración:

Por definición,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \implies p! = k!(p-k)!\binom{p}{k}$$

Ahora, p divide a $p!$, pero p no divide $k!(p-k)!$ dado que esta expresión es un producto de enteros menores y, por tanto, coprimos con p. Por tanto, p divide a $\binom{p}{k}$. □

Lema 1.3 *Si $l \geq 1$ y $a \equiv b \ \ (p^l)$ entonces $a^p \equiv b^p \ \ (p^{l+1})$.*

Demostración:

Podemos escribir $a = b + cp^l, c \in \mathbb{Z}$ por lo que

$$a^p = b^p + \left[\binom{p}{1} b^{p-1} c p^l + A \right],$$

donde A es un entero divisible por p^{l+2}. El segundo término es claramente divisible por p^{l+1}. por lo que $a^p \equiv b^p \ \ (p^{l+1})$. □

Corolario 1.3 *Si $l \geq 2$ y $p \neq 2$ entonces $(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \ \ (p^l) \ \forall a \in \mathbb{Z}$.*

Demostración:

La prueba es por inducción sobre l. Para $l = 2$, la implicación es trivial. Supongamos que es cierto para algún $l \geq 2$. Vamos a probar que es cierto para $l+1$. Aplicando el **Lema 1.3** se obtiene:

$$(1+ap)^{p^{l-1}} \equiv (1 + ap^{l-1})^p \ \ (p^{l+1})$$

Por el binomio de Newton:

$$(1 + ap^{l-1})^p = 1 + \binom{p}{1} ap^{l-1} + B$$

donde B es una suma de $p-2$ términos. Usando el **Lema 1.2** es fácil ver que todos esos términos son divisibles por $p^{1+2(l-1)}$ excepto quizás el último término, $a^p p^{p(l-1)}$. Como $l \geq 2$, $1+2(l-1) \geq l+1$, y como también $p \geq 3$, $p(l-1) \geq l+1$. Por tanto, $p^{l+1} \mid B$ y

$$(1+ap)^{p^{l-1}} \equiv 1 + ap^l \ \ (p^{l+1}),$$

que es lo que queríamos demsotrar.□

Corolario 1.4 *Si $p \neq 2$ y $p \nmid a$ entonces p^{l-1} es el orden de $1 + ap$ módulo p^l.*

Demostración:

Por el **Corolario 1.3**, $(1+ap)^{p^{l-1}} \equiv 1 + ap^l \ \ (p^{l+1})$, implicando que $(1+ap)^{p^{l-1}} \equiv 1 (p^l)$ por lo que $1 + ap$ tiene orden divisible por p^{l-1}. Como

$$(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \ \ (p^l),$$

nos muestra que p^{l-2} no es el orden de $1 + ap$ (aquí es donde usamos que $p \nmid a$). Con esto ya se tiene el resultado. □

Ahora estamos en posición de extender el **Teorema 1.1**. Debemos tratar al primo 2 separado de los primos impares, lo cual ocurre repetidas veces en Teoría de Números.

Teorema 1.2 *Si p es un primo impar y $l \in \mathbb{Z}_{>0}$ entonces $U(\mathbb{Z}/\mathbb{Z}p^l)$ es cíclico. En particular, existe una raíz primitiva módulo p^l.*

Demostración:

Por el **Teorema 1.1** existen raíces primitivas módulo p. Si $g \in \mathbb{Z}$ es una raíz primitiva módulo p entonces $g + p$ también lo es. Si $g^{p-1} \equiv 1 \ \ (p^2)$ entonces

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \ \ (p^2).$$

Dado que p^2 no divide a $(p-1)(g^{p-2}p)$ podemos asumir desde el principio que g es una raíz primitiva módulo p y que $g^{p-1} \equiv 1 \ \ (p^2)$.

Queremos probar que g es una raíz primitiva módulo p^l. Para ello será suficiente probar que si $g^n \equiv 1 \ \ (p^l)$ entonces $\phi(p^l) = p^{l-1}(p-1) \mid n$.

Por tanto, se tiene que $g^{p-1} = 1 + ap$ donde $p \nmid a$. Por el **Corolario 1.4**, p^{l-1} es el orden de $1 + ap$ módulo p^l . Dado que $(1 + ap)^n \equiv 1 \ (p^l)$ se tiene que $p^l \mid n$.

Sea $n = p^{l-1}n'$. Entonces

$$g^n = (g^{p^{l-1}})^{n'} \equiv g^{n'} \ (p),$$

y por tanto $g^{n'} \equiv 1 \ (p)$. Dado que g es una raíz primitiva módulo p se tiene que $(p-1) \mid n'$. Hemos probado que $p^{l-1}(p-1) \mid n$, como necesitamos. □

Teorema 1.3 *Sea $l \in \mathbb{Z}_{>0}$. Se cumple que 2^l tiene raíces primitivas para $l = 1, 2$ pero no para $l \geq 3$. Si $l \geq 3$ entonces el conjunto*

$$\left\{(-1)^a 5^b \mid a = 0, 1 \ y \ 0 \leq b < 2^{l-2}\right\}$$

constituye un sistema de residuos reducido módulo 2^l. Por tanto, para todo $l \geq 3$, $U(\mathbb{Z}/\mathbb{Z}2^l)$ es el producto directo de dos grupos cíclicos, uno de orden 2 y el otro de orden 2^{l-2}.

Demostración:

Se puede ver trivialmente que 1 es una raíz primitiva módulo 2 y 3 es una raíz primitiva módulo 4. A partir de ahora vamos a asumir que $l \geq 3$.

Vamos a probar que

$$5^{2^{l-3}} \equiv 1 + 2^{l-1} \ (2^l). \tag{1.1}$$

Eso es verdad para $l = 3$. Asumimos que es verdad para $l \geq 3$ y probaremos que también lo es para $l + 1$. Primero debemos ver que

$$(1 + 2^{l-1})^2 = 1 + 2^l + 2^{2l-2}$$

y que $2l - 2 \geq l + 1$, $\forall l \geq 3$. Aplicando el **Lema 1.3** a la congruencia (1.1), se obtiene

$$5^{2^{l-2}} \equiv 1 + 2^l \ (2^{l+1}). \tag{1.2}$$

Con esto, nuestra prueba se puede realizar por inducción.

A partir de (1.2) vemos que $5^{2^{l-2}} \equiv 1 \ (2^l)$ y del mismo modo por (1.1) $5^{2^{l-3}} \not\equiv 1 \ (2^l)$ por lo que 2^{l-2} es el orden de 5 módulo 2^l.

Consideremos el conjunto

$$\left\{(-1)^a 5^b \ \mid \ a = 0, 1 \text{ y } 0 \leq b < 2^{l-2}\right\}.$$

Vamos a probar que estos 2^{l-1} números no son congruentes módulo 2^l. Dado que $\phi(2^l) = 2^{l-1}$, esto nos mostrará que nuestro conjunto es de hecho un sistema de residuos reducido módulo 2^l.

Si se cumple que

$$(-1)^a 5^b \equiv (-1))^{a'} 5^{b'} \ (2^l),$$

para un $l \geq 3$ entonces

$$(-1)^a \equiv (-1)^{a'} \ (4)$$

lo cual implica que $a \equiv a' \ (2)$ y por tanto $a = a'$. Esto implica que $5^b \equiv 5^{b'} \ (2^l)$ o que $5^{b-b'} \equiv 1 \ (2^l)$ por lo que $b \equiv b' \ (2^{l-2})$, lo que nos lleva a que $b = b'$.

Finalmente debemos darnos cuenta que $(-1)^a 5^b$ elevado a la 2^{l-2}-ésima potencia es congruente con 1 módulo 2^l por lo que 2^l no tiene raíces primitivas si $l \geq 3$. □

Los **Teoremas 1.2** y **1.3** nos permiten dar una descripción completa del grupo $U(\mathbb{Z}/\mathbb{Z}n)$ para un n arbitrario.

Teorema 1.4 *Sea $n = 2^a p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ la descomposición en primos de n. Entonces*

$$U(\mathbb{Z}/\mathbb{Z}n) \approx U(\mathbb{Z}/\mathbb{Z}2^a) \times U(\mathbb{Z}/\mathbb{Z}p_1^{a_1}) \times \cdots \times U(\mathbb{Z}/\mathbb{Z}p_l^{a_l})$$

donde:

(1) *$U(\mathbb{Z}/\mathbb{Z}p_i^{a_i})$ es un grupo cíclico de orden $p_i^{a_i-1}(p_i - 1)$.*

(2) *$U(\mathbb{Z}/\mathbb{Z}2^a)$ es un grupo cíclico de orden 1 y 2 para $a = 1, 2$ respectivamente. Si $a \geq 3$ entonces es el producto de dos grupos cíclicos, uno de orden 2 y el otro de orden 2^{a-2}.*

Demostración:

Usar los **Teoremas 1.2** y **1.3** y el **Teorema Chino del Resto** (0.1). □

Vamos a concluir esta sección dando una respuesta a la preguntas de qué enteros poseen raíces primitivas.

Proposición 1.1.3 *Un número entero n posee raíces primitivas si y sólo si n es de la forma 2, 4, p^a o $2p^a$, donde p es un primo impar y $a \in \mathbb{Z}_{>0}$.*

Demostración:

Ya hemos probado que 2, 4, p^a poseen raíces primitivas para todo $a \in \mathbb{Z}_{>0}$. Dado que

$$U(\mathbb{Z}/\mathbb{Z}2p^a) \approx U(\mathbb{Z}/\mathbb{Z}2) \times U(\mathbb{Z}/\mathbb{Z}p^a) \approx U(\mathbb{Z}/\mathbb{Z}p^a)$$

se tiene que $U(\mathbb{Z}/\mathbb{Z}2p^a)$ es cíclico y por tanto, $2p^a$ posee raíces primitivas $\forall a \in \mathbb{Z}_{>0}$.

Por el **Teorema 1.3** podemos asumir que $n \neq 2^l$, $l \geq 3$. Para cualquier otro valor de n distinto de los vistos anteriormente es fácil ver que podemos escribir n como el producto $m_1 m_2$, donde $\gcd(m_1, m_2) = 1$ y $m_1, m_2 > 2$. Por lo tanto, $\phi(m_1)$ y $\phi(m_2)$ son ambos pares y

$$U(\mathbb{Z}/\mathbb{Z}n) \approx U(\mathbb{Z}/\mathbb{Z}m_1) \times U(\mathbb{Z}/\mathbb{Z}m_2).$$

Ambos $U(\mathbb{Z}/\mathbb{Z}m_1)$ y $U(\mathbb{Z}/\mathbb{Z}m_2)$ tienen elementos de orden 2, pero esto demuestra que $U(\mathbb{Z}/\mathbb{Z}n)$ no es cíclico dado que un grupo cíclico contiene a lo sumo un subgrupo de orden 2. Por tanto, n no posee raíces primitivas. □

1.2. Residuos de la n-ésima potencia

Definición 1.3 *Si m, $n \in \mathbb{Z}_{>0}$, $a \in \mathbb{Z}$ y $\gcd(a, m) = 1$ entonces decimos que a es un residuo de la n-ésima potencia módulo m si la congruencia $x^n \equiv a \pmod{m}$ tiene solución.*

Proposición 1.2.1 *Si $m \in \mathbb{Z}_{>0}$ posee raíces primitivas y $\gcd(a, m) = 1$ entonces a es un residuo de la n-ésima potencia módulo m si y sólo si $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$, donde $d = \gcd(n, \phi(m))$.*

Demostración:

Sea g una raíz primitiva módulo m y $a = g^b$, $x = g^y$. Entonces se tiene que la congruencia $x^n \equiv a \pmod{m}$ es equivalente a $g^{ny} \equiv g^b \pmod{m}$, la cual es equivalente a $ny \equiv b \pmod{\phi(m)}$. La última congruencia tiene solución si y sólo si $d \mid b$. Es más, es útil darse cuenta de que si hay una solución entonces hay exactamente d soluciones, lo cual ya hemos visto en la asignatura de **Álgebra Básica**.

Si $d \mid b$ entonces

$$a^{\frac{\phi(m)}{d}} \equiv g^{\frac{b\phi(m)}{d}} \equiv 1 \pmod{m}.$$

Por el contrario, si $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$ entonces $g^{\frac{b\phi(m)}{d}} \equiv 1 \pmod{m}$, lo cual implica que $\phi(m)$ divide a $\frac{b\phi(m)}{d}$ o $d \mid b$. Esto prueba el resultado. □

Esta demostración nos lleva a la siguiente información adicional: si $x^n \equiv a \pmod{m}$ tiene solución, hay exactamente $\gcd(n, \phi(m))$ soluciones.

Ahora supongamos que $m = 2^e p_1^{e_1} \cdots p_l^{e_l}$ entonces $x^n \equiv a \pmod{m}$ tiene solución si y sólo si el sistema de congruencias

$$\begin{cases} x^n \equiv a \pmod{2^e} \\ x^n \equiv a \pmod{p_1^{e_1}} \\ \vdots \\ x^n \equiv a \pmod{p_l^{e_l}} \end{cases}$$

tiene solución. Dado que las potencias de los primos impares poseen raíces primitivas podemos aplicar la **Proposición 1.2.1** a las últimas l congruencias. Hemos reducido a considerar la congruencia $x^n \equiv a \pmod{2^e}$. Dado que 2 y 4 poseen raíces primitivas vamos a asumir que $e \geq 3$.

Proposición 1.2.2 *Supongamos que a es impar, $e \geq 3$, y consideremos la congruencia $x^n \equiv a \pmod{2^e}$. Si n es impar, siempre existe una única solución.*

Si n es par, una solución existe si y sólo si

$$\begin{cases} a \equiv 1 \pmod{4} \\ a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e} \end{cases}$$

donde $d = \gcd(n, 2^{e-2})$. En caso de existir solución, existen exactamente $2d$ soluciones.

Demostración:

Expresemos

$$\begin{cases} a \equiv (-1)^s 5^t \pmod{2^e} \\ x \equiv (-1)^y 5^z \pmod{2^e} \end{cases}$$

Entonces

$$(-1)^s 5^t \equiv (-1)^{ny} 5^{nz} \pmod{2^e}.$$

Por el **Teorema 1.3** se tiene que $s \equiv ny \pmod{2}$.

Si n es impar se tiene que $s \equiv y \pmod{2}$ lo cual nos lleva nuevamente a $5^t \equiv 5^{nz} \pmod{2^e}$, llevándonos a $nz \equiv t \pmod{2^{e-2}}$. Por tanto, se tiene $\gcd(n, 2^{e-2})$ soluciones y dado que n es impar la solución es única.

Si n es par se tiene que $s \equiv 0 \pmod{2}$ y por lo tanto $a \equiv 5^t \pmod{2^e}$. Si $5^{nz} \equiv 5^t \pmod{2^e}$ entonces $5^{t-nz} \equiv 1 \pmod{2^e}$ y por tanto $nz \equiv t \pmod{2^{e-2}}$. Del mismo modo, se tiene que $d = \gcd(n, 2^{e-2})$ y por tanto hay d soluciones. Pero, como se puede ver, si x es solución, entonces $-x$ también lo es, por lo que hay exactamente $2d$ soluciones. Por lo que, si existe solución se tiene que de la congruencia $a \equiv 5^t \pmod{2^e}$ se deduce trivialmente que $a \equiv 1 \pmod{4}$ y además

$$a^{\frac{2^{e-2}}{d}} \equiv 5^{\frac{t2^{e-2}}{d}} \equiv (5^{2^{e-2}})^{\frac{t}{d}} \overset{d|t}{\equiv} 1 \pmod{2^e}.$$

La otra implicación se tiene usando la **Proposición 1.2.1**. □

Las **Proposiciones 1.2.1** y **1.2.2** nos dan una respuesta satisfactoria de la pregunta: ¿Cuándo un entero a es un residuo de la n-ésima potencia módulo n? Es posible ir un poco más lejos en algunos casos.

Proposición 1.2.3 *Si p es un primo impar, $p \nmid a$ y $p \nmid n$ entonces si $x^n \equiv a \pmod{p}$ tiene solución entonces $x^n \equiv a \pmod{p^e}$ para todo $e \geq 1$. Todas estas congruencias tienen el mismo número de soluciones.*

Demostración:

Si $n = 1$, la afirmación es trivial, así que asumiremos que $n \geq 2$.

Supongamos que $x^n \equiv a \pmod{p^e}$ tiene solución. Vamos a probar que $x^n \equiv a \pmod{p^{e+1}}$ tiene solución. Sea x_0 una solución y definamos $x_1 = x_0 + bp^e$. Si elevamos ambos términos a la n-ésima potencia y aplicamos congruencia módulo p^{e+1} se muestra que

$$x_1^n \equiv x_0^n + nbp^e x_0^{n-1} \pmod{p^{e+1}}.$$

Ahora vamos a resolver $x_1^n \equiv a \pmod{p^{e+1}}$, lo cual es equivalente a encontrar un entero b tal que

$$nx_0^{n-1}b \equiv \frac{a - x_0^n}{p^e} \pmod{p}.$$

Podemos ver que, dado que $x_0^n \equiv a \pmod{p^e}$ entonces $\frac{a-x_0^n}{p^e} \in \mathbb{Z}$ y por hipótesis de inducción $p \nmid nx_0^{n-1}$ por lo que tiene solución únicamente para un cierto b módulo p y, para dicho valor de b, se cumple que

$$x_1^n \equiv a \pmod{p^{e+1}}.$$

Por otro lado, si $x^n \equiv a \pmod{p}$ no tiene soluciones entonces $x^n \equiv a \pmod{p^e}$ tampoco las tiene.

Por la **Proposición 1.2.1**, en caso de existir alguna, la congruencia $x^n \equiv a \pmod{p^e}$ tiene exactamente $\gcd(n, \phi(p^e))$ soluciones. Si $p \nmid n$ entonces es fácil ver que

$$\gcd(n, p-1) = \gcd(n, \phi(p)) = \gcd(n, \phi(p^e)) = \gcd(n, p(p-1)), \ \forall e \geq 1.$$

Esto concluye la prueba. □

Como es habitual, la resolución para las potencias de 2 es más complicado.

Proposición 1.2.4 *Sea 2^l la mayor potencia de 2 que divide a n. Supongamos que a es impar y que $x^n \equiv a \pmod{2^{2l+1}}$ tiene solución entonces $x^n \equiv a \pmod{2^e}$ tiene solución para todo $e \geq 2l+1$ (y por tanto para todo $e \geq 1$). Es más, todas estas congruencias tienen el mismo número de soluciones.*

Demostración:

Podemos escribir $n = 2^l q$ con q impar. Asumamos que la congruencia $x^n \equiv a \pmod{2^m}$, $m \geq 2l+1$ tiene una solución x_0. Vamos a probar que la congruencia $x^n \equiv a \pmod{2^{m+1}}$ también tiene una solución y para ello definamos entonces $x_1 = x_0 + b2^{m-l}$. De manera análoga a la de la **Proposición 1.2.3**, podemos obtener la congruencia

$$x_1^n \equiv x_0^n + nb2^{m-l}x_0^{n-1} \pmod{2^{m+1}}.$$

Queremos probar la congruencia $x_1^n \equiv a \pmod{2^{m+1}}$, la cual es equivalente a encontrar un entero b tal que

$$nx_0^{n-1}b \equiv \frac{a - x_0^n}{2^{m-l}} \pmod{2^{l+1}}.$$

Podemos comprobar nuevamente que $\frac{a-x_0^n}{2^{m-l}} \in \mathbb{Z}$ y $2^{l+1} \nmid nx_0^{n-1} = 2^l q x_0^{n-1}$, dado que tanto q como x_0 son impares se tiene que la congruencia es tiene solución para un cierto b módulo 2^{l+1}, y para ese valor de b , $x_1^n \equiv a \pmod{2^{l+1}}$.

Del mismo modo, si $x^n \equiv a \pmod{2^{2l+1}}$ no tiene soluciones es porque n es par y no cumple las condiciones de la **Proposición 1.2.2**, por lo que $x^n \equiv a \pmod{2^m}$, $m \geq 2l+1$ tampoco tiene soluciones.

Nuevamente, por la **Proposición 1.2.2** el número de soluciones de $x^n \equiv a \pmod{2^m}$, $m \geq 2l+1$ es

$$\gcd(n, 2^l) = \gcd(n, \phi(2^{2l+1})) = \gcd(n, \phi(2^m)) = \gcd(2^l q, 2^{m-1})) = 2^l \quad \forall m \geq 2l+1.$$

Esto concluye la prueba. □

Podemos ver que $x^2 \equiv 5 \ \ (2^2)$ tiene solución (por ejemplo, $x = 1$) pero $x^2 \equiv 5 \ \ (2^3)$ no lo es. Por el contrario, es fácil probar por la **Proposición 1.2.4** que $a \equiv 1 \ \ (8)$ si y sólo si $x^2 \equiv a \ \ (2^e)$ tiene solución para todo $e \geq 1$, como veremos en el siguiente capítulo.

Una vez entendidos todos los conceptos básicos vistos en el capítulo anterior vamos a centrar nuestra atención en resolver el siguiente problema:

Sea $a \in \mathbb{Z}$, ¿para qué p primos la congruencia $x^2 \equiv a \ \ (p)$ tiene solución?

La solución nos la va a proporcionar la **Ley de Reciprocidad Cuadrática**, que va a ser nuestro objetivo principal de estudio a lo largo del resto del trabajo, la cual demostraremos de varias formas distintas.

Capítulo 2

Ley de Reciprocidad Cuadrática usando los residuos cuadráticos

2.1. Residuos cuadráticos

Antes de poder enunciar esta ley, y dar su primera demostración, debemos definir el concepto de *residuo cuadrático*, lo cual haremos en esta primera sección.

Definición 2.1 *Si* $\gcd(a,m)=1$*, a es llamado un residuo cuadrático módulo m si la congruencia* $x^2 \equiv a \pmod{m}$ *tiene una solución. En otro caso, a es un residuo no-cuadrático módulo m.*

Por ejemplo, 2 es un residuo cuadrático módulo 7 pero 3 no lo es. En efecto, 1^2, 2^2, 3^2, 4^2, 5^2 y 6^2 son congruentes con 1, 4, 2, 2, 4 y 1 respectivamente. Entonces, 1, 2 y 4 son residuos cuadráticos módulo 7 mientras que 3, 5 y 6 no lo son.

Este método podemos aplicarlo para cualquier entero positivo m, tal y como hemos hecho con $m=7$ pero la siguiente proposición nos da una forma mucho menos tediosa para decidir cuando un entero dado es un residuo cuadrático módulo m.

Proposición 2.1.1 *Sea* $m = 2^e p_1^{e_1} \cdots p_l^{e_l}$ *sea la factorización en primos de m, y suponemos* $\gcd(a,m)=1$*. Entonces* $x^2 \equiv a \pmod{m}$ *tiene solución si y sólo si se cumplen las siguientes condiciones:*

(a) *Si* $e=2$ *entonces* $a \equiv 1 \pmod{4}$.
Si $e \geq 3$ *entonces* $a \equiv 1 \pmod{8}$.
(Si $e = 0, 1$ *entonces no hay condiciones.)*

(b) *Para todo i se tiene que:* $a^{\frac{p_i-1}{2}} \equiv 1 \pmod{p_i}$.

Demostración:

Por el **Teorema Chino del Resto** (0.1), la congruencia $x^2 \equiv a \pmod{m}$ es equivalente al sistema

$$\begin{cases} x^2 \equiv a \pmod{2^e} \\ x^2 \equiv a \pmod{p_1^{e_1}} \\ \vdots \\ x^2 \equiv a \pmod{p_l^{e_l}} \end{cases}$$

Consideremos $x^2 \equiv a \pmod{2^e}$. Se puede ver que 1 es el único residuo cuadrático módulo 4 y lo mismo ocurre módulo 8. Por tanto tiene solución si y sólo si $a \equiv 1 \pmod{4}$ si $e=2$ y $a \equiv 1 \pmod{8}$ si $e=3$. Una aplicación directa de la **Proposición 1.2.4** nos muestra que $x^2 \equiv a \pmod{8}$ tiene solución si y sólo si $x^2 \equiv a \pmod{2^e}$ para todo $e \geq 3$.

Ahora consideremos $x^2 \equiv a \ \ (p_i^{e_i})$. Dado que $\gcd(2, p_i) = 1$ se sigue que por la **Proposición 1.2.3** que la congruencia tiene solución si y sólo si $x^2 \equiv a \ \ (p_i)$ tiene solución. A esa congruencia aplicamos la **Proposición 1.2.1** con $n = 2$, $m = p$ y $d = \gcd(n, \phi(m)) = \gcd(2, p-1) = 2$. Se obtiene que $x^2 \equiv a \ \ (p_i)$ tiene solución si y sólo si $a^{\frac{p_i-1}{2}} \equiv 1 \ \ (p_i)$. □

Este resultado reduce las cuestiones sobre los residuos cuadráticos a las correspondentes para congruencias en módulo primo. En lo que sigue, p va a denotar a un primo impar.

Definición 2.2 *El símbolo de Legendre, denotado como* $\left(\frac{a}{p}\right)$*, sigue que:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } p|a; \\ 1, & \text{si } a \text{ es un residuo cuadrático módulo } p; \\ -1, & \text{si } a \text{ es un residuo no-cuadrático módulo } p. \end{cases}$$

Este símbolo nos será de gran utilidad para tratar con los residuos cuadráticos, tal y como se hará a continuación. Vamos a listar algunas propiedades:

Proposición 2.1.2 *En las condiciones anteriores:*

(a) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ \ (p)$.

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(c) *Si* $a \equiv b \ \ (p)$ *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Demostración:

Si p divide a a ó b, las tres afirmaciones son triviales. Asumimos que $p \nmid a$ y $p \nmid b$.
Sabemos que $a^{p-1} \equiv 1 \ \ (p)$ y por tanto,

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) = a^{p-1} - 1 \equiv 0 \ \ (p).$$

De esto se sigue que $a^{\frac{p-1}{2}} \equiv \pm 1 \ \ (p)$. Por la **Proposición 2.1.1**, $a^{\frac{p-1}{2}} \equiv 1 \ \ (p)$ si y sólo si a es un residuo cuadrático módulo p. Esto prueba el apartado **(a)**.
Para probar el apartado **(b)** aplicamos el apartado **(a)**:

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \ \ (p)$$

y

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ \ (p)$$

Por tanto,

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ \ (p) \Longrightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

El apartado **(c)** es obvio por la definición. □

Corolario 2.1 *Hay tantos residuos cuadráticos como no-cuadráticos módulo* p.

Demostración:

La congruencia $a^{\frac{p-1}{2}} \equiv 1 \ \ (p)$ tiene $\frac{p-1}{2}$ soluciones. Por tanto hay $\frac{p-1}{2}$ residuos cuadráticos y $\frac{p-1}{2}$ residuos no-cuadráticos. □

Corolario 2.2 *El producto de dos residuos cuadrátricos es un residuo cuadrático, el producto de dos residuos no-cuadráticos es un residuo cuadrático y el producto de un residuo cuadrático y uno no-cuadrático es un residuo no-cuadrático.*

Demostración:

Esta demostración se sigue fácilmente del apartado **(b)** de la **Proposición 2.1.2**. □

Corolario 2.3 *En las condiciones anteriores:*

$$(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right).$$

Demostración:

Se sigue de sustituir $a = -1$ en el apartado **(a)** de la **Proposición 2.1.2**. □

El **Corolario 2.3** es particularmente interesante. Cada primo impar es de la forma $4k+1$ o $4k+3$. Usando eso uno puede replantearse el **Corolario 2.3** como sigue: $x^2 \equiv -1 \ (p)$ tiene una solución si y sólo si p es la forma $4k+1$. Entonces, -1 es un residuo cuadrático de los primos 5, 13, 17, 29, ... y un residuo no-cuadrático de los primos 3, 7, 11, 19, ...

Esto nos lleva a preguntarnos una cuestión más general. Si a es un entero, ¿para qué primos p es a un residuo cuadrático módulo p? La respuesta de esta pregunta nos la proporciona la *Ley de Reciprocidad Cuadrática* cuyo enunciado y prueba tendrán pronto nuestra atención.

El **Corolario 2.3** nos permite probar que hay infinitos primos de la forma $4k+1$. Supongamos que $p_1, p_2, \ldots, p_m$ son un conjunto finito de esos primos y consideremos $(2p_1p_2\cdots p_m)^2 + 1$. Supongamos que p divide a este entero. Entonces tendríamos que -1 sería un residuo cuadrático módulo p y entonces p será de la forma $4k+1$. Se puede comprobar fácilmente que p no está entre los p_i dado que $(2p_1p_2\cdots p_m)^2 + 1$ nos deja resto 1 cuando lo dividimos entre p_i. Esto nos muestra que todo conjunto finito de primos de la forma $4k+1$ excluye algunos primos de esa forma por tanto el conjunto de estos primos es infinito.

Volviendo a la teoría de residuos cuadráticos vamos a introducir otra caracterización del símbolo $\left(\frac{a}{p}\right)$ dada por Gauss.

Consideremos el conjunto

$$S = \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Se le denomina el conjunto de los menores residuos módulo p. Si $p \nmid a$, sea μ el número de menores residuos negativos de los enteros a, $2a$, $3a$,..., $\frac{p-1}{2}a$. Por ejemplo, sea $p = 7$ y $a = 4$. Entonces $\frac{p-1}{2} = 3$, y $1 \cdot 4$, $2 \cdot 4$ y $3 \cdot 4$ son congruentes con -3, 1, -2 respectivamente por lo que, en este caso, $\mu = 2$.

Lema 2.1 (Lema de Gauss) $\left(\frac{a}{p}\right) = (-1)^{\mu}$.

Demostración:

Sea l un entero entre 1 y $\frac{p-1}{2}$ y $\pm m_l$ el menor residuo de la, donde m_l es positivo, por lo que μ es claramente el número de signos negativos que surgen de esta forma. Vamos a probar que $m_l \neq m_k$, si $l \neq k$ y $1 \leq l, k \leq \frac{p-1}{2}$.

Supongamos que $m_l = m_k$. Entonces $la \equiv \pm ka \ (p)$ y dado que $p \nmid a$ esto implica que $l \pm k \equiv 0 \ (p)$. Esta congruencia es imposible dado que $l \neq k$ y

$$| l \pm k | \leq | l | + | k | \leq \ p - 1.$$

De esto se sigue que los conjuntos $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ y $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\}$ son el mismo. Multiplicando las congruencias

$$\begin{cases} 1 \cdot a & \equiv & \pm m_1 \ (p) \\ 2 \cdot a & \equiv & \pm m_2 \ (p) \\ & \vdots & \\ \frac{p-1}{2} \cdot a & \equiv & \pm m_{\frac{p-1}{2}} \ (p) \end{cases}$$

se obtiene:

$$\left(\frac{p-1}{2}\right)! \, a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \left(\frac{p-1}{2}\right)! \quad (p)$$

Esto nos conduce a

$$a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \ (p).$$

Por la **Proposición 2.1.2** $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ (p)$ y por la definición del símbolo de Legendre el resultado es obvio. □

El **Lema de Gauss** (2.1) es una herramienta extremadamente útil. Vamos a basar nuestra primera prueba de la *Ley de Reciprocidad Cuadrática* en ello. Antes de ponernos con ello, sin embargo, vamos a usarlo para una caracterización de los primos para los cuales 2 es un residuo cuadrático.

Proposición 2.1.3 *El número 2 es un residuo cuadrático de los primos de la forma $8k+1$ y $8k+7$. Del mismo modo, 2 es un residuo no-cuadrático de los primos de la forma $8k+3$ y $8k+5$. Esto se puede resumir en la siguiente fórmula:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Demostración:

Sea p un primo impar y veamos que el número μ es igual al número de elementos del conjunto $2 \cdot 1, \ 2 \cdot 2, \ldots, \ 2 \cdot \frac{p-1}{2}$ que exceden a $\frac{p-1}{2}$. Determinemos m por dos condiciones: $2m \leq \frac{p-1}{2}$ y $2(m+1) > \frac{p-1}{2}$. Por tanto $\mu = \frac{p-1}{2} - m$.

Si $p = 8k+1$ entonces $\frac{p-1}{2} = 4k$ y $m = 2k$. Por tanto, $\mu = 4k - 2k = 2k$ es par y $\left(\frac{2}{p}\right) = 1$.

Si $p = 8k+7$ entonces $\frac{p-1}{2} = 4k+3$ y $m = 2k+1$. Por tanto, $\mu = 4k+3-(2k+1) = 2k+2$ es par y $\left(\frac{2}{p}\right) = 1$ también.

Si $p = 8k+3$ entonces $\frac{p-1}{2} = 4k+1$ y $m = 2k$. Por tanto, $\mu = 4k+1-2k = 2k+1$ es impar y $\left(\frac{2}{p}\right) = -1$.

Finalmente, si $p = 8k+5$ entonces $\frac{p-1}{2} = 4k+2$ y $m = 2k+1$. Por tanto,

$$\mu = 4k+2-(2k+1) = 2k+1$$

es impar, $\left(\frac{2}{p}\right) = -1$ y hemos concluido la prueba. □

Como ejemplo, consideremos $p = 7$ y $p = 17$. Estos primos son congruentes a 7 y 1, respectivamente, módulo 8 y, de hecho, $3^2 \equiv 2 \ (7)$ y $6^2 \equiv 2 \ (17)$. Por el otro lado, $p = 19$ y $p = 5$ son congruentes con 3 y 5, respectivamente, módulo 8 y es fácil comprobar numéricamente que 2 es un residuo no-cuadrático para ambos primos.

Se puede usar la **Proposición 2.1.3** para probar que hay infinitos primos de la forma $8k+7$. Sea $p_1, \ldots, p_m$ una colección finita de esos primos y consideremos $(4p_1p_2\cdots p_m)^2 - 2$. Los primos impares divisores de este número son de la forma $8k+1$ o $8k+7$ dado que, para esos primos, 2 es un residuo cuadrático. No todos los primos impares divisores pueden ser de la forma $8k+1$. Eso se puede probar dado que

$$(4p_1p_2\cdots p_m)^2 - 2 \equiv 6 \pmod 8 \quad (8)$$

y, si todos los divisores primos fueran de la forma $8k+1$ nos daría que es congruente con 1 módulo 8, que multiplicado por potencias de 2 nunca va a ser congruente con 6 módulo 8. Si existiera uno de la forma $8k+7$ multiplicado por 2 nos da que es congruente con 6 módulo 8. Sea entonces p un divisor primo de la forma $8k+7$. Entonces p no está en conjunto $\{p_1, p_2, \ldots, p_m\}$ y lo hemos demostrado.

2.2. Ley de Reciprocidad Cuadrática

Teorema 2.1 (Ley de Reciprocidad Cuadrática) *Sean p y q dos primos impares, Entonces se cumplen las siguientes propiedades:*

(a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

(b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Vamos a posponer esta prueba hasta más adelante. En cualquier caso, los apartados **(a)** y **(b)** del **Teorema 2.1** ya se han probado y hemos mecionado algunas de sus consecuencias. Vamos a centrar nuestra atención en el apartado **(c)**.

Si p o q son de la forma $4k+1$ entonces

$$\frac{p-1}{2}\frac{q-1}{2} \equiv 0 \pmod 2.$$

Si p y q son de la forma $4k+3$ entonces

$$\frac{p-1}{2}\frac{q-1}{2} \equiv 1 \pmod 2.$$

Esto nos permite reformular el apartado **(c)**:

(1) Si p o q son de la forma $4k+1$ entonces p es un residuo cuadrático módulo q si y sólo si q es un residuo cuadrático módulo p.

(2) Si p y q son de la forma $4k+3$ entonces p es un residuo cuadrático módulo q si y sólo si q es un residuo no-cuadrático módulo p.

Una primera aplicación de la reciprocidad cuadrática será mostrar como, unida a la **Proposición 2.1.2**, puede ser usado en computaciones numéricas del símbolo de Legendre.

Anteriormente hemos visto antes que -1 es un residuo cuadrático de los primos de la forma $4k+1$ y 2 es un residuo cuadrático de los primos de la forma $8k+1$ o $8k+7$. Si a es un entero cualquiera, ¿para qué primos p es a un residuo cuadrático módulo p? Ahora ya podemos dar la respuesta. Empezaremos considerando el caso donde $a = p$, un primo impar.

Teorema 2.2 *Sea q un primo impar:*

(a) *Si $q \equiv 1 \ (4)$ entonces q es un residuo cuadrático módulo p si y sólo si $p \equiv r \ (q)$ donde r es un residuo cuadrático módulo q.*

(b) *Si $q \equiv 3 \ (4)$ entonces q es un residuo cuadrático módulo p si y sólo si $p \equiv \pm b^2 \ (4q)$ donde b es un entero impar coprimo con q.*

Demostración:

Si $q \equiv 1 \ (4)$ entonces, por el **Teorema 2.1**, se tiene que $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Esto nos demuestra el apartado **(a)**. Si $q \equiv 3 \ (4)$, el **Teorema 2.1** nos conduce a que

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right).$$

Asumiremos primero que $p \equiv \pm b^2 \ (4q)$, donde b es impar. Si elegimos el signo positivo, obtendremos

$$\begin{cases} p \equiv b^2 \equiv 1 \ (4), \\ p \equiv b^2 \ (q). \end{cases}$$

por lo que $(-1)^{\frac{p-1}{2}} = 1$ y $\left(\frac{p}{q}\right) = 1$, y por tanto $\left(\frac{q}{p}\right) = 1$. Si elegimos el signo negativo entonces

$$\begin{cases} p \equiv -b^2 \equiv -1 \equiv 3 \ (4), \\ p \equiv -b^2 \ (q). \end{cases}$$

La primera congruencia nos muestra que $(-1)^{\frac{p-1}{2}} = -1$. La segunda congruencia nos muestra que

$$\left(\frac{p}{q}\right) = \left(\frac{-b^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{b}{q}\right)^2 = \left(\frac{-1}{q}\right) = -1, \text{ dado que } q \equiv 3 \ (4).$$

De nuevo se tiene que $\left(\frac{q}{p}\right) = 1$.

Para probar la otra aplicación, asumimos que $\left(\frac{q}{p}\right) = 1$. Se tienen dos casos a tratar:

(1) $(-1)^{\frac{p-1}{2}} = -1$ y $\left(\frac{p}{q}\right) = -1$.

(2) $(-1)^{\frac{p-1}{2}} = 1$ y $\left(\frac{p}{q}\right) = 1$.

En el caso **(2)** se tiene que $p \equiv b^2 \ (q)$ y $p \equiv 1 \ (4)$. Se puede asumir que b es impar dado que si fuera par usaríamos $b' = b + q$. Si b es impar entonces $b^2 \equiv 1 \ (4)$ y $p \equiv b^2 \ (q)$ por lo que $p \equiv b^2 \ (4q)$, como necesitamos.

En el caso **(1)** se tiene que $p \equiv 3 \ (4)$ y $p \equiv -b^2 \ (q)$. La última congruencia se obtiene debido a $q \equiv 3 \ (4)$ e implica que cada residuo no-cuadrático es el negativo de un residuo cuadrático. Esto se puede probar de la siguiente forma. Sea u un residuo no-cuadrático módulo q entonces $\left(\frac{u}{q}\right) = -1$. Por lo tanto,

$$\left(\frac{-u}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{u}{q}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{u}{q}\right).$$

Dado que $q = 4k + 3$ entonces

$$(-1)^{\frac{q-1}{2}} = (-1)^{2k+1},$$

y por tanto $\left(\frac{-u}{q}\right) = -\left(\frac{u}{q}\right) = 1$ lo que no sólo nos prueba lo que queríamos demostrar sino también el recíproco siempre que $q \equiv 3 \ (4)$. De nuevo, asumimos que b es impar. En este caso, $-b^2 \equiv 3 \ (4)$ así que $p \equiv -b^2 \ (4)$ y $p \equiv -b^2 \ (4q)$. Esto concluye la prueba. □

Tomemos $q = 3$ como primer ejemplo. Por apartado **(b)** del **Teorema 2.2** debemos encontrar los residuos módulo 12 de los cuadrados de los primos impares coprimos con 3. Se puede ver que 1^2, 5^2, 7^2 y 11^2 son todos congruentes con 1. Por tanto, 3 es un residuo cuadrático de los primos p congruentes con ± 1 (12) y un residuo no-cuadrático con los primos congruentes con ± 5 (12).

Consideremos ahora $q = 5$. Dado que $5 \equiv 1$ (4), estamos en el apartado **(a)** del **Teorema 2.2**. Se tiene que 1 y 4 son residuos cuadráticos módulo 5 mientras que 2 y 3 no lo son. Por tanto, 5 es un residuo cuadrático de los primos congruentes con 1 o 4 módulo 5 y un residuo no-cuadrático con los primos congruentes con 2 o 3 módulo 5.

Para $a = -3$, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. Por tanto, -3 es un residuo cuadrático módulo p si, o bien $\left(\frac{-1}{p}\right) = 1$ y $\left(\frac{3}{p}\right) = 1$, o bien $\left(\frac{-1}{p}\right) = -1$ y $\left(\frac{3}{p}\right) = -1$. Por nuestros resultado anteriores, el primero se obtiene cuando $p \equiv 1$ (4) y $p \equiv \pm 1$ (12). Si $p \equiv -1$ (12) entonces $p \equiv -1$ (4). Por tanto, los únicos primos que cumplen ambas congruencias son los de la forma $p \equiv 1$ (12). En el segundo caso, $p \equiv 3$ (4) y $p \equiv \pm 5$ (12). Si $p \equiv 5$ (12) entonces $p \equiv 1$ (4) y por lo tanto, los únicos primos que cumplen ambas congruencias son los de la forma $p \equiv -5$ (12). Resumiendo, -3 es un residuo cuadrático módulo p si y sólo si p es congruente a 1 o -5 módulo 12.

Ahora consideremos $a = 6$. Dado que $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$ se tiene otra vez dos casos: o bien $\left(\frac{2}{p}\right) = 1$ y $\left(\frac{3}{p}\right) = 1$, o bien $\left(\frac{2}{p}\right) = -1$ y $\left(\frac{3}{p}\right) = -1$. El primer caso nos dice que $p \equiv 1, 7$ (8) y $p \equiv 1, 11$ (12). Los únicos dos pares de congruencias compatibles entre sí son $p \equiv 1$ (8) y $p \equiv 1$ (12) y $p \equiv 7$ (8) y $p \equiv 11$ (12). Aplicando el Teorema Chino del Resto (0.1), se tiene que los primos que satisfacen estas congruencias son de la forma $p \equiv 1, 23$ (24). En el segundo caso, $p \equiv 3, 5$ (8) y $p \equiv 5, 7$ (12). Por tanto, las únicas soluciones congruentes son de la forma $p \equiv 5, 19$ (24). Resumiendo, 6 es un residuo cuadrático módulo p si y sólo si $p \equiv 1, 5, 19, 23$ (24). Como rápida comprobación, podemos ver los primos 73, 5, 19 y 23 verifican que

$$\begin{cases} 15^2 \equiv 6 \ (73) \\ 1^2 \equiv 6 \ (5) \\ 5^2 \equiv 6 \ (19) \\ 11^2 \equiv 6 \ (23) \end{cases}$$

Como aplicación final a la *Ley de Reciprocidad Cuadrática* investigaremos la pregunta: si a es residuo cuadrático módulo todos los primos p que no dividen a a, ¿qué se puede decir sobre a?

Lo que sí tenemos es que si a es un cuadrado, es un residuo cuadrático para todos los primos que no dividen a dividen a a. Esto nos lleva a que el recíproco de esta afirmación también se cumple. De hecho, pronto probaremos un resultado todavía más fuerte. Primero, sin embargo, es necesario definir e investigar brevemente un nuevo símbolo.

Definición 2.3 *Sea b un entero positivo e impar y a un entero cualquiera. Sea $b = p_1 p_2 \cdots p_m$, donde p_i son primos (no necesariamente distintos). El símbolo $\left(\frac{a}{b}\right)$ definido de la forma:*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right)$$

es denominado símbolo de Jacobi.

El símbolo de Jacobi tiene propiedades que son considerablemente parecidas a las del símbolo de Legendre, al cual generaliza, pero se debe tener cuidado. El símbolo de Jacobi $\left(\frac{a}{b}\right)$ puede ser igual a 1 sin que a sea un residuo cuadrático módulo b. Por ejemplo $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, pero 2 no es un residuo cuadrático módulo 15. Lo que sí es cierto es que, si $\left(\frac{a}{b}\right) = -1$ entonces a es un residuo no-cuadrático módulo b.

Proposición 2.2.1 *En las condiciones anteriores:*

(a) $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$ *si* $a_1 \equiv a_2 \ \ (b)$.

(b) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.

(c) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

Demostración:

Los apartados **(a)** y **(b)** son inmediatos a partir de los correspondientes del símbolo de Legendre. El apartado **(c)** es obvio de la definición. □

Lema 2.2 *Sean r y s enteros impares. Entonces,*

(a) $\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \ \ (2)$.

(b) $\frac{r^2s^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \ \ (2)$.

Demostración:

Dado que

$$(r-1)(s-1) \equiv 0 \ \ (4),$$

se tiene que

$$rs - 1 \equiv (r-1) + (s-1) \ \ (4).$$

El apartado **(a)** se consigue dividiendo entre 2.

Por otro lado, se tiene fácilmente que $r^2 - 1$ y $s^2 - 1$ son ambos divisibles entre 4 por lo que

$$(r^2-1)(s^2-1) \equiv 0 \ \ (16),$$

y por tanto,

$$r^2s^2 - 1 \equiv (r^2-1) + (s^2-1) \ \ (16).$$

El apartado **(b)** se consigue dividiendo entre 8. □

Corolario 2.4 *Sean $r_1, r_2, \ldots, r_m$ enteros impares. Entonces:*

(a) $\sum_{i=1}^{m} \frac{r_i-1}{2} \equiv \frac{r_1 r_2 \cdots r_m - 1}{2} \ \ (2)$.

(b) $\sum_{i=1}^{m} \frac{r_i^2-1}{8} \equiv \frac{r_1^2 r_2^2 \cdots r_m^2 - 1}{8} \ \ (2)$.

Demostración:

Esta prueba se hace por inducción en m, usando el **Lema 2.2** para caso inicial. □

Proposición 2.2.2 *En las condiciones anteriores:*

(a) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

(b) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.

(c) *Si a y b son enteros positivos e impares. Entonces*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

Demostración:

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_m}\right) =$$

$$= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_m-1}{2}} = (-1)^{\sum_{i=1}^{m}\frac{p_i-1}{2}}.$$

Por el **Corolario 2.4**,

$$\sum_{i=1}^{m}\frac{p_i-1}{2} \equiv \frac{p_1p_2\cdots p_m-1}{2} \equiv \frac{b-1}{2} \quad (2).$$

Esto prueba el apartado **(a)**. El apartado **(b)** se prueba de la misma manera.
Ahora si $a = q_1q_2\cdots q_l$, entonces

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \prod_{i=1}^{l}\prod_{j=1}^{m}\left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = (-1)^{\sum_i\sum_j\frac{q_i-1}{2}\frac{p_j-1}{2}}.$$

El producto y la suma están en el intervalo $1 \le i \le l$ y $1 \le j \le m$. Otra vez, por el **Corolario 2.4** se tiene

$$\sum_{i}^{l}\sum_{j}^{m}\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right) \equiv \frac{a-1}{2}\sum_{j}^{m}\frac{p_j-1}{2} \equiv \left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right) \quad (2).$$

Esto prueba el apartado **(c)**. □

El símbolo de Jacobi tiene muchos usos. Por ejemplo, es una ayuda muy conveniente para calcular el símbolo de Legendre. Ahora vamos a probar el siguiente teorema.

Teorema 2.3 *Sea a un entero no cuadrado. Entonces hay infinitos primos p para los cuales a es un residuo no-cuadrático.*

Demostración:

Se puede ver fácilmente que podemos asumir que a no tiene cuadrados. Sea $a = 2^e q_1q_2\cdots q_n$, donde q_i son primos impares distintos y $e = 0, 1$. El caso $a = 2$ será tratado por separado. Asumiremos que $n \ge 1$, es decir, que a es divisible por un primo impar.

Sean $l_1, l_2, \ldots, l_k$ un conjunto finito de primos impares que no incluyen a ningún q_i. Sea s un residuo no-cuadrático módulo q_n. Encontremos una solución simultánea a las congruencias:

$$\begin{aligned} &x \equiv 1 \ (l_i) \quad i = 1, \ldots, k \\ &x \equiv 1 \ (8) \\ &x \equiv 1 \ (q_i) \quad i = 1, \ldots, n-1 \\ &x \equiv s \ (q_n) \end{aligned}$$

Llamemos b a la solución, donde b es impar. Supongamos que $b = p_1 p_2 \cdots p_m$ su descomposición en primos. Dado que $b \equiv 1 \pmod 8$ se tiene que $\left(\frac{2}{b}\right) = 1$ y $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$ por la **Proposición 2.2.2** y por tanto

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{q_1}{b}\right) \cdots \left(\frac{q_{n-1}}{b}\right)\left(\frac{q_n}{b}\right) = \left(\frac{b}{q_1}\right) \cdots \left(\frac{b}{q_{n-1}}\right)\left(\frac{b}{q_n}\right) = \left(\frac{1}{q_1}\right) \cdots \left(\frac{1}{q_{n-1}}\right)\left(\frac{s}{q_n}\right) = -1.$$

Por otro lado, por la definición $\left(\frac{a}{b}\right)$, se tiene que

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_m}\right).$$

Por tanto, se sigue que $\left(\frac{a}{p_i}\right) = -1$ para algún i.

Observemos que l_j no divide a b. Por tanto $p_i \notin \{l_1, l_2, \ldots, l_k\}$.

Resumiendo, si a no tiene cuadrados y es divisible por un primo impar, hemos encontrado un primo p, fuera del conjunto de primos $\{2, l_1, l_2, \ldots, l_k\}$ tal que $\left(\frac{a}{p}\right) = -1$. Esto prueba **Teorema 2.3** en este caso.

Nos falta considerar el caso $a = 2$. Sean $l_1, \ldots, l_k$ un conjunto finito de primos, excluyendo 3, para el cual $\left(\frac{2}{l_i}\right) = -1$ para algún i. Sea $b = 8l_1 l_2 \cdots l_k + 3$. Entonces b no es divisible por 3 o ningún l_i. Dado que $b \equiv 3 \pmod 8$ se tiene que

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = -1.$$

Supongamos que $b = p_1 p_2 \cdots p_m$ es la factorización en primos de b. Entonces, como antes, vemos que $\left(\frac{2}{p_i}\right) = -1$ para algún i. $p_i \notin \{3, l_1, l_2, \ldots, l_k\}$. Esto prueba el **Teorema 2.3** para $a = 2$. □

2.3. Primera demostración de la Ley de Reciprocidad Cuadrática

Una vez vistos todos estos conceptos ya podemos empezar a preparar la demostración de la *Ley de Reciprocidad Cuadrática* realizada por Eisenstein.

Definición 2.4 *Un número complejo ζ es llamado raíz n-ésima de la unidad si se cumple que $\zeta^n = 1$ para algún $n \geq 1$. Además, si n es el menor entero positivo con esta propiedad entonces ζ es una raíz n-ésima primitiva de la unidad.*

Las raíces n-ésimas de la unidad son

$$1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}.$$

Entre ellos las raíces n-ésimas primitivas de la unidad son $e^{\frac{2k\pi i}{n}}$, donde $\gcd(k, n) = 1$.

Si ζ es una raíz n-ésima de la unidad y $m \equiv l \pmod n$ entonces $\zeta^m = \zeta^l$. Si ζ es una raíz n-ésima primitiva de la unidad y $\zeta^m = \zeta^l$ entonces $m \equiv l \pmod n$. Estas propiedades elementales son fáciles de probar.

Consideremos la función

$$f(z) = e^{2\pi i z} - e^{-2\pi i z} = 2i \operatorname{sen} 2\pi z.$$

Esta función satisface $f(z+1) = f(z)$ y $f(-z) = -f(z)$. Además, sus únicos ceros reales son los enteros divididos entre 2 o lo que es lo mismo, si r es un número real tal que $2r \notin \mathbb{Z}$ entonces $f(r) \neq 0$.

Queremos probar una identidad importante sobre $f(z)$ pero antes necesitamos demostrar un lema técnico.

Lema 2.3 *Si $n \geq 0$ es impar se tiene que*

$$x^n - y^n = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y), \text{ donde } \zeta = e^{\frac{2\pi i}{n}}.$$

Demostración:

$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ son todas las raíces del polinomio $z^n - 1$. Dado que hay n raíces y todas son distintas se tiene que

$$z^n - 1 = \prod_{k=0}^{n-1}(z - \zeta^k).$$

Sea $z = \frac{x}{y}$ y multipliquemos ambos lados por y^n. Se tiene que

$$x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^k y).$$

Dado que n es impar y k recorre un sistema completo de residuos módulo n también lo hace $-2k$.

$$x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^{-2k} y) = \zeta^{-(1+2+\cdots+n-1)} \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y) = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y).$$

En el último paso hemos usado el hecho de que $1 + 2 + 3 + \cdots + (n-1) = \frac{n(n-1)}{2}$ es divisible entre n. □

Proposición 2.3.1 *Si n es un entero positivo impar y $f(z) = e^{2\pi i z} - e^{-2\pi i z}$ entonces*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Demostración:

Sustituyendo $x = e^{2\pi i z}$ y $y = e^{-2\pi i z}$ en el **Lema 2.3** podemos que ver que

$$f(nz) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right)$$

Podemos observar que

$$f\left(z + \frac{k}{n}\right) = f\left(z + \frac{k}{n} - 1\right) = f\left(z - \frac{n-k}{n}\right).$$

También cabe ver que, del mismo modo que k va de $\frac{n+1}{2}$ a $n-1$, $-k$ va de $\frac{n-1}{2}$ a 1. Por tanto

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z + \frac{k}{n}\right) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z - \frac{n-k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Esto completa la prueba. □

Proposición 2.3.2 *Si p es un primo impar, $a \in \mathbb{Z}$ y $a \nmid p$. Entonces*

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right).$$

Demostración:

Por el **Lema 2.1** se tiene que $la \equiv \pm m_l \ (p)$ donde $1 \leq m_l \leq \frac{p-1}{2}$ por lo que la diferencia entre $\frac{la}{p}$ y $\pm\frac{m_l}{p}$ es un entero. Esto implica que

$$f\left(\frac{la}{p}\right) = f\left(\pm\frac{m_l}{p}\right) = \pm f\left(\frac{m_l}{p}\right).$$

El resultado se sigue de tomar el producto en l desde 1 a $\frac{p-1}{2}$ y aplicar el **Lema de Gauss (2.1)**. □

Ahora ya estamos en posición de demostrar la *Ley de Reciprocidad Cuadrática*. Sean p y q primos impares. Por la **Proposición 2.3.2**.

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right).$$

Por la **Proposición 2.3.1**

$$\frac{f\left(q\frac{l}{p}\right)}{f\left(\frac{l}{p}\right)} = \prod_{m=1}^{\frac{q-1}{2}} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).$$

Poniendo las dos ecuaciones juntas

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).$$

Del mismo modo podemos obtener

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{m}{q}+\frac{l}{p}\right) f\left(\frac{m}{q}-\frac{l}{p}\right).$$

Dado que $f\left(\frac{m}{q}-\frac{l}{p}\right) = -f\left(\frac{l}{p}-\frac{m}{q}\right)$ podemos ver que

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

y por tanto que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Esto completa la prueba. ■

Antes de acabar este apartado vamos a dar una formulación equivalente de la *Ley de Reciprocidad Cuadrática*.

Proposición 2.3.3 *Sean p y q primos impares distintos y $a \geq 1$ un entero. Entonces las siguientes afirmaciones son equivalentes:*

(a) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

(b) *Si $p \equiv \pm q \ \ (4a)$, $p \nmid a$ entonces $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Demostración:

Para probar la implicación **(a)** $\Rightarrow$ **(b)** es suficiente probar que **(b)** se cumple con a primo. Para $a = 2$ se sigue de la **Proposición 2.1.3**. Si a es un primo impar por **(a)** se tiene que

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{p}{a}\right).$$

Por tanto, si $p \equiv q \ \ (4a)$ entonces $\left(\frac{p}{a}\right) = \left(\frac{q}{a}\right)$, por lo que

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{q}{a}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{q}\right).$$

Pero $p \equiv q \ \ (4a)$ implica que $p + q - 2 \equiv 0 \ \ (4)$ y el resultado se sigue. Si, por el contrario, $p \equiv -q \ \ (4a)$ se tiene que

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{-q}{a}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{-1}{a}\right)\left(\frac{q}{a}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{a-1}{2}}\left(\frac{q}{a}\right) =$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{a-1}{2}}(-1)^{\frac{q-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{q}\right) = (-1)^{\frac{a-1}{2}\cdot\left(\frac{p+q-2}{2}+1\right)}\left(\frac{a}{q}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{p+q}{2}}\left(\frac{a}{q}\right).$$

Y del mismo modo, de que $p \equiv -q \ \ (4a)$ implica que $p + q \equiv 0 \ \ (4)$, por lo que el resultado se cumple en este caso.

Para probar la implicación **(b)** $\Rightarrow$ **(a)** supongamos antes que nada que $p > q$.

Primero supongamos que $p \equiv q \ \ (4)$. Entonces, $p = q + 4a$ con $a \geq 1$. Se tiene que

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right).$$

Si $p \equiv 1 \ (4)$ entonces $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ lo que nos prueba **(a)**.

Si $p \equiv 3 \ (4)$ entonces $q \equiv 3 \ (4)$ y se obtiene que $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, que es el apartado **(a)** en este caso.

Finalmente, si $p \equiv -q \ \ (4)$ entonces $p + q = 4a$ y

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{q}{p}\right).$$

Por lo tanto, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, que es la afirmación del apartado **(a)** en este caso, o bien p o bien q tiene que ser congruente con 1 módulo 4. La demostración está completa. □

Podemos observar que, por el apartado **(b)** de la **Proposición 2.3.3** se ve que si $\gcd(r, 4a) = 1$ el carácter cuadrático de a es el mismo para *todos* primos de la progresión aritmética $r + 4at$ con $t \in \mathbb{Z}$. Además, el conjunto de primos de esa forma es infinito. Esto se puede probar usando el **Teorema de Dirichlet para sucesiones aritméticas** (0.4) viendo que su densidad es mayor que 0, aunque en esto no nos centraremos en nuestro trabajo.

Capítulo 3

Ley de Reciprocidad Cuadrática usando las sumas cuadráticas de Gauss

3.1. Números algebraicos y enteros algebraicos

Aunque la demostración que acabamos de realizar es ingeniosa, resulta difícil de generalizar para otras situaciones. Este apartado vamos a dar otra prueba que está basada en métodos que podremos usar también para leyes de reciprocidad superiores. En concreto vamos a introducir el concepto de suma de Gauss, aunque antes de eso vamos a definir los conceptos de números algebraicos y enteros algebraicos en esta primera sección.

Definición 3.1 *Un número algebraico es un número complejo α que es una raíz de un polinomio $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$, donde $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q}$ y $a_n \neq 0$.*

Definición 3.2 *Un entero algebraico ω es un número complejo que es una raíz de un polinomio $x^n + b_1x^{n-1} + \cdots + b_n = 0$ donde $b_1, b_2, \ldots, b_n \in \mathbb{Z}$.*

Claramente se cumple que un entero algebraico es un número algebraico. El recíproco es falso, como veremos.

Proposición 3.1.1 *Un número racional $r \in \mathbb{Q}$ es un entero algebraico si y sólo si $r \in \mathbb{Z}$.*

Demostración:

Si $r \in \mathbb{Z}$ entonces r es una raíz de $x - r = 0$. Por tanto, r es un entero algebraico.

Supongamos que $r \in \mathbb{Q}$ y que r es un entero algebraico, es decir, satisface una ecuación $x^n + b_1x^{n-1} + \cdots + b_n = 0$ con $b_1, \ldots, b_n \in \mathbb{Z}$. Sea $r = \frac{c}{d}$, donde c, $d \in \mathbb{Z}$ y podemos asumir que c y d son coprimos. Escribamos $\frac{c}{d}$ en la ecuación y multiplicando ambos lados por d^n nos lleva a

$$c^n + b_1c^{n-1}d + \cdots + b_nd^n = 0.$$

Se sigue que d divide a c^n y, dado que $\gcd(c, d) = 1$ se tiene que $d \mid c$. De nuevo, dado que $\gcd(c, d) = 1$ se tiene que $d = \pm 1$ y por tanto $\frac{c}{d} \in \mathbb{Z}$. $\square$

Los principales resultados de este apartado son que el conjunto de los números algebraicos forman un cuerpo y el conjunto de los enteros algebraicos forma un anillo. Necesitamos algo de trabajo preliminar antes.

Proposición 3.1.2 *Sea V un $\mathbb{Q}$-espacio vectorial finitamente generado y supongamos que $\alpha \in \mathbb{C}$ tiene la propiedad de que $\alpha\gamma \in V$, para todo $\gamma \in V$. Entonces α es un número algebraico.*

Demostración:

Se puede ver que $\alpha\gamma_i \in V$ para $i = 1, 2, \ldots, l$. Por tanto, $\alpha\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j$ donde $a_{ij} \in \mathbb{Q}$. De esto se sigue que

$$\sum_{j=1}^{l}(a_{ij} - \delta_{ij}\alpha)\gamma_j = 0,$$

donde $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ij} = 1$ si $i = j$. Por el **Teorema de Rouché-Frobenius** se tiene que $\mid a_{ij} - \delta_{ij}\alpha \mid = 0$. Si escribimos el determinante entero podemos ver que α satisface un polinomio de grado l con coeficientes racionales. Por tanto, α es un número algebraico. □

Proposición 3.1.3 *El conjunto de los números algebraicos forman un cuerpo, el cual se llama cierre algebraico o clausura algebraica de $\mathbb{Q}$ y se denota como $\overline{\mathbb{Q}}$.*

Demostración:

Supongamos que α_1 y α_2 son números algebraicos. Vamos a probar que $\alpha_1\alpha_2$ y $\alpha_1 + \alpha_2$ son números algebraicos.

Supongamos que

$$\alpha_1^n + r_1\alpha_1^{n-1} + r_2\alpha_1^{n-2} + \cdots + r_n = 0$$

y

$$\alpha_2^m + s_1\alpha_2^{m-1} + s_2\alpha_1^{m-2} + \cdots + s_m = 0,$$

donde r_i, $s_j \in \mathbb{Q}$. Sea V el $\mathbb{Q}$-espacio vectorial obtenido a partir de todas las combinaciones lineales en $\mathbb{Q}$ de $\alpha_1^i\alpha_2^j$ donde $1 \leq i < n$ y $1 \leq j < m$. Para $\gamma \in V$ se tiene que $\alpha_1\gamma, \alpha_2\gamma \in V$.

Vamos a probar que $\alpha_1\gamma \in V$ (el otro caso se prueba análogamente). Se tiene que

$$\gamma = \sum_{i,j=0}^{n-1,\, m-1} r_{ij}\alpha_1^i\alpha_2^j$$

con $r_{ij} \in \mathbb{Q}$. Supongamos que $r_{n-1,j} = 0$ para todo j. Por tanto,

$$\alpha_1\gamma = \sum_{i,j=0}^{n-2,\, m-1} r_{ij}\alpha_1^{i+1}\alpha_2^j$$

y de esto se tiene que $\alpha_1\gamma \in V$. En caso de que $r_{n-1,j} \neq 0$ para algún j, el grado de ese monomio se sale fuera de la base de V pero esto se puede solucionar dado que

$$\alpha_1^n = -r_1\alpha_1^{n-1} - r_2\alpha_1^{n-2} - \cdots - r_n$$

por lo que llegamos al caso inicial. Se tiene también de forma similar que $(\alpha_1 + \alpha_2)\gamma \in V$ y $(\alpha_1\alpha_2)\gamma \in V$. Por la **Proposición 3.1.2** se sigue que tanto $\alpha_1 + \alpha_2$ como $\alpha_1\alpha_2$ son números algebraicos.

Finalmente, si α es un número algebraico, distinto de cero, podemos ver que α^{-1} es un número algebraico. Esto se tiene dado que, como

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

donde $a_i \in \mathbb{Q}$, entonces

$$a_n\alpha^{-n} + a_{n-1}\alpha^{-(n-1)} + \cdots + a_0 = 0.$$

Esto prueba la afirmación. □

Para probar que el conjunto de los enteros algebraicos es un anillo sólo hace falta modificar la demostración anterior ligeramente.

Proposición 3.1.4 *Sea $W \subseteq \mathbb{C}$ un $\mathbb{Z}$-módulo finitamente generado y supongamos que $\omega \in \mathbb{C}$ cumple que $\omega\gamma \in W$ para todo $\gamma \in W$. Entonces ω es un entero algebraico.*

Demostración:

La demostración se sigue de manera exactamente igual a la de la **Proposición 3.1.2** excepto de que ahora $a_{ij} \in \mathbb{Z}$. Al desarrollar la ecuación $\mid a_{ij} - \delta_{ij}\omega \mid = 0$ nos muestra que ω satisface una ecuación mónica de grado l con coeficientes enteros. Por lo tanto, ω es un entero algebraico. □

Proposición 3.1.5 *El conjunto de los enteros algebraicos, el cual denotaremos como Ω a partir de ahora, forman un anillo.*

Demostración:

La demostración se sigue de la **Proposición 3.1.4** del mismo modo que la **Proposición 3.1.3** se sigue de la **Proposición 3.1.2**.

Sean ω_1 y ω_2 dos enteros algebraicos. Probemos que $\omega_1\omega_2$ y $\omega_1 + \omega_2$ también lo son.

Por tanto se tiene que

$$\omega_1^n + b_1\omega_1^{n-1} + b_2\omega_1^{n-2} + \cdots + b_n = 0$$

y

$$\omega_2^m + c_1\omega_2^{m-1} + c_2\omega_1^{m-2} + \cdots + c_m = 0$$

donde b_i, $c_j \in \mathbb{Z}$. Sea W el $\mathbb{Z}$-módulo creado a partir de todas las combinaciones lineales en $\mathbb{Z}$ de $\omega_1^i\omega_2^j$ donde $1 \leq i < n$ y $1 \leq j < m$. Basta probar que para todo $\gamma \in W$ se tiene que $\omega_1\gamma$, $\omega_2\gamma \in W$.

Probemos que $\omega_1\gamma \in W$ (el otro se prueba análogamente). Dado que $\omega \in W$ se tiene que

$$\gamma = \sum_{i,j=0}^{n-1,\, m-1} b_{ij}\omega_1^i\omega_2^j$$

con $b_{ij} \in \mathbb{Z}$. Si se tiene que $b_{n-1,j} = 0$ para todo j entonces

$$\omega_1\gamma = \sum_{i,j=0}^{n-2,\, m-1} b_{ij}\omega_1^{i+1}\omega_2^j$$

y por tanto $\omega_1\gamma \in W$. En caso de que para algún j se tenga que $b_{n-1,j} \neq 0$, el grado de ese monomio se sale fuera de la base de W pero esto se puede solucionar dado que

$$\omega_1^n = -b_1\omega_1^{n-1} - b_2\omega_1^{n-2} - \cdots - b_n$$

al llevándonos caso anterior. Por lo tanto se tiene que $(\omega_1 + \omega_2)\gamma \in W$ y $(\omega_1\omega_2)\gamma \in W$ y por la **Proposición 3.1.4** se sigue que tanto $\omega_1 + \omega_2$ y $\omega_1\omega_2$ son enteros algebraicos. □

Si $\omega_1, \omega_2, \gamma \in \Omega$, decimos que $\omega_1 \equiv \omega_2 \ \ (\gamma)$ (ω_1 es congruente con ω_2 módulo γ) si $\omega_1 - \omega_2 = \gamma\alpha$ con $\alpha \in \Omega$. Esta idea de congruencias satisface todas las propiedades formales de las congruencias en $\mathbb{Z}$.

Si a, b, $c \in \mathbb{Z}$, con $c \neq 0$ entonces se tiene que $a \equiv b \ \ (c)$ es ambigua dado que denota una congruencia tanto en $\mathbb{Z}$ como en Ω. Esta ambigüedad es sólo aparente, sin embargo. Si $a - b = c\alpha$ con $\alpha \in \Omega$ entonces α es tanto un número racional como un entero algebraico por lo que α es un entero ordinario por la **Proposición 3.1.1**.

La siguiente proposición nos será útil.

Proposición 3.1.6 *Si $\omega_1, \omega_2 \in \Omega$ y $p \in \mathbb{Z}$ es un primo, entonces*

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \ \ (p).$$

Demostración:

Se tiene que

$$(\omega_1 + \omega_2)^p = \sum_{k=0}^{p} \binom{p}{k} \omega_1^k \omega_2^{p-k}.$$

Por el **Lema 1.2**, se tiene que $p \mid \binom{p}{k}$ para $1 \leq k \leq p-1$. El resultado se sigue de esto y del hecho de que Ω es un anillo. □

Una raíz de la unidad es una solución de una ecuación de la forma $x^n - 1 = 0$ por lo que las raíces de la unidad son enteros algebraicos, y también lo son las combinaciones lineales en $\mathbb{Z}$ de las raíces de la unidad.

Vamos a concluir este apartado presentando varias propiedades importantes sobre los números algebraicos.

Proposición 3.1.7 *Si α es un número algebraico entonces α es la raíz de un único polinomio mónico irreducible $f(x) \in \mathbb{Q}[x]$. Es más, si $g(x) \in \mathbb{Q}[x]$ con $g(\alpha) = 0$ debe cumplirse que $f(x) \mid g(x)$.*

Demostración:

Sea $f(x)$ un polinomio irreducible con $f(\alpha) = 0$. Vamos a probar primero la segunda afirmación. Si $f(x) \nmid g(x)$ entonces $\gcd(f(x), g(x)) = 1$. Por la *Identidad de Bézout* podemos escribir $f(x)h(x) + g(x)t(x) = 1$ con $h(x), t(x) \in \mathbb{Q}[x]$. Sustituyendo $x = \alpha$ nos da una contradicción. La unicidad se obtiene inmediatamente. □

El polinomio definido en la **Proposición 3.1.7** depende por tanto sólo de α. A este polinomio se le denomina el *polinomio mínimo de* α. Si el grado del polinomio mínimo es n entonces se dice que α es un número algebraico de grado n. Si $f(x)$ es irreducible de grado n entonces, usando el **Teorema Fundamental del Álgebra** y el hecho de que si α es un número algebraico con polinomio mínimo $f(x)$ se tiene que $f(x)$ no tiene raíces repetidas en $\mathbb{C}$, podemos ver que $f(x)$ es el polinomio mínimo para cada una de sus n raíces. Si α, β son raíces de $f(x)$ entonces α y β se dice que son conjugadas.

El conjunto de los números complejos

$$\left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(x), h(x) \in \mathbb{Q}[x],\ h(\alpha) \neq 0 \right\},$$

forma un cuerpo denotado como $\mathbb{Q}(\alpha)$. Denotemos como $\mathbb{Q}[\alpha]$ como al anillo de polinomios en α con coeficientes racionales entonces se tiene el siguente resultado importante.

Proposición 3.1.8 *Si $\alpha \in \overline{\mathbb{Q}}$, entonces $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.*

Demostración:

Claramente $\mathbb{Q}[\alpha] \subset \mathbb{Q}(\alpha)$. Si $h(\alpha) \in \mathbb{Q}(\alpha)$, $h(\alpha) \neq 0$. Entonces, por la **Proposición 3.1.7**, $f(x) \nmid h(x)$ donde $f(x)$ es el polinomio mínimo de α por lo que $\gcd(f(x), h(x)) = 1$ así por la **Identidad de Bézout** se tiene que $s(x)f(x) + t(x)h(x) = 1$ para algunos $s(x), t(x) \in \mathbb{Q}[x]$. Sustituyendo $x = \alpha$ se tiene que $t(\alpha)h(\alpha) = 1$ por lo que $h(\alpha)^{-1} \in \mathbb{Q}[\alpha]$. Si $\beta \in \mathbb{Q}(\alpha)$, se tiene que $\beta = g(\alpha)h(\alpha)^{-1}$ para algunos $g(x), h(x) \in \mathbb{Q}[x]$ y por lo visto anteriormente se tiene que $\beta \in \mathbb{Q}[\alpha]$. □

Corolario 3.1 *Si α es un número algebraico de grado n entonces* $[\mathbb{Q}(\alpha):\mathbb{Q}] = n$.

Demostración:

Por la **Proposición 3.1.8** es suficiente con demostrar que $[\mathbb{Q}[\alpha]:\mathbb{Q}] = n$. Dado que $f(\alpha) = 0$ se puede ver que $1, \ldots, \alpha^{n-1}$ generan $\mathbb{Q}[\alpha]$. Si, por el otro lado,

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0,$$

con $a_i \in \mathbb{Q}$, se tiene que $g(\alpha) = 0$ para

$$g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

Entonces, por la **Proposición 3.1.7** $f(x) \mid g(x)$. Pero $\deg(g(x)) < \deg(f(x))$, lo cual implica que

$$a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0.$$

Por lo tanto $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre $\mathbb{Q}$. □

Cabe destacar que lo visto en esta sección tiene cierto solapamiento con lo impartido en la asignatura **Estructuras Algebraicas**.

3.2. El carácter cuadrático de 2

Sea $\zeta = e^{\frac{2\pi i}{8}}$. Entonces ζ es una raíz primitiva octava de la unidad. Por tanto,

$$0 = \zeta^8 - 1 = (\zeta^4 - 1)(\zeta^4 + 1).$$

Dado que $\zeta^4 \neq 1$, se tiene que $\zeta^4 = -1$. Multiplicando por ζ^{-2} y añadiendo ζ^{-2} a ambos lados se tiene que $\zeta^2 + \zeta^{-2} = 0$. Esta ecuación también se deduce fácilmente de la observación de que $\zeta^2 = e^{\frac{\pi}{2}i} = i$.

El carácter cuadrático de 2 proviene ahora de la relación

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2$$

Sea $\tau = \zeta + \zeta^{-1}$. Podemos ver que ζ y τ son enteros algebraicos. Vamos a trabajar con congruencias en el anillo de los enteros algebraicos.

Sea p un primo impar en $\mathbb{Z}$ y podemos ver que

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \ (p).$$

De esto se sigue que $\tau^p \equiv \left(\frac{2}{p}\right)\tau \ (p)$. Por la **Proposición 3.1.6**, se tiene que

$$\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \ (p).$$

Recordando que $\zeta^8 = 1$ se tiene que $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ para $p \equiv \pm 1 \ (8)$ y $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$ para $p \equiv 3 \ (8)$. El resultado en el último caso puede ser simplificado observando que $\zeta^4 = -1$ lo que implica que $\zeta^3 = -\zeta^{-1}$ por lo que $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$ si $p \equiv \pm 3 \ (8)$. Resumiendo,

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau, & \text{si } p \equiv \pm 1 \ (8) \\ -\tau, & \text{si } p \equiv \pm 3 \ (8) \end{cases}$$

Sustituyendo este resultado en la relación $\tau^p \equiv \left(\frac{2}{p}\right)\tau \ (p)$ nos lleva a que

$$(-1)^{\varepsilon}\tau \equiv \left(\frac{2}{p}\right)\tau \ (p), \text{ donde } \varepsilon \equiv \frac{p^2-1}{8} \ (2).$$

Multiplicando ambos lados de la congruencia por τ se tiene

$$(-1)^{\varepsilon}2 \equiv \binom{2}{p}2 \ \ (p),$$

lo cual implica que

$$(-1)^{\varepsilon} \equiv \binom{2}{p} \ \ (p),$$

La última congruencia implica que $\binom{2}{p} = (-1)^{\varepsilon}$, que es el apartado **(b)** de la **Ley de Reciprocidad Cuadrática**.

3.3. Sumas cuadráticas de Gauss

La igualdad $(\zeta + \zeta^{-1})^2 = 2$ dada en la **Sección 3.2**, uno puede preguntarse si hay una relación similar cuando 2 es reemplazado por un primo impar p. La respuesta es sí, y, es más, la *Ley de Reciprocidad Cuadrática* completa se sigue de esta nueva igualdad usando el método de la **Sección 3.2**.

Durante esta sección ζ denotará $e^{\frac{2\pi i}{p}}$, una raíz primitiva p-ésima de la unidad.

Lema 3.1 *En las condiciones anteriores:*

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & \text{si } a \equiv 0 \ \ (p), \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Demostración:

Si $a \equiv 0 \ \ (p)$, entonces $\zeta^a = 1$, y por tanto, $\sum_{t=0}^{p-1} \zeta^{at} = p$. Si $a \not\equiv 0 \ \ (p)$, entonces $\zeta^a \neq 1$ y

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

Esto concluye la prueba. □

Corolario 3.2 *En las condiciones anteriores:*

$$p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y),$$

donde $\delta(x, y) = 1$ *si* $x \equiv y \ \ (p)$ *y* $\delta(x, y) = 0$ *si* $x \not\equiv y \ \ (p)$.

Demostración:

La demostración es inmediata a partir del **Lema 3.1**. □

Todos los sumatorios de lo que queda de la sección van desde 0 a $p - 1$. Esto simplificará la notación para evitar escribirlo completo cada vez.

Lema 3.2 *En las condiciones anteriores:*

$$\sum_t \left(\frac{t}{p}\right) = 0,$$

donde $\left(\frac{t}{p}\right)$ *es el símbolo de Legendre.*

Demostración:

Por definición, $\left(\frac{0}{p}\right) = 0$. De los $p-1$ términos restantes del sumatorio, la mitad son $+1$ y la mitad son -1 y por el **Corolario 2.1**, existen tantos residuos cuadráticos como residuos no-cuadráticos módulo p. □

Ahora estamos en posición de introducir la noción de suma de Gauss.

Definición 3.3 *Una suma cuadrática de Gauss es una suma de la siguiente forma:*

$$g_a = \sum_t \left(\frac{t}{p}\right)\zeta^{at}.$$

Proposición 3.3.1 *En las condiciones anteriores:*

$$g_a = \left(\frac{a}{p}\right) g_1.$$

Demostración:

Si $a \equiv 0 \pmod{p}$, entonces $\zeta^{at} = 1$ para todo t y $g_a = \sum_t \left(\frac{t}{p}\right) = 0$ por el **Lema 3.2**. Esto nos da el resultado en el caso de que $a \equiv 0 \pmod{p}$.

Ahora supongamos que $a \not\equiv 0 \pmod{p}$

$$\left(\frac{a}{p}\right) g_a = \sum_t \left(\frac{at}{p}\right)\zeta^{at} = \sum_s \left(\frac{s}{p}\right)\zeta^{s} = g_1.$$

Hemos usado el hecho de que at recorre un sistema completo de residuos módulo p cuando t lo hace y que $\left(\frac{s}{p}\right)$ y ζ^s dependen sólo de la clase residual de s módulo p.

Dado que $\left(\frac{a}{p}\right)^2 = 1$ cuando $a \not\equiv 0 \pmod{p}$ nuestro resultado se sigue multiplicando la ecuación $\left(\frac{a}{p}\right) g_a = g_1$ en ambos lados por $\left(\frac{a}{p}\right)$. □

De ahora en adelante denotaremos g_1 como g. Se sigue de la **Proposición 3.3.1** que $g_a^2 = g^2$ si $a \not\equiv 0 \pmod{p}$. Vamos a deducir ahora este valor en común.

Proposición 3.3.2 *En las condiciones anteriores:*

$$g^2 = (-1)^{\frac{p-1}{2}} p.$$

Demostración:

La idea de la demostración es evaluar la suma $\sum_a g_a g_{-a}$ de dos formas. Si $a \not\equiv 0 \pmod{p}$, entonces

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2.$$

Se sigue que

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)g^2.$$

Ahora podemos ver que

$$g_a g_{-a} = \sum_x \sum_y \binom{x}{p}\binom{y}{p}\zeta^{a(x-y)}.$$

Sumando ambos lados sobre a y usando el **Corolario 3.2** nos lleva a que

$$\sum_a g_a g_{-a} = \sum_x \sum_y \binom{x}{p}\binom{y}{p}\delta(x,y)p = (p-1)p.$$

Poniendo juntos estos resultados se obtiene $\binom{-1}{p}(p-1)g^2 = (p-1)p$ y por tanto, $g^2 = \binom{-1}{p}p$. □

Sea $p^* = (-1)^{\frac{p-1}{2}}p$. La ecuación $g^2 = p^*$ es la analogía deseada de la ecuación $\tau^2 = 2$. Sea también $q \neq p$ otro primo impar. Procederemos a probar la *Ley de Reciprocidad Cuadrática* trabajando con congruencias módulo q en el anillo de los enteros algebraicos:

$$g^{q-1} = (g^2)^{\frac{q-1}{2}} = {p^*}^{\frac{q-1}{2}} \equiv \binom{p^*}{q} \ (q).$$

Por lo tanto,

$$g^q \equiv \binom{p^*}{q} g \ (q).$$

Usando la **Proposición 3.1.6** vemos que

$$g^q = \left(\sum_t \binom{t}{p}\zeta^t\right)^q \equiv \sum_t \binom{t}{q}^q \zeta^{qt} \equiv g_q \ (q).$$

De aquí se sigue que $g^q \equiv g_q \equiv \binom{q}{p} g \ (q)$ y entonces

$$\binom{q}{p} g \equiv \binom{p^*}{q} g \ (q).$$

Multiplicando ambos lados por g y usando que $g^2 = p^*$:

$$\binom{q}{p} p^* \equiv \binom{p^*}{q} p^* \ (q),$$

lo cual implica que

$$\binom{q}{p} \equiv \binom{p^*}{q} \ (q),$$

y finalmente

$$\binom{q}{p} = \binom{p^*}{q}.$$

Para ver que este resultado es lo que queremos simplemente debemos ver que

$$\binom{p^*}{q} = \binom{-1}{q}^{\frac{p-1}{2}} \binom{p}{q} = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \binom{p}{q}. \ \blacksquare$$

La noción de sumas cuadráticas de Gauss que hemos usado puede ser generalizada. Las sumas cúbicas y cuárticas de Gauss se usan para probar las *Leyes de Reciprocidad Cúbica y Bicuadrática* respectivamente (las cual se ven en el proyecto complementario).

3.4. El signo de la suma cuadrática de Gauss

De acuerdo a la **Proposición 3.3.2** la suma cuadrática tiene valor

$$g = \begin{cases} \pm\sqrt{p} & \text{si } p \equiv 1 \ \ (4) \\ \pm i\sqrt{p} & \text{si } p \equiv 3 \ \ (4) \end{cases}$$

por lo que el valor de g está determinado por su signo. La determinación del signo es un problema mucho más complicado. Aunque en mayo de 1801 Gauss registró en su diario la conjetura de ambos casos el signo era positivo no fue hasta cuatro años más tarde que se encontró dicha prueba. En esta sección vamos a presentar una de las demostraciones realizadas por Kronecker.

Como en los apartados previos, se tendrá que $\zeta = e^{\frac{2\pi i}{p}}$ por lo que $1, \zeta, \ldots, \zeta^{p-1}$ son las raíces de $x^p - 1$.

Proposición 3.4.1 *El polinomio* $1 + x + \cdots + x^{p-1}$ *es irreducible en* $\mathbb{Q}[x]$.

Demostración:

Aplicando el **Lema de Gauss** visto en la asignatura **Álgebra Básica** bastará demostrar que:

$$1 + x + \cdots + x^{p-1}$$

no tiene una factorización no trivial en $\mathbb{Z}[x]$. Supongamos que, por el contrario, que

$$1 + x + \cdots + x^{p-1} = f(x)g(x)$$

donde $f(x)$, $g(x) \in \mathbb{Z}[x]$ y cada uno tiene grado mayor que uno. Poniendo $x = 1$ nos da que $p = f(1)g(1)$. Por tanto, vamos a asumir que $g(1) = 1$. Usando una barra para denotar la clase módulo p se tiene que $g(\overline{1}) \neq 0$.

Por el otro lado, dado que $p \mid \binom{p}{j}$ para $j = 1, \ldots, p-1$ se tiene que $x^p - 1 \equiv (x-1)^p \ \ (p)$ y dividiendo ambos lados entre $x - 1$ nos muestra que

$$1 + x + \cdots + x^{p-1} \equiv (x-1)^{p-1} \ \ (p).$$

Por la factorización única en polinomios mónicos irreducibles de un polinomio y al estar en cuerpo (al ser p primo) se sigue que

$$g(x) \equiv (x-1)^s \ \ (p)$$

para algún entero positivo s. Sin embargo, esto contradice el hecho de $g(\overline{1}) \neq \overline{0}$. □

Combinando las **Proposiciones 3.4.1 y 3.1.7** podemos ver que si $g(\zeta) = 0$ con $g(x) \in \mathbb{Q}[x]$ entonces

$$(1 + x + \cdots + x^{p-1}) \mid g(x).$$

Esta observación nos será muy útil más adelante.

Proposición 3.4.2

$$\prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^{2k-1} - \zeta^{-(2k-1)}\right)^2 = (-1)^{\frac{p-1}{2}} p.$$

Demostración:

Se tiene que

$$x^p - 1 = (x-1) \prod_{j=1}^{p-1} \left(x - \zeta^j\right).$$

Dividiendo ambos por $x-1$ y sustituyendo $x=1$ se tiene $p=\prod_{j=1}^{p-1}(1-\zeta^j)$ donde el producto recorre un conjunto completo de unidades módulo p. Los enteros $\pm(4k-2)$ con $k=1,\,2,\,\ldots,\,\frac{p-1}{2}$ se puede ver fácilmente que son un sistema completo de residuos. Por tanto

$$p=\prod_k\left(1-\zeta^{4k-2}\right)\prod_k\left(1-\zeta^{-(4k-2)}\right)=$$

$$=\prod_k\left(\zeta^{-(2k-1)}-\zeta^{2k-1}\right)\prod_k\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)=(-1)^{\frac{p-1}{2}}\prod_k\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)^2.$$

donde todos los productos son sobre $k=0,1,2,\ldots,\frac{p-1}{2}$. □

Proposición 3.4.3

$$\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)=\begin{cases}\sqrt{p}, & si\ p\equiv 1\ \ (4),\\ i\sqrt{p}, & si\ p\equiv 3\ \ (4).\end{cases}$$

Demostración:

Por la **Proposición 3.4.2** sólo se tiene que calcular el signo del producto, el cual es

$$i^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}2\,\mathrm{sen}\left(\frac{(4k-2)\pi}{p}\right).$$

Pero

$$\mathrm{sen}\left(\frac{(4k-2)\pi}{p}\right)<0\ \ \text{si}\ \frac{p+2}{4}<k\leq\frac{p-1}{2}.$$

Se sigue que el producto tiene $\frac{p-1}{2}-\left[\frac{p+2}{4}\right]$ términos negativos y se puede ver que son $\frac{p-1}{4}$ o $\frac{p-3}{4}$ dependiendo de si $p\equiv 1\ \ (4)$ o $p\equiv 3\ \ (4)$ respectivamente, en cualquier caso lo denotaremos como $(-1)^k$ con $k\in\mathbb{Z}$.

Por otro lado, se tiene $i^{\frac{p-1}{2}}$:

- Si $p\equiv 1\ (4)$, entonces $p=4k+1$ con $k\in\mathbb{Z}$, por lo que $i^{2k}=(-1)^k$ y, multiplicado por el otro $(-1)^k$, se tiene que es igual a 1.
- Si $p\equiv 3\ (4)$, entonces $p=4k+3$ con $k\in\mathbb{Z}$, por lo cual $i^{2k+1}=(-1)^k i$ y, multiplicado por el otro $(-1)^k$, se tiene que es igual a i.

Con esto se consigue la demostración. □

Por las **Proposiciones 3.3.2 y 3.4.2** sabemos que

$$g=\varepsilon\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right),\tag{3.1}$$

donde $\varepsilon=\pm 1$. La evaluación de las sumas de Gauss es completa por la **Proposición 3.4.3** si podemos ver que $\varepsilon=+1$. El siguiente argumento de Kronecker nos permite ver que es ese el caso.

Proposición 3.4.4 *En las condiciones anteriores se tiene que* $\varepsilon = +1$.

Demostración:

Consideremos el polinomio

$$f(x) = \sum_{j=1}^{p-1} \binom{j}{p} x^j - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} \left(x^{2k-1} - x^{p-(2k-1)} \right). \tag{3.2}$$

Por tanto, $f(\zeta) = 0$ por (3.1) y $f(1) = 0$ por el **Lema 3.2**. Por el comentario anterior a la **Proposición 3.4.2** y por el hecho de que $1+x+\cdots+x^{p-1}$ y $x-1$ son coprimos, podemos concluir que $(x^p-1) \mid f(x)$. Escribamos $(x^p-1)h(x)$ y reemplacemos x por e^z para obtener

$$f(x) = \sum_{j=1}^{p-1} \binom{j}{p} e^{jz} - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} \left(e^{(2k-1)z} - x^{(p-(2k-1))z} \right). \tag{3.3}$$

El coeficiente de $z^{\frac{p-1}{2}}$ en el lado izquierdo de (3.3) se puede ver que es

$$\frac{\sum_{j=1}^{p-1} \binom{j}{p} j^{\frac{p-1}{2}}}{\left(\frac{p-1}{2}\right)!} - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (4k-p-2).$$

Por el otro lado, el coeficiente de $z^{\frac{p-1}{2}}$ por el lado derecho de (3.3) es $\frac{pA}{B}$ donde $p \nmid B$ con A y B enteros. Igualando coeficientes, multiplicando por $B\left(\frac{p-1}{2}\right)!$ y reduciendo módulo p podemos ver que

$$\sum_{j=1}^{p-1} \binom{j}{p} j^{\frac{p-1}{2}} \equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} (4k-2) \equiv$$

$$\equiv \varepsilon(2 \cdot 4 \cdot 6 \cdots (p-1)) \prod_{k=1}^{\frac{p-1}{2}} (2k-1) \equiv \varepsilon(p-1)! \equiv -\varepsilon \ \ (p).$$

usando el Teorema de Wilson (**Corolario 1.2**).

Por la **Proposición 2.1.2** $j^{\frac{p-1}{2}} \equiv \left(\frac{j}{p}\right) \ \ (p)$, así que se tiene

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right)^2 \equiv p-1 \equiv -\varepsilon \ \ (p)$$

y por tanto $\varepsilon \equiv 1 \ \ (p)$.

Dado que $\varepsilon = \pm 1$ concluimos finalmente $\varepsilon = 1$. □

Con todo esto se puede establecer el siguiente resultado:

Teorema 3.1 *El valor de la suma cuadrática de Gauss es*

$$g = \begin{cases} \sqrt{p}, & \text{si } p \equiv 1 \ \ (4) \\ i\sqrt{p}, & \text{si } p \equiv 3 \ \ (4) \end{cases}$$

Capítulo 4

Ley de Reciprocidad Cuadrática usando cuerpos finitos

Ya hemos visto ejemplos de cuerpos finitos, los cuerpos $\mathbb{Z}/\mathbb{Z}p$ donde p es un número primo. En esta sección vamos a probar que hay muchos más cuerpos finitos y vamos a investigar sus propiedades. Esta teoría no es sólo interesante por sí misma sino que además es una herramienta muy útil en investigaciones sobre Teoría de Números. En el último apartado de la sección vamos a dar otra prueba de la *Ley de Reciprocidad Cuadrática*.

4.1. Propiedades básicas de los cuerpos finitos

En este apartado vamos a discutir propiedades de los cuerpos finitos sin preocuparnos sobre preguntas de existencia. La construcción de cuerpos finitos la realizaremos en la **Sección 4.2**.

Sea F un cuerpo finito con q elementos. El grupo multiplicativo F^* de F tiene $q-1$ elementos. Por tanto, para todo $\alpha \in F^*$ satisface la ecuación $x^{q-1} = 1$ (en este contexto 1 representa a la identidad multiplicativa de F y no al entero 1) y todo $\alpha \in F$ satisface la ecuación $x^q = x$.

Proposición 4.1.1

$$x^q - x = \prod_{\alpha \in F} (x - \alpha)$$

Demostración:

Ambos elementos son considerados elementos de $F[x]$.

Todo $\alpha \in F$ es una raíz de $x^q - x$. Dado que F tiene q elementos y dado que el grado $x^q - x$ es q, la demostración se sigue. □

Corolario 4.1 *Sea $F \subset K$ donde K es un cuerpo. Un elemento $\alpha \in K$ está en F si y sólo si $\alpha^q = \alpha$.*

Demostración:

Se puede ver fácilmente que $\alpha^q = \alpha$ si y sólo si α es una raíz de $x^q - x$. Por la **Proposición 2.3.1** las raíces de $x^q - x$ son precisamente los elementos de F. □

Corolario 4.2 *Si $f(x)$ divide a $x^q - x$, entonces $f(x)$ tiene d raíces distintas donde $d = \deg(f(x))$.*

Demostración:

Sea $f(x)g(x) = x^q - x$. El polinomio $g(x)$ tiene grado $q - d$. Si $f(x)$ tiene menos de d raíces distintas, entonces, por el **Lema 1.1**, $f(x)g(x)$ tiene menos de $d + (q - d) = q$ raíces distintas, que no es el caso. □

Teorema 4.1 *El grupo multiplicativo de un cuerpo finito es cíclico.*

Demostración:

Este teorema es una generalización del **Teorema 1.1**. La demostración es casi idéntica.

Si $d \mid (q-1)$, entonces $x^d - 1$ divide a $x^{q-1} - 1$ y se sigue por el **Corolario 4.2** que $x^d - 1$ tiene d raíces distintas. Por tanto, el subgrupo de F^* formado por los elementos que satisfacen $x^d - 1$ tiene orden d.

Sea $\psi(d)$ el número de elementos en F^* de orden d. Por tanto, se tiene que $\sum_{c|d} \psi(c) = d$. Por la **Fórmula de Inversión de Möbius** (0.3)

$$\psi(d) = \sum_{c|d} \mu(c)\frac{d}{c} = \phi(d).$$

En particular, $\psi(q-1) > 1$ a no ser que estemos en el caso trivial de $q = 2$. Esto concluye la demostración. □

El hecho de que F^* sea cíclico cuando F es finito nos permite dar la siguiente generalización parcial de la **Proposición 1.2.1**.

Proposición 4.1.2 *Sea $\alpha \in F^*$. La ecuación $x^n = \alpha$ tiene solución si y sólo si $\alpha^{\frac{q-1}{d}} = 1$ donde $d = \gcd(n, q-1)$. Además, de haber soluciones, hay exactamente d soluciones.*

Demostración:

Sea γ un generador de F^* y establezcamos que $\alpha = \gamma^a$ y $x = \gamma^y$. Por tanto, la ecuación $x^n = \alpha$ es equivalente a la congruencia $ny \equiv a \ \ (q-1)$. Aplicando las propiedades las congruencias del tipo $ax \equiv b \ \ (m)$ se tiene la demostración. □

Merece la pena examinar qué ocurre en los casos extremos $n \mid (q-1)$ y $\gcd(n, q-1) = 1$.

- Si $n \mid (q-1)$, entonces hay exactamente $\frac{q-1}{n}$ elementos de F^* que son potencias n-ésimas y si α es una potencia n-ésima, entonces $x^n = \alpha$ tiene n soluciones.
- Si $\gcd(n, q-1) = 1$, entonces cada elemento es una potencia n-ésima de manera única, es decir, para todo $\alpha \in F^*$ $x^n = \alpha$ tiene una única solución.

Hemos investigado la estructura de F^*. Ahora vamos a prestar nuestra atención al grupo aditivo de F.

Lema 4.1 *Sea F un cuerpo finito. Los elementos múltiplos de la identidad forman un subcuerpo de F es isomorfo a $\mathbb{Z}/\mathbb{Z}p$ para algún número primo p.*

Demostración:

Para no generar confusiones, vamos a llamar temporalmente e a la identidad de F^* en vez de 1. Consideremos una aplicación de $\mathbb{Z}$ en F que lleva n en ne. Se puede ver fácilmente que se puede extender a un homomorfismo de anillos. La imagen es un subanillo finito de F y en particular es un dominio de integridad. El núcleo es un ideal primo no nulo. Por lo tanto, la imagen es isomorfa a $\mathbb{Z}/\mathbb{Z}p$ para algún primo p. □

Debemos identificar $\mathbb{Z}/\mathbb{Z}p$ con su imagen en F y pensemos en F como un espacio vectorial de dimensión finita sobre $\mathbb{Z}/\mathbb{Z}p$. Denotemos n a esa dimensión y sea $\omega_1, \omega_2, \ldots, \omega_n$ una base. Se cumple que cualquier $\omega \in F$ puede ser expresado de manera única de la forma $a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$ donde $a_i \in \mathbb{Z}/\mathbb{Z}p$. Se sigue que F tiene p^n elementos. Hemos probado entonces que

Proposición 4.1.3 *El número de elementos de un cuerpo finito es una potencia de un primo.*

Si e es la identidad del cuerpo finito F, sea p el menor entero tal que $pe = 0$. Hemos visto que p debe ser un número primo, que denominaremos la *característica de* F. Para $\alpha \in F$ se tiene que

$$p\alpha = p(e\alpha) = (pe)\alpha = 0 \cdot \alpha = 0.$$

Esta observación nos lleva la siguiente proposición.

Proposición 4.1.4 *Si F tiene característica p, se cumple la siguiente igualdad:*

$$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} \quad \forall \alpha, \beta \in F, \ \ \forall d \in \mathbb{Z}.$$

Demostración:

Esta prueba la haremos por inducción sobre d. Para $d = 1$ se tiene

$$(\alpha + \beta)^p = \alpha^p + \sum_{k=1}^{p-1} \alpha^{p-k}\beta^k + \beta^p = \alpha^p + \beta^p.$$

Todos los términos intermedios desaparecen porque $p \mid \binom{p}{k}$ para $1 \leq k \leq p-1$ por el **Lema 1.2**.

Para pasar de d a $d+1$ sólo elevamos ambos lados de $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ a la p-ésima potencia. □

Supongamos que F es un cuerpo finito de dimensión n sobre $\mathbb{Z}/\mathbb{Z}p$. Queremos encontrar qué cuerpos E hay entre $\mathbb{Z}/\mathbb{Z}p$ y F. Si d es la dimensión de E sobre $\mathbb{Z}/\mathbb{Z}p$, entonces se tiene trivialemente que $d|n$. Resultará que hay un solo cuerpo intermedio correspodiente a cada divisor d de n, como veremos más adelante.

Lema 4.2 *Sea F un cuerpo. Se cumple que $(x^l - 1) \mid (x^m - 1)$ en $F[x]$ si y sólo si $l \mid m$.*

Demostración:

Sea $m = ql + r$ donde $0 \leq r < l$ y $q \in \mathbb{Z}$. Entonces se tiene

$$\frac{x^m - 1}{x^l - 1} = x^r \frac{x^{ql} - 1}{x^l - 1} + \frac{x^r - 1}{x^l - 1}.$$

Dado que $\frac{x^{ql}-1}{x^l-1} = (x^l)^{q-1} + (x^l)^{q-2} + \cdots x^l + 1$, nos lleva a que el término de la derecha de la ecuación anterior es un polinomio si y sólo si $\frac{x^r-1}{x^l-1}$ es un polinomio. Ese es el caso si y sólo si $r = 0$. Por tanto, $l \mid m$. □

Lema 4.3 *Si a es un entero positivo, entonces $(a^l - 1) \mid (a^m - 1)$ si y sólo si $l \mid m$.*

Demostración:

La prueba es análoga a la del **Lema 4.2** con el número a jugando el rol de x. Sea $m = ql + r$ donde $0 \leq r < l$ y $q \in \mathbb{Z}$. Entonces se tiene

$$\frac{a^m - 1}{a^l - 1} = a^r \frac{a^{ql} - 1}{a^l - 1} + \frac{a^r - 1}{a^l - 1}.$$

Dado que $\frac{a^{ql}-1}{a^l-1} = (a^l)^{q-1} + (a^l)^{q-2} + \cdots a^l + 1$, el término de la derecha de la igualdad anterior es un entero si y sólo si $\frac{a^r-1}{a^l-1}$ es un entero. Ese es el caso si y sólo si $r = 0$. Por tanto, $l \mid m$. □

Proposición 4.1.5 *Sea F un cuerpo finito de dimensión n sobre $\mathbb{Z}/\mathbb{Z}p$. Los subcuerpos de F están en correspondencia uno a uno con los divisores de n.*

Demostración:

Supongamos que $d \mid n$. Sea $E = \{\alpha \in F \mid \alpha^{p^d} = \alpha\}$. Vamos a probar que E es un cuerpo. Si α, $\beta \in F$ entonces

(a) $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta$.

(b) $(\alpha\beta)^{p^d} = \alpha^{p^d}\beta^{p^d} = \alpha\beta$.

(c) $(\alpha^{-1})^{p^d} = (\alpha^{p^d})^{-1} = \alpha^{-1}$ para $\alpha \neq 0$.

En el apartado **(a)** hacemos uso de la **Proposición 4.1.4**.

Ahora E es el conjunto de soluciones de $x^{p^d} - x = 0$. Dado que $d \mid n$ se tiene $(p^d - 1) \mid (p^n - 1)$ y $(x^{p^d-1} - 1) \mid (x^{p^n-1} - 1)$ por los **Lemas 4.2 y 4.3**. Por tanto, $(x^{p^d} - x) \mid (x^{p^n} - x)$ y por el **Corolario 4.2**, se tiene que E tiene p^d elementos y tiene dimensión d sobre $\mathbb{Z}/\mathbb{Z}p$.

Finalmente, si E' es otro subcuerpo de F de dimensión sobre $\mathbb{Z}/\mathbb{Z}p$, entonces los elementos de E' deben cumplir que $x^{p^d} - x = 0$, es decir E' debe coincidir con E. □

4.2. La existencia de cuerpos finitos

A partir de ahora vamos a denotar $\mathbb{Z}/\mathbb{Z}q$ al cuerpo finito de q elementos. En la **Sección 4.1** hemos probado que el número de elementos en un cuerpo finito tiene la forma p^n donde p es un primo. Ahora vamos a mostrar que dado un número p^n existe un cuerpo finito con p^n elementos. Para hacerlo necesitamos algunos resultados de *Teoría de Cuerpos* que conecta nuestro problema con la existencia de polinomios irreducibles. Entonces debemos probar un teorema (volviendo a Gauss) que nos muestra que $\mathbb{Z}/\mathbb{Z}p[x]$ contiene polinomios irreducibles de cada grado.

Sea k un cuerpo arbitrario y $f(x)$ un polinomio irreducible en $k[x]$. Se tiene entonces:

Proposición 4.2.1 *Existen un cuerpo $K \supset k$ y un elemento $\alpha \in K$ tal que $f(\alpha) = 0$.*

Demostración:

Sabiendo que $k[x]$ es un dominio de ideales principales, se sigue que $(f(x))$ es un ideal maximal y entonces $k[x]/(f(x))$ es un cuerpo. Sea $K' = k[x]/(f(x))$ y sea ϕ el homomorfismo que va de $k[x]$ en K' llevando cada elemento en su clase módulo $(f(x))$. Se tiene el diagrama

$$\begin{array}{ccc} k[x] & \xrightarrow{\phi} & K' \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\ k & \xrightarrow{\phi/k} & \phi(k) \end{array}$$

Se tiene que $\phi(k)$ es un subcuerpo de K'. Vamos a probar que es isomorfo a k. Es suficiente mostrar que ϕ restringido a k es biyectivo. Sea $a \in k$. Si $\phi(a) = 0$ entonces $a \in (f(x))$. Si $a \neq 0$, es una unidad y no puede haber un elemento de un ideal propio. Por tanto, $a = 0$, como queríamos probar.

Dado que ϕ es un isomorfismo de k vamos a identificar k con $\phi(k)$. Una vez hecho vamos a renombrar K' como K.

Sea α la clase de x en K. Entonces $0 = \phi(f(x)) = f(\phi(x)) = f(\alpha)$, es decir, α es una raíz de $f(x)$ en K. □

Denotemos a este cuerpo K como $k(\alpha)$.

Proposición 4.2.2 *Los elementos* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *son una base del espacio vectorial para* $k(\alpha)$ *sobre* k*, donde* n *es el grado de* $f(x)$*.*

La demostración de esta proposición es la misma que la de la **Proposición 3.1.8** y el **Corolario 3.1** pero reemplazando $\mathbb{Q}$ por k y el número complejo α por el α descrito antes.

La proposición nos muestra que si queremos encontrar una extensión de cuerpos K de k de grado n entonces es suficiente con dar un polinomio irreducible $f(x) \in k[x]$ de grado n.

En $\mathbb{Z}/\mathbb{Z}p[x]$ hay un número finito de polinomios para un grado dado. Sea $F_d(x)$ el producto de polinomios mónicos irreducibles en $\mathbb{Z}/\mathbb{Z}p[x]$ de grado d.

Teorema 4.2 *En las condiciones anteriores:*

$$x^{p^n} - x = \prod_{d|n} F_d(x)$$

Demostración:

Antes de nada podemos ver que si $f(x)$ divide a $x^{p^n} - x$, entonces $f(x)^2$ no divide a $x^{p^n} - x$. Si fuera así, se sigue que

$$-1 = 2f(x)f'(x)g(x) + f(x)^2 g'(x)$$

por derivación formal. Esto es imposible dado que implica que $f(x)$ divide a 1.

Nos queda por probar que si $f(x)$ es un polinomio mónico irreducible de grado d entonces $f(x) \mid (x^{p^n} - x)$ si y sólo si $d \mid n$.

Consideremos $K = \mathbb{Z}/\mathbb{Z}p(\alpha)$ donde α es una raíz de $f(x)$, como en la **Proposición 4.2.2**. Entonces K tiene dimensión d sobre $\mathbb{Z}/\mathbb{Z}p$ y tiene p^d elementos. Los elementos de K satisfacen $x^{p^d} - x = 0$.

Asumamos que $x^{p^n} - x = f(x)g(x)$. Entonces $\alpha^{p^n} = \alpha$. Si

$$b_1\alpha^{d-1} + b_2\alpha^{d-2} + \cdots + b_d$$

es un elemento cualquiera de K entonces

$$(b_1\alpha^{d-1} + b_2\alpha^{d-2} + \cdots + b_d)^{p^n} = b_1(\alpha^{p^n})^{d-1} + \cdots + b_d = b_1\alpha^{d-1} + \cdots + b_d.$$

Por tanto, los elementos de K satisfacen $x^{p^d} - x = 0$. Se sigue que $x^{p^d} - x$ divide $x^{p^n} - x$ y por los **Lemas 4.2** y **4.3**, d divide n.

Asumamos ahora que $d \mid n$. Dado que $\alpha^{p^d} = \alpha$ y $f(x)$ es un polinomio mónico irreducible para α se tiene que $f(x) \mid (x^{p^d} - x)$. Del mismo modo, dado que $d \mid n$ se tiene que $(x^{p^d} - x) \mid (x^{p^n} - x)$ otra vez por los **Lemas 4.2** y **4.3**. Por lo tanto $f(x) \mid (x^{p^n} - x)$. □

Sea N_d el número de polinomios mónicos irreducibles de grado d en $\mathbb{Z}/\mathbb{Z}p[x]$. Igualando los grados en ambos lados de la identidad del **Teorema 4.2** nos lleva a

Corolario 4.3 *En las condiciones anteriores:*

$$p^n = \sum_{d|n} dN_d.$$

Corolario 4.4 *En las condiciones anteriores:*

$$N_n = n^{-1} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Demostración:

Aplicando la **Fórmula de Inversión de Möbius** (0.3) a la ecuación del **Corolario 4.3** se tiene la demostración. □

Corolario 4.5 *Para todo entero $n \geq 1$ existe un polinomio irreducible de grado n en $\mathbb{Z}/\mathbb{Z}p[x]$.*

Demostración:

Se tiene que $N_n = n^{-1}(p^n - \cdots + p\mu(n))$ por el **Corolario 4.4**. El término entre paréntesis no puede ser cero dado que es la suma de distintas potencias de p con coeficientes 1 y -1. □

Resumiendo se tiene que

Teorema 4.3 *Sea $n \geq 1$ un entero y p un primo. Entonces existe un cuerpo finito con p^n elementos.*

4.3. Una aplicación a los residuos cuadráticos

En el **Capítulo 3** hemos probado la *Ley de Reciprocidad* usando las sumas de Gauss y los elementos de la teoría de números algebraicos. Ahora vamos a dar una prueba extremadamente corta usando cuerpos finitos.

Sea p y q distintos primos impares. Dado que $\gcd(p, q) = 1$ hay un entero n (por ejemplo, $p-1$) tal que $q^n \equiv 1 \quad (p)$. Sea F un cuerpo finito de dimensión n sobre $\mathbb{Z}/\mathbb{Z}q$. Entonces F^* es cíclico de orden $q^n - 1$. Sea γ un generador de F^* y definamos $\lambda = \gamma^{\frac{q^n-1}{p}}$. Entonces λ tiene orden p. Definamos

$$\tau_a = \sum_{t=0}^{p-1} \binom{t}{p} \lambda^{at},$$

donde $a \in \mathbb{Z}$. El elemento $\tau_a \in F$ es análogo al visto en el **Capítulo 3** de las sumas cuadráticas de Gauss. Definamos $\tau_1 = \tau$. Por tanto, las demostraciones de las **Proposiciones 3.3.1** y **3.3.2** pueden ser usadas para mostrar que

(1) $\tau_a = \binom{a}{p}\tau$.

(2) $\tau^2 = (-1)^{\frac{p-1}{2}}\overline{p}$.

En la igualdad **(2)**, $\overline{p}$ es la clase p en $\mathbb{Z}/\mathbb{Z}q$. Sea $p^* = (-1)^{\frac{p-1}{2}}p$. Entonces la igualdad **(2)** podemos escribirla como

$$\tau^2 = \overline{p^*},$$

lo cual implica que $\binom{p^*}{q} = 1$ si y sólo si $\tau \in \mathbb{Z}/\mathbb{Z}q$. Por el **Corolario 4.1** esto se cumple si y sólo si $\tau^q = \tau$. Ahora

$$\tau^q = \left(\sum_t \binom{t}{p}\lambda^t\right)^q = \sum_t \binom{t}{p}\lambda^{qt} = \tau_q.$$

En la igualdad (1) se tiene

$$\tau_q = \binom{q}{p}\tau.$$

Por lo tanto,

$$\tau^q = \tau \iff \binom{q}{p} = 1.$$

Por lo que hemos probado que

$$\left(\frac{p^*}{q}\right) = 1 \Longleftrightarrow \left(\frac{q}{p}\right) = 1.$$

Esto nos prueba la *Ley de Reciprocidad Cuadrática*. ■

Una demostración de que $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$ puede ser dada usando la misma técnica. En el **Capítulo 3** dimos la prueba de que $\left(\frac{2}{q}\right) = 1$ si $q \equiv 1 \ (8)$. Si $q \not\equiv 1 \ (8)$, es en cualquier caso cierto que $q^2 \equiv 1 \ (8)$. En este caso podemos resolverlo en un cuerpo finito F de dimensión 2 sobre $\mathbb{Z}/\mathbb{Z}q$. Se puede ver que 2 siempre es residuo cuadrático. Esto se puede probar de la siguiente manera:

Se sabe que F tiene q^2 elementos y por tanto F^* tiene $q^2 - 1$ elementos y además es un grupo cíclico. Sea λ un posible generador de F^*, el cual cumple que:

$$\lambda^{q^2-1} \equiv 1 \ (q)$$

Definamos entonces $\zeta = \lambda^{\frac{q^2-1}{8}}$, el cual se puede ver que tiene orden 8. A partir de aquí usaremos lo visto en la **Sección 3.2** y dado que, como se puede probar fácilmente, existe ζ^{-1} entonces se tiene que

$$\alpha^2 = (\zeta + \zeta^{-1})^2 = 2$$

por lo que 2 es un residuo cuadrático en F.

Por otro lado, 2 es residuo cuadrático en $\mathbb{Z}/\mathbb{Z}q$ si y sólo si $\alpha \in \mathbb{Z}/\mathbb{Z}q$. Esto es equivalente, dado que $\mathbb{Z}/\mathbb{Z}q$ es un cuerpo finito, a que

$$\alpha^q \equiv \alpha \ (q)$$

De lo que se tiene que

$$\alpha^{q-1} \equiv 1 \ (q)$$

De lo cual, dado que $\alpha^2 = 2$, se tiene que

$$2^{\frac{q-1}{2}} \equiv 1 \ (q)$$

Con esto hemos demostrado, usando cuerpos finitos, los resultados previos a la primera demostración de la *Ley de Reciprocidad Cuadrática* para 2. A partir de aquí, usando **Proposición 2.1.3** se tiene que 2 es residuo cuadrático en $\mathbb{Z}/\mathbb{Z}q$ si y sólo $q \equiv \pm 1 \ (8)$.

Capítulo 5

Ley de Reciprocidad Cuadrática usando las sumas de Jacobi

5.1. Caracteres multiplicativos

Antes de ponernos con la *Ley de Reciprocidad Cuadrática* en sí vamos a necesitar generalizar el concepto de *sumas de Gauss* definido en el **Capítulo 3** en su versión cuadrática.

También nos va a interesar considerar el problema de contar el número de soluciones de ecuaciones con coeficientes en un cuerpo finito. Esto nos llevará a definir el concepto de *suma de Jacobi*.

Definición 5.1 *Un carácter multiplicativo en $\mathbb{Z}/\mathbb{Z}p$ es una aplicación que va $(\mathbb{Z}/\mathbb{Z}p)^*$ en los números complejos no nulos que satisface*

$$\chi(ab) = \chi(a)\chi(b) \quad \forall a, b \in (\mathbb{Z}/\mathbb{Z}p)^*.$$

Es decir, es un homomorfismo de grupos multiplicativos.

El símbolo de Legendre, $\left(\frac{a}{p}\right)$, es un ejemplo de un carácter si se ve como una función de la clase de a módulo p.

Otro ejemplo es el carácter multiplicativo trivial definida por

$$\varepsilon(a) = 1, \quad \forall a \in (\mathbb{Z}/\mathbb{Z}p)^*.$$

Va a ser útil extender el dominio de la definición de un carácter multiplicativo a todo $\mathbb{Z}/\mathbb{Z}p$. Si $\chi \neq \varepsilon$, asumiremos que $\chi(0) = 0$. Para ε denotaremos $\varepsilon(0) = 1$.

Proposición 5.1.1 *Sea χ un carácter multplicativo y $a \in \mathbb{Z}/\mathbb{Z}p$. Entonces*

(a) $\chi(1) = 1$[1].

(b) $\chi(a)$ *es una raíz $(p-1)$-ésima de la unidad.*

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Demostración:

Para probar el apartado **(a)** usaremos que $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Entonces $\chi(1) = 1$ dado que $\chi(1) \neq 0$.

Para probar el apartado **(b)** usaremos que la ecuación $a^{p-1} = 1$ implica que $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.

El apartado **(c)** se tiene trivialmente por ser un homomorfismo y porque si ζ es una raíz n-ésima, entonces $\zeta^{-1} = \overline{\zeta}$. □

[1] Cabe mencionar que en el apartado **(a)** el 1 en el lado izquierdo es la unidad de $\mathbb{Z}/\mathbb{Z}p$ mientras que el 1 en el lado derecho es el número complejo 1. La barra del apartado **(c)** es el conjugado complejo.

Proposición 5.1.2 *Sea χ un carácter multplicativo. Entonces*

$$\sum_{t\in\mathbb{Z}/\mathbb{Z}p}\chi(t)=\begin{cases}0 & si\ \chi\neq\varepsilon,\\ p & si\ \chi=\varepsilon.\end{cases}$$

Demostración:

El caso $\chi=\varepsilon$ es obvio así que asumiremos que $\chi\neq\varepsilon$. En este caso hay un elemento $a\in(\mathbb{Z}/\mathbb{Z}p)^*$ tal que $\chi(a)\neq 1$. Sea $T=\sum_{t\in\mathbb{Z}/\mathbb{Z}p}\chi(t)$. Entonces

$$\chi(a)T=\sum_{t\in\mathbb{Z}/\mathbb{Z}p}\chi(a)\chi(t)=\sum_{t\in\mathbb{Z}/\mathbb{Z}p}\chi(at)=T.$$

La última igualdad se sigue de que at recorre todos los elementos de $\mathbb{Z}/\mathbb{Z}p$ del mismo modo que lo hace t. Dado que $\chi(a)T=T$ y que $\chi(a)\neq 1$ se tiene que $T=0$. □

Veamos que los caracteres multiplicativos forman un grupo. Vamos a obviar a partir de ahora la palabra *multiplicativo*.

(1) Si χ y λ son caracteres, entonces $\chi\lambda$ es la aplicación que lleva el elemento $a\in(\mathbb{Z}/\mathbb{Z}p)^*$ en $\chi(a)\lambda(a)$.

Probemos que $\chi\lambda$ es un carácter:

Sean $a,\ b\in(\mathbb{Z}/\mathbb{Z}p)^*$. Dado que $(\mathbb{Z}/\mathbb{Z}p)^*$ es un grupo entonces $ab\in(\mathbb{Z}/\mathbb{Z}p)^*$ y por la definición de $\chi\lambda$ se tiene que:

$$\chi\lambda(ab)=\chi(ab)\lambda(ab)$$

Dado que tanto χ como λ son caracteres se tiene que:

$$\begin{cases}\chi(ab) &= \chi(a)\chi(b)\\ \lambda(ab) &= \lambda(a)\lambda(b)\end{cases}$$

Por lo tanto tenemos:

$$\chi\lambda(ab)=\chi(a)\chi(b)\lambda(a)\lambda(b)$$

Usando la conmutatividad del producto en $(\mathbb{Z}/\mathbb{Z}p)^*$ se tiene que

$$\chi\lambda(ab)=\chi(a)\lambda(a)\chi(b)\lambda(b)$$

Si volvemos a aplicar la definición de $\chi\lambda$ se tiene que

$$\chi\lambda(ab)=\chi\lambda(a)\chi\lambda(b)$$

que es lo queríamos probar.

(2) Si χ es un carácter, entonces χ^{-1} es la aplicación que lleva el elemento $a\in(\mathbb{Z}/\mathbb{Z}p)^*$ en $\chi(a)^{-1}$.

Probemos que χ^{-1} es un carácter:

Sean $a,\ b\in(\mathbb{Z}/\mathbb{Z}p)^*$. Por ser $(\mathbb{Z}/\mathbb{Z}p)^*$ un grupo se tiene que $ab\in(\mathbb{Z}/\mathbb{Z}p)^*$ y por la definición de χ^{-1} se tiene que:

$$\chi^{-1}(ab)=\chi(ab)^{-1}$$

Dado que tanto χ es un carácter se tiene que:

$$\chi(ab)=\chi(a)\chi(b)$$

Por lo tanto tenemos:

$$\chi^{-1}(ab) = (\chi(a)\chi(b))^{-1}$$

Usando que se cumple que la potencia del producto es igual al producto de las potencias en $(\mathbb{Z}/\mathbb{Z}p)^*$ tiene que

$$\chi^{-1}(ab) = \chi(a)^{-1}\chi(b)^{-1}$$

Si volvemos a aplicar la definición de χ^{-1} se tiene que

$$\chi^{-1}(ab) = \chi^{-1}(a)\chi^{-1}(b)$$

que es lo queríamos probar.

Además, se tiene trivialmente que la identidad es este grupo es el carácter ε.

Proposición 5.1.3 *El grupo de los caracteres es un grupo cíclico de orden $p-1$. Si $a \in (\mathbb{Z}/\mathbb{Z}p)^*$ y $a \neq 1$, entonces hay un carácter χ tal que $\chi(a) \neq 1$.*

Demostración:

Sabemos que $(\mathbb{Z}/\mathbb{Z}p)^*$ es cíclico (por el **Teorema 1.1**). Sea $g \in (\mathbb{Z}/\mathbb{Z}p)^*$ un generador. Entonces cualquier elemento $a \in (\mathbb{Z}/\mathbb{Z}p)^*$ es una potencia de g. Si $a = g^l$ y χ es un carácter, entonces $\chi(a) = \chi(g)^l$. Esto nos muestra que χ está completamente determinado por el valor de $\chi(g)$. Dado que $\chi(g)$ es una $(p-1)$-ésima raíz de la unidad y dado que hay $p-1$ de ellas, se sigue que el grupo de los carácteres tiene orden a lo sumo $p-1$.

Ahora definamos una función λ por la ecuación $\lambda(g^k) = e^{\frac{2\pi ik}{p-1}}$. Se puede ver fácilmente que λ está bien definida y es un carácter. Se va a probar que $p-1$ es el menor entero n tal que $\lambda^n = \varepsilon$.

Si $\lambda^n = \varepsilon$, entonces $\lambda^n(g) = \varepsilon(g) = 1$. Sin embargo,

$$\lambda^n(g) = \lambda(g)^n = e^{\frac{2\pi in}{p-1}}.$$

De lo cual se sigue que $(p-1) \mid n$. Dado que

$$\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1$$

tenemos que $\lambda^{p-1} = \varepsilon$. Hemos establecido que los carcteres ε, λ, λ^2, $\ldots$, λ^{p-2} son todas distintas. Dado que, por la primera parte de la prueba, hay a lo sumo $p-1$ caracteres, se tiene que hay exactamente $p-1$ caracteres y que el grupo es cíclico con λ como generador.

Si $a \in (\mathbb{Z}/\mathbb{Z}p)^*$ y $a \neq 1$ entonces $a = g^l$ con $(p-1) \nmid l$. Se tiene que

$$\lambda(a) = \lambda(g)^l = e^{\frac{2\pi il}{p-1}} \neq 1.$$

Esto concluye la prueba. □

Corolario 5.1 *Si $a \in \mathbb{Z}/\mathbb{Z}p$ y $a \neq 1$, entonces $\sum_\chi \chi(a) = 0$, donde el sumatorio es sobre todos los caracteres.*

Demostración:

Sea $S = \sum_\chi \chi(a)$. Dado que $a \neq 1$ hay, por la **Proposición 5.1.3**, un carácter λ tal que $\lambda(a) \neq 1$. Entonces

$$\lambda(a)S = \sum_\chi \lambda(a)\chi(a) = \sum_{\lambda\chi} \lambda\chi(a) = S.$$

La última igualdad se tiene dado que $\lambda\chi$ recorre todos los caracteres, del mismo modo que χ lo hace. Se sigue que $(\lambda(a) - 1)S = 0$ y por tanto $S = 0$. □

Los caracteres pueden resultarnos muy útiles en el estudio de ecuaciones. Para ilustrarlo, consideremos la ecuación $x^n = a$ con $a \in (\mathbb{Z}/\mathbb{Z}p)^*$. Por la **Proposición 1.2.1**, se tiene que una solución existe si y sólo si $a^{\frac{p-1}{d}} = 1$ donde $d = \gcd(n, p-1)$ y, si existe una solución, entonces hay exactamente d soluciones. Por simplicidad, vamos a asumir que $n \mid (p-1)$ y por tanto, $d = \gcd(n, p-1) = n$.

Ahora se va dar un criterio para la solución de la ecuación $x^n = a$ usando caracteres.

Proposición 5.1.4 *Si $a \in (\mathbb{Z}/\mathbb{Z}p)^*$, $n \mid (p-1)$ y $x^n = a$ no tiene solución, entonces hay un carácter χ tal que*

(a) $\chi^n = \varepsilon$.

(b) $\chi(a) \neq 1$.

Demostración:

Sean g y λ como en la **Proposición 5.1.3** y definamos $\chi = \lambda^{\frac{p-1}{n}}$. Entonces

$$\chi(g) = \lambda^{\frac{p-1}{n}}(g) = \lambda(g)^{\frac{p-1}{n}} = e^{\frac{2\pi i}{n}}.$$

Sea $a = g^l$ para algún l, y dado que $x^n = a$ no tiene solución, se tiene que $n \nmid l$. Entonces

$$\chi(a) = \chi(g)^l = e^{\frac{2\pi i l}{n}} \neq 1.$$

Finalmente, $\chi^n = \lambda^{p-1} = \varepsilon$. □

Para un elemento $a \in (\mathbb{Z}/\mathbb{Z}p)^*$, denotemos a $N(x^n - a)$ como el número de soluciones para la ecuación $x^n = a$. Si $n \mid (p-1)$, se tiene que

Proposición 5.1.5

$$N(x^n - a) = \sum_{\chi^n = \varepsilon} \chi(a)$$

donde el sumatorio recorre todos los caracteres de orden divisor de n.

Demostración:

Se va a probar primero que hay exactamente n caracteres de orden divisor de n. Dado que el valor de $\chi(g)$ para ese carácter debe ser una raíz n-ésima de la raíz, hay, a lo sumo, n de esos caracteres. En la **Proposición 5.1.4** se pudo encontrar un carácter χ tal que $\chi(g) = e^{\frac{2\pi i}{n}}$. Se sigue que ε, χ, χ^2, …, χ^{n-1} son n caracteres distintos de orden disivor de n.

Para probar la fórmula, se tiene que $x^n = 0$ tiene una solución, $x = 0$. Por otro lado, $\sum_{\chi^n = \varepsilon} \chi(0) = 1$, dado que $\varepsilon(0) = 1$ y $\chi(0) = 0$ para $\chi \neq \varepsilon$.

Ahora supongamos que $a \neq 0$ y que $x^n = a$ tiene solución, es decir, hay un elemento b tal que $b^n = a$. Si $\chi^n = \varepsilon$, entonces

$$\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \varepsilon(b) = 1.$$

Por tanto,

$$\sum_{\chi^n = \varepsilon} \chi(a) = n,$$

que es $N(x^n - a)$ en este caso.

Finalmente, supongamos que $a \neq 0$ y que $x^n = a$ no tiene solución. Vamos a probar que

$$\sum_{\chi^n = \varepsilon} \chi(a) = 0.$$

Denotemos la suma anterior como T. Por la **Proposición 5.1.4**, hay un carácter ρ tal que $\rho(a) \neq 1$ y $\rho^n = \varepsilon$. Un cálculo sencillo muestra que $\rho(a)T = T$ (usando el hecho de que los caracteres de orden divisor de n forman un grupo). Entonces, $(\rho(a) - 1)T = 0$ y por tanto, $T = 0$, tal y como queríamos demostrar. □

Como un caso especial, se supone que p es impar y $n = 2$. Entonces, la **Proposición 5.1.5** dice que

$$N(x^2 - a) = 1 + \left(\frac{a}{p}\right),$$

donde $\left(\frac{a}{p}\right)$ es el símbolo de Legendre.

En la **Sección 5.3** volveremos a las ecuaciones sobre $\mathbb{Z}/\mathbb{Z}p$.

5.2. Sumas de Gauss

En el **Capítulo 3** introdujimos las sumas cuadráticas de Gauss. La próxima definición generaliza ese concepto.

Definición 5.2 *Sea χ un carácter de $\mathbb{Z}/\mathbb{Z}p$ y $a \in \mathbb{Z}/\mathbb{Z}p$. Sea $g_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}$ y $\zeta = e^{\frac{2\pi i}{p}}$. Se dice que $g_a(\chi)$ es la suma de Gauss sobre $\mathbb{Z}/\mathbb{Z}p$ asociada al carácter χ.*

Proposición 5.2.1 *Sea $g_a(\chi)$ la suma de Gauss sobre $\mathbb{Z}/\mathbb{Z}p$ asociada al carácter χ. Se cumple la siguiente igualdad:*

$$g_a(\chi) = \begin{cases} \chi(a^{-1})g_1(\chi) & \text{si } a \neq 0 \text{ y } \chi \neq \varepsilon \\ 0 & \text{si } a \neq 0 \text{ y } \chi = \varepsilon \\ 0 & \text{si } a = 0 \text{ y } \chi \neq \varepsilon \\ p & \text{si } a = 0 \text{ y } \chi = \varepsilon \end{cases}$$

Demostración:

Veamos el primer caso. Multiplicando ambos lados de la igualdad de la suma de Gauss por $\chi(a)$ se tiene que

$$\chi(a)g_a(\chi) = \chi(a)\sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \sum_{at=0}^{p-1} \chi(at)\zeta^{at} = g_1(\chi).$$

donde la última igualdad se cumple porque at recorre todos los elementos de $\mathbb{Z}/\mathbb{Z}p$ al igual que lo hace t. Esto prueba el primer caso.

Vamos a ver ahora con el segundo caso:

$$g_a(\varepsilon) = \sum_{t=0}^{p-1} \varepsilon(t)\zeta^{at} = \sum_{t=0}^{p-1} \zeta^{at} = 0.$$

Para ello hemos usado el **Lema 3.1**.

A continuación veamos el tercer caso:

$$g_0(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^{0t} = \sum_{t=0}^{p-1} \chi(t) = 0.$$

donde la última igualdad se cumple por la **Proposición 5.1.2**.

Finalmente, veamos el último caso:

$$g_0(\varepsilon) = \sum_{t=0}^{p-1} \epsilon(t)\zeta^{0t} = \sum_{t=0}^{p-1} \varepsilon(t) = p.$$

donde la última igualdad se cumple nuevamente por la **Proposición 5.1.2**. □

A partir de ahora, se va a denotar $g_1(\chi)$ como $g(\chi)$. Nuestro objetivo va a ser determinar el valor absoluto de $g(\chi)$. Esto se puede hacer fácilmente imitando la prueba de la **Proposición 3.3.2**.

Proposición 5.2.2 *Si $\chi \neq \varepsilon$, entonces*

$$|\, g(\chi)\,| = \sqrt{p}.$$

Demostración:

La idea consiste en evaluar la suma

$$\sum_{a \in \mathbb{Z}/\mathbb{Z}p} g_a(\chi)\overline{g_a(\chi)}$$

de dos formas.

Si $a \neq 0$, entonces por la **Proposición 5.2.1**, se tiene

$$\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$$

y

$$g_a(\chi) = \chi(a^{-1})g(\chi).$$

Entonces

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\zeta(a)g(\chi)\overline{g(\chi)} = g(\chi)\overline{g(\chi)} = |\, g(\chi)\,|^2 .$$

Dado que $g_0(\chi) = 0$ el sumatorio vale $(p-1)\,|\, g(\chi)\,|^2$. Por otro lado, se tiene que

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x \in \mathbb{Z}/\mathbb{Z}p} \sum_{y \in \mathbb{Z}/\mathbb{Z}p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Sumando en ambos lados sobre a y usando el **Corolario 3.2** nos lleva a que

$$\sum_{a \in \mathbb{Z}/\mathbb{Z}p} g_a(\chi)\overline{g_a(\chi)} = \sum_{x \in \mathbb{Z}/\mathbb{Z}p} \sum_{y \in \mathbb{Z}/\mathbb{Z}p} \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p.$$

donde

$$\delta(x,y) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{si } x \neq y \end{cases}$$

Por tanto,

$$(p-1)\,|\, g(\chi)\,|^2 = (p-1)p.$$

y el resultado se sigue. □

La relación entre el resultado anterior y la **Proposición 3.3.2** se hará más clara tras las siguientes consideraciones.

La relación entre $\overline{g(\chi)}$ y $g(\overline{\chi})$, donde $\overline{\chi}$ es el carácter que lleva el elemento a hasta $\overline{\chi(a)}$ (o lo que es lo mismo, el carácter χ^{-1}) es la siguiente:

$$\overline{g(\chi)} = \sum_{t=0}^{p-1} \overline{\chi(t)}\zeta^{-t} = \chi(-1) \sum_{-t=0}^{p-1} \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi}).$$

Se ha usado en la segunda igualdad el hecho de que $\overline{\chi(-1)} = \chi(-1)$, lo cual es obvio dado que $\chi(-1) = \pm 1$. Entonces, el hecho de que $|\, g(\chi)\,|^2 = p$ se puede escribir como $g(\chi)g(\overline{\chi}) = \chi(-1)p$. Si χ es el símbolo de Legendre, esta relación es precisamente el resultado en la **Proposición 3.3.2**.

5.3. Sumas de Jacobi

Consideremos la ecuación $x^2+y^2=1$ sobre el cuerpo $\mathbb{Z}/\mathbb{Z}p$. Dado que $\mathbb{Z}/\mathbb{Z}p$ es finito, la ecuación sólo tiene un número finito de soluciones. Sea $N(x^2+y^2-1)$ ese número. Vamos a determinar ese valor explícitamente.

Notemos que

$$N(x^2+y^2-1)=\sum_{a+b=1} N(x^2-a)N(y^2-b),$$

donde el sumatorio recorre todos los pares a, $b\in\mathbb{Z}/\mathbb{Z}p$ tales que $a+b=1$. Dado que $N(x^2-a)=1+\left(\frac{a}{p}\right)$, se obtiene por sustitución que

$$N(x^2+y^2-1)=p+\sum_{a\in\mathbb{Z}/\mathbb{Z}p}\left(\frac{a}{p}\right)+\sum_{b\in\mathbb{Z}/\mathbb{Z}p}\left(\frac{b}{p}\right)+\sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Los primeros sumatorios son cero, por lo que sólo nos queda evaluar el último sumatorio. Veremos en breve que su valor es $-(-1)^{\frac{p-1}{2}}$. Entonces

$$N(x^2+y^2-1)=\begin{cases} p-1 & \text{si } p\equiv 1 \pmod 4\\ p+1 & \text{si } p\equiv 3 \pmod 4\end{cases}$$

Yendo un paso más allá, evaluemos $N(x^3+y^3-1)$. Como antes tenemos que

$$N(x^3+y^3-1)=\sum_{a+b=1} N(x^3-a)N(y^3-b).$$

Si $p\equiv 2 \pmod 3$, entonces $N(x^3-a)=1$ para todo a dado que $\gcd(3,p-1)=1$. Esto implicaría que $N(x^3+y^3-1)=p$ en este caso.

Asumamos entonces que $p\equiv 1 \pmod 3$. Sea $\chi\neq\varepsilon$ un carácter de orden 3. Entonces χ^2 es un carácter de orden 3 y $\chi^2\neq\varepsilon$. Por lo tanto, ε, χ y χ^2 son todas los caracteres de orden 3 a las que llamaremos a partir de ahora *caracteres cúbicos*. Por la **Proposición 5.1.5** tenemos que $N(x^3-a)=1+\chi(a)+\chi^2(a)$. Entonces

$$N(x^3+y^3-1)=\sum_{a+b=1}\sum_{i=0}^{2}\chi^i(a)\sum_{j=0}^{2}\chi^j(b)=\sum_{i=0}^{2}\sum_{j=0}^{2}\left(\sum_{a+b=1}\chi^i(a)\chi^j(b)\right).$$

El sumatorio interior es similar al sumatorio que ocurría en el análisis de $N(x^2+y^2-1)$.

Definición 5.3 *Sean χ y λ caracteres de $\mathbb{Z}/\mathbb{Z}p$. Se denomina suma de Jacobi a $J(\chi,\lambda)$, el cual viene expresado como*

$$J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b)$$

Para completar el análisis de $N(x^2+y^2-1)$ y de $N(x^3+y^3-1)$ se necesita obtener información del valor de las sumas de Jacobi. El siguiente teorema no sólo nos proporcionará esta información sino que muestra también una gran conexión entre las sumas de Jacobi y las de Gauss.

Teorema 5.1 *Sean χ y λ caracteres no triviales. Entonces*

(a) $J(\varepsilon, \varepsilon) = p$.

(b) $J(\varepsilon, \chi) = 0$.

(c) $J(\chi, \chi^{-1}) = -\chi(-1)$.

(d) *Si $\chi\lambda \neq \varepsilon$, entonces*

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Demostración:

El apartado **(a)** es inmediato y el apartado **(b)** también lo es por la **Proposición 5.1.2**.

Para probar el apartado **(c)** se debe notar que

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right)$$

Escribamos $\frac{a}{1-a} = c$. Si $c \neq -1$, entonces $a = \frac{c}{1+c}$. Se sigue que, del mismo modo que a recorre todos los elementos de $\mathbb{Z}/\mathbb{Z}p$ menos el elemento 1, c recorre todos los elementos de $\mathbb{Z}/\mathbb{Z}p$ menos el elemento -1. Entonces

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

Para probar el apartado **(d)** se debe notar que

$$g(\chi)g(\lambda) = \left(\sum_{x\in\mathbb{Z}/\mathbb{Z}p} \chi(x)\zeta^x\right)\left(\sum_{y\in\mathbb{Z}/\mathbb{Z}p} \lambda(y)\zeta^y\right) = \sum_{x,y\in\mathbb{Z}/\mathbb{Z}p} \chi(x)\lambda(y)\zeta^{x+y} = \sum_{t\in\mathbb{Z}/\mathbb{Z}p}\left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^t. \tag{5.1}$$

Si $t = 0$, entonces

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x\in\mathbb{Z}/\mathbb{Z}p} \chi(x)\lambda(-x) = \lambda(-1)\sum_{x\in\mathbb{Z}/\mathbb{Z}p} \chi\lambda(x) = 0,$$

dado que $\chi\lambda \neq \varepsilon$ por hipótesis.

Si $t \neq 0$, definimos x' y y' como $x = tx'$ y $y = ty'$. Si $x + y = t$, entonces $x' + y' = 1$. Se sigue que

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi, \lambda).$$

Sustituyendo en la **ecuación** (5.1) se tiene que

$$g(\chi)g(\lambda) = \sum_{t\in\mathbb{Z}/\mathbb{Z}p} \chi\lambda(t)J(\chi, \lambda)\zeta^t = J(\chi, \lambda)g(\chi\lambda).$$

Esto concluye la prueba. □

Corolario 5.2 *Si χ, λ y $\chi\lambda$ son distintos de ε, entonces*

$$|J(\chi,\lambda)| = \sqrt{p}.$$

Demostración:

Tomando el valor absoluto a ambos lados de la ecuación del apartado **(d)** del **Teorema 5.1** y usando la **Proposición 5.2.2** se tiene la demostración. □

Volviendo de nuevo al análisis de $N(x^2+y^2-1)$ y $N(x^3+y^3-1)$, donde era necesario evaluar el sumatorio $\sum_{a+b=1}\binom{a}{p}\binom{b}{p}$. El apartado **(c)** del **Teorema 5.1** da el resultado

$$-\binom{-1}{p} = -(-1)^{\frac{p-1}{2}},$$

tal y como se usó anteriormente.

Para el caso de $N(x^3+y^3-1)$ es necesario evaluar el sumatorio $\sum_{a+b=1}\chi^i(a)\chi^j(b)$, donde χ es un carácter cúbico. Aplicando el **Teorema 5.1** se llega al siguiente resultado

$$N(x^3+y^3-1) = p - \chi(-1) - \chi^2(-1) + J(\chi,\chi) + J(\chi^2,\chi^2).$$

Dado que $-1 = (-1)^3$ se tiene que $\chi(-1) = \chi^3(-1) = 1$. Se debe notar también que $\chi^2 = \chi^{-1} = \overline{\chi}$. Entonces

$$N(x^3+y^3-1) = p - 2 + 2\ \mathrm{Re}\ J(\chi,\chi).$$

Este resultado no es tan elegante como el dado para $N(x^2+y^2-1)$ al no conocer $J(\chi,\chi)$ explícitamente. Sin embargo, por el **Corolario 5.2** sabemos que $|J(\chi,\chi)| = \sqrt{p}$ y se tiene entonces la estimación

$$|N(x^3+y^3-1) - p + 2| \le 2\sqrt{p}.$$

Si se escribe N_p para el número de soluciones de $x^3+y^3=1$ en el cuerpo $\mathbb{Z}/\mathbb{Z}p$, entonces la estimación nos dice que es aproximadamente a $p-2$ con un *término de error* igual a $2\sqrt{p}$. Esto muestra que, para primos grandes p hay siempre muchas soluciones.

Si $p \equiv 1 \pmod 3$, hay al menos 6 soluciones dado que $x^3 = 1$ y $y^3 = 1$ tienen 3 soluciones cada uno y obviamente se tiene que $1+0=1$ y $0+1=1$. Para $p = 7, 13$ sólo existen esas soluciones mientras que, para $p = 19$ existen otras soluciones, como $3^3 + 10^3 \equiv 1 \pmod{19}$. Estas soluciones "no triviales" existen para todo $p \ge 19$ dado que se sigue de la estimación que $N_p \ge p - 2 - 2\sqrt{p} > 6$ para $p \ge 19$.

Usando las sumas de Jacobi se puede extender nuestro análisis a ecuaciones de la forma $ax^n + by^n = 1$.

El **Corolario 5.2** tiene dos consecuencias inmediatas de interés.

Proposición 5.3.1 *Si $p \equiv 1 \pmod 4$, entonces existen enteros a y b tales que $a^2+b^2 = p$.*

Si $p \equiv 1 \pmod 3$, entonces existen enteros a y b tales que $a^2 - ab + b^2 = p$.

Demostración:

Si $p \equiv 1 \pmod 4$, hay un carácter χ de orden 4 (si λ tiene orden $p-1$, sea $\chi = \lambda^{\frac{p-1}{4}}$). Los valores de χ son los del conjunto $\{1, -1, i, -i\}$. Entonces

$$J(\chi,\chi) = \sum_{s+t=1}\chi(s)\chi(t) \in \mathbb{Z}[i].$$

Se sigue que $J(\chi,\chi) = a + bi$, donde $a, b \in \mathbb{Z}$. Por lo tanto,

$$p = |J(\chi,\chi)|^2 = a^2 + b^2.$$

Lo que demuestra la primera afirmación.

Si $p \equiv 1 \pmod 3$, hay un carácter χ de orden 3. Los valores de χ son los del conjunto $\{1, \omega, \omega^2\}$ donde $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$. Entonces $J(\chi, \chi) \in \mathbb{Z}[\omega]$. Como se ve arriba, se tiene que $J(\chi, \chi) = a + b\omega$, donde a, $b \in \mathbb{Z}$ y por tanto,

$$p = |J(\chi, \chi)|^2 = |a + b\omega|^2 = a^2 - ab + b^2.$$

Lo que lleva a la demostración de la proposición. □

El hecho de que los $p \equiv 1 \pmod 4$ pueden ser escritos como la suma de dos cuadrados fue descubierto por Fermat. No es fácil probar que si a, $b > 0$, con a impar y b par, entonces la representación $p = a^2 + b^2$ es único.

Si $p \equiv 1 \pmod 3$, la representación $p = a^2 - ab + b^2$ no es única incluso si se escribe que a, $b > 0$. Esto se puede ver de las ecuaciones

$$a^2 - ab + b^2 = (b-a)^2 - (b-a)b + b^2 = a^2 - a(a-b) + (a-b)^2.$$

Sin embargo, se pueden reformular las cosas para que el resultado sea único. Si $p = a^2 - ab + b^2$, entonces

$$4p = (2a-b)^2 + 3b^2 = (2b-a)^2 + 3a^2 = (a+b)^2 + 3(a-b)^2.$$

Se quiere demostrar que 3 divide a a, a b o a $a - b$. Supongamos que $3 \nmid a$ y que $3 \nmid b$. Si $a \equiv 1 \pmod 3$ y $b \equiv 2 \pmod 3$ o viceversa, entonces $a^2 - ab + b^2 \equiv 0 \pmod 3$, lo cual implica que $3 \mid p$, que sería una contradicción. Entonces, $3 \mid (a - b)$, que lleva al siguiente resultado:

Proposición 5.3.2 *Si $p \equiv 1 \pmod 3$, entonces hay unos enteros A y B tales que $4p = A^2 + 27B^2$. En esta representación para $4p$, A y B están unívocamente determinados salvo signo.*

Demostración:

Tomando congruencia módulo 3 se tiene que

$$1 \equiv A^2 \pmod 3$$

dado que $p \equiv 1 \pmod 3$. Por lo tanto se tiene que

$$A \equiv \pm 1 \pmod 3$$

Si suponemos que $A \equiv 1 \pmod 3$ se tiene que A está unívocamente determinado. En cualquier caso, A está unívocamente determinado salvo signo y por tanto, al estar tanto $4p$ como A fijados, B también está unívocamente determinado salvo signo. □

El **Teorema 5.1** junto con un argumento simple nos lleva a una interesante relación entre las sumas de Gauss y las de Jacobi.

Proposición 5.3.3 *Supongamos que $p \equiv 1 \pmod n$ y que χ es un carácter de orden $n > 2$. Entonces*

$$g(\chi)^n = \chi(-1)J(\chi, \chi)J(\chi, \chi^2)\cdots J(\chi, \chi^{n-2})p.$$

Demostración:

Usando el apartado **(d)** del **Teorema 5.1** se tiene que

$$g(\chi)^2 = J(\chi, \chi)g(\chi^2).$$

Multiplicando ambos lados por $g(\chi)$ se tiene que

$$g(\chi)^3 = J(\chi, \chi)J(\chi, \chi^2)g(\chi^3).$$

Continuando de esta manera se tiene

$$g(\chi)^{n-1} = J(\chi, \chi)J(\chi, \chi^2)\cdots J(\chi, \chi^{n-2})g(\chi^{n-1}). \tag{5.2}$$

Por otro lado, se sabe que, dado que χ tiene carácter n, $\chi^{n-1} = \chi^{-1} = \overline{\chi}$. Por tanto, como ya hemos visto antes,

$$g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

Por tanto el resultado se tiene multiplicando ambos lados de la ecuación (5.2) por $g(\chi)$. □

Corolario 5.3 *Si χ es un carácter cúbico, entonces*

$$g(\chi)^3 = pJ(\chi, \chi).$$

Demostración:

Esto es simplemente un caso especial de la **Proposición 5.3.3** y el hecho de que $\chi(-1) = \chi((-1)^3) = 1$. □

Usando este corolario, se puede ya analizar en mayor profundidad el número complejo $J(\chi, \chi)$ que aparecía en la discusión sobre $N(x^3 + y^3 - 1)$. Se ha visto que $J(\chi, \chi) = a + b\omega$, donde $a, b \in \mathbb{Z}$ y $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$.

Proposición 5.3.4 *Supongamos que $p \equiv 1$ (3) y que χ es un carácter cúbico. Denotemos $J(\chi, \chi) = a + b\omega$ como anteriormente. Entonces,*

(a) $b \equiv 0$ (3).

(b) $a \equiv -1$ (3).

Demostración:

Se va a trabajar con las congruencias del anillo de enteros algebraicos al igual que hicimos en el **Capítulo 3**:

$$g(\chi)^3 = \left(\sum_{t \in \mathbb{Z}/\mathbb{Z}p} \chi(t)\zeta^t \right)^3 \equiv \sum_{t \in \mathbb{Z}/\mathbb{Z}p} \chi(t)^3 \zeta^{3t} \quad (3).$$

Dado que $\chi(0) = 0$ y $\chi(t)^3 = 1$ para todo $t \neq 0$ se tiene que

$$\sum_{t \in \mathbb{Z}/\mathbb{Z}p} \chi(t)^3 \zeta^{3t} = \sum_{t \in (\mathbb{Z}/\mathbb{Z}p)^*} \zeta^{3t} = -1.$$

Por lo tanto,

$$g(\chi)^3 = pJ(\chi, \chi) \equiv a + b\omega \equiv -1 \quad (3).$$

Trabajando con $\overline{\chi}$ en vez de con χ y recordando que $\overline{g(\chi)} = g(\overline{\chi})$ se tiene que

$$g(\overline{\chi})^3 = pJ(\overline{\chi}, \overline{\chi}) \equiv a + b\overline{\omega} \equiv -1 \quad (3).$$

Restando nos lleva a que

$$b(\omega - \overline{\omega}) \equiv 0 \quad (3),$$

o equivalentemente

$$b\sqrt{-3} \equiv 0 \quad (3).$$

Entonces se tiene que

$$-3b^2 \equiv 0 \quad (9)$$

y por tanto que $3 \mid b$. Dado que $3 \mid b$ y que $a + b\omega \equiv -1$ (3), se tiene que $a \equiv -1$ (3), como se quería probar. □

Corolario 5.4 *Sea* $A = 2a - b$ *y* $B = \frac{b}{3}$. *Entonces* $A \equiv 1 \pmod 3$ *y*

$$4p = A^2 + 27B^2.$$

Demostración:

Dado que $J(\chi, \chi) = a + b\omega$ por la **Proposición 5.3.4** y que $|J(\chi, \chi)|^2 = p$ por el **Corolario 5.2** se tiene que $p = a^2 - ab + b^2$. Entonces, tal y como se vio anteriormente

$$4p = (2a - b)^2 + 3b^2 = A^2 + 27B^2.$$

Por la **Proposición 5.3.4** se tiene que $3 \mid b$ y $a \equiv -1 \pmod 3$. Por lo tanto,

$$A = 2a - b \equiv 1 \pmod 3.$$

tal y como se quería probar. □

Con todo esto ya se cuentan con las herramientas necesarias para probar un bonito teorema demostrado por Gauss.

Teorema 5.2 *Supongamos que* $p \equiv 1 \pmod 3$. *Entonces existen enteros* A *y* B *tales que* $4p = A^2 + 27B^2$. *Si suponemos además que* $A \equiv 1 \pmod 3$, *entonces* A *está unívocamente determinado y*

$$N(x^3 + y^3 - 1) = p - 2 + A.$$

Demostración:

Ya hemos visto anteriormente que

$$N(x^3 + y^3 - 1) = p - 2 + 2 \text{ Re } J(\chi, \chi).$$

Dado que $J(\chi, \chi) = a + b\omega$ como hemos en casos anteriores, se tiene que

$$\text{Re } J(\chi, \chi) = \frac{2a - b}{2}.$$

Entonces,

$$2 \text{ Re } J(\chi, \chi) = 2a - b = A \equiv 1 \pmod 3.$$

La unicidad de A se tiene por la **Proposición 5.3.2**. □

Ilustremos este teorema con dos ejemplos:

1. Sea $p = 61$. Se tiene que

$$4 \cdot 61 = 1^2 + 27 \cdot 3^2.$$

   Entonces, el número de soluciones de $x^3 + y^3 = 1$ en $\mathbb{Z}/\mathbb{Z}61$ es $61 - 2 + 1 = 60$.

2. Sea ahora $p = 67$. Se tiene que

$$4 \cdot 67 = 5^2 + 27 \cdot 3^2.$$

   Se debe tener cuidado aquí; dado que $5 \not\equiv 1 \pmod 3$ se debe elegir $A = -5$. Por tanto, el número de soluciones de $x^3 + y^3 = 1$ en $\mathbb{Z}/\mathbb{Z}67$ es $67 - 2 - 5 = 60$, coincidiendo con las de $p = 61$.

El **Teorema 5.1** puede generalizarse pero se necesita antes una definición.

Definición 5.4 *Sean χ_1, χ_2, …, χ_l caracteres en $\mathbb{Z}/\mathbb{Z}p$. La suma de Jacobi de estos caracteres se define como*

$$J(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1+\cdots+t_l=1} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l).$$

Se puede notar que cuando $l = 2$ se reduce a nuestra definición anterior de las sumas de Jacobi. Definiremos otra suma que será útil en el futuro, la cual se dejará sin nombrar:

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1+\cdots+t_l=0} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l).$$

Proposición 5.3.5 *Sean χ_1, χ_2, …, χ_l caracteres sobre $\mathbb{Z}/\mathbb{Z}p$. Se cumplen las siguientes propiedades:*

(a) $J_0(\varepsilon, \varepsilon, \ldots, \varepsilon) = J(\varepsilon, \varepsilon, \ldots, \varepsilon) = p^{l-1}$.

(b) *Si alguno, pero no todos los χ_i, son triviales entonces*

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = J(\chi_1, \chi_2, \ldots, \chi_l) = 0.$$

(c) *Si $\chi_l \neq \varepsilon$ entonces*

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \begin{cases} 0, & \text{si } \chi_1\chi_2\cdots\chi_l \neq \varepsilon \\ \chi_l(-1)(p-1)J(\chi_1, \chi_2, \ldots, \chi_{l-1}) & \text{en caso contrario} \end{cases}$$

Demostración:

Se debe notar que para t_1, t_2, …, t_{l-1} cualesquiera fijos en $\mathbb{Z}/\mathbb{Z}p$, se tiene que t_l está unívocamente determinado por la condición $t_1 + t_2 + \cdots + t_{l-1} + t_l = 0$. Por lo tanto,

$$J_0(\varepsilon, \varepsilon, \ldots, \varepsilon) = J(\varepsilon, \varepsilon, \ldots, \varepsilon) = p^{l-1}.$$

Para probar el apartado **(b)**, se asume que χ_1, χ_2, …, χ_s son no triviales y que $\chi_{s+1} = \chi_{s+2} = \cdots = \chi_l = \varepsilon$. Entonces

$$\sum_{t_1+\cdots+t_l=0,1} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l) = \sum_{t_1,t_2,\ldots,t_s} \chi_1(t_1)\chi_2(t_2)\cdots\chi_s(t_s) =$$

$$= p^{l-s-1}\left(\sum_{t_1\in\mathbb{Z}/\mathbb{Z}p} \chi_1(t_1)\right)\left(\sum_{t_2\in\mathbb{Z}/\mathbb{Z}p} \chi_2(t_2)\right)\cdots\left(\sum_{t_l\in\mathbb{Z}/\mathbb{Z}p} \chi_l(t_l)\right) = 0.$$

Para ello se ha usado la **Proposición 5.1.2**. Entonces

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = J(\chi_1, \chi_2, \ldots, \chi_l) = 0.$$

Para probar el apartado **(c)**, se debe notar que

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{s\in\mathbb{Z}/\mathbb{Z}p} \left(\sum_{t_1+\cdots+t_{l-1}=-s} \chi_1(t_1)\cdots\chi_{l-1}(t_{l-1})\right)\chi_l(s)$$

Dado que $\chi_l \neq \varepsilon$, $\chi_l(0) = 0$ por lo que vamos a asumir que $s \neq 0$ en el sumatorio anterior. Si $s \neq 0$, se definen t'_i como $t_i = -st'_i$. Entonces

$$\sum_{t_1+\cdots+t_{l-1}=-s} \chi_1(t_1)\cdots\chi_{l-1}(t_{l-1}) = \chi_1\chi_2\cdots\chi_{l-1}(-s) \sum_{t'_1+\cdots+t'_{l-1}=1} \chi_1(t'_1)\cdots\chi_{l-1}(t'_{l-1}) =$$

$$= \chi_1\chi_2\cdots\chi_{l-1}(-s)J(\chi_1, \ldots, \chi_{l-1}).$$

Combinando estos resultados se llega a que

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \chi_1\chi_2\cdots\chi_{l-1}(-1)J(\chi_1, \ldots, \chi_{l-1}) \sum_{s\in(\mathbb{Z}/\mathbb{Z}p)^*} \chi_1\chi_2\cdots\chi_l(s).$$

El resultado se tiene dado que el sumatorio es 0 si $\chi_1\chi_2\cdots\chi_l \neq \varepsilon$ y $p-1$ si $\chi_1\chi_2\cdots\chi_l = \varepsilon$. □

Teorema 5.3 *Asumiendo que tanto* χ_1, χ_2, …, χ_l *como* $\chi_1\chi_2\cdots\chi_l$ *no son triviales,*

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = J(\chi_1, \chi_2, \ldots, \chi_r)g(\chi_1\chi_2\cdots\chi_r).$$

Demostración:

Sea $\psi : \mathbb{Z}/\mathbb{Z}p \to \mathbb{C}$ definida como $\psi(t) = \zeta^t$. Entonces $\psi(t_1 + t_2) = \psi(t_1)\psi(t_2)$ y $g(\chi) = \sum_{t\in\mathbb{Z}/\mathbb{Z}p} \chi(t)\psi(t)$. El introducir de ψ se realiza por conveniencia en la notación.

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = \left(\sum_{t_1\in\mathbb{Z}/\mathbb{Z}p} \chi_1(t_1)\psi(t_1)\right)\left(\sum_{t_2\in\mathbb{Z}/\mathbb{Z}p} \chi_2(t_2)\psi(t_2)\right)\cdots\left(\sum_{t_l\in\mathbb{Z}/\mathbb{Z}p} \chi_l(t_l)\psi(t_l)\right) =$$

$$= \sum_{s\in\mathbb{Z}/\mathbb{Z}p}\left(\sum_{t_1+t_2+\cdots+t_r=s} \chi_1(t_1)\chi_2(t_2)\cdots\chi_r(t_r)\right)\psi(s).$$

Si $s = 0$, entonces por el apartado **(c)** de la **Proposición 5.3.5** y la hipótesis de que $\chi_1\cdots\chi_r \neq \varepsilon$ se tiene que

$$\sum_{t_1+t_2+\cdots+t_r=0} \chi_1(t_1)\chi_2(t_2)\cdots\chi_r(t_r) = 0.$$

Si $s \neq 0$, la sustitución $t_i = st_i'$ para todo i muestra del mismo modo que vimos en la prueba del apartado **(c)** de la **Proposición 5.3.5** que

$$\sum_{t_1+\cdots+t_r=s} \chi(t_1)\cdots\chi_r(t_r) = \chi_1\chi_2\cdots\chi_r(s)J(\chi_1, \chi_2, \ldots, \chi_r).$$

Poniendo estas observaciones juntas se tiene que

$$g(\chi_1)\cdots g(\chi_r) = J(\chi_1, \chi_2, \ldots, \chi_r) \sum_{s\in(\mathbb{Z}/\mathbb{Z}p)^*} \chi_1\chi_2\cdots\chi_r(s)\psi(s) = J(\chi_1, \chi_2, \ldots, \chi_r)g(\chi_1\chi_2\cdots\chi_r).$$

Esto concluye la prueba. □

Corolario 5.5 *Supongamos que* χ_1, χ_2, …, χ_r *no son triviales pero que* $\chi_1\chi_2\cdots\chi_r$ *lo es. Entonces*

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = \chi_r(-1)pJ(\chi_1, \chi_2, \ldots, \chi_{r-1}).$$

Demostración:

Dado que $\chi_1\chi_2\cdots\chi_{r-1} = (\chi_r)^{-1} \neq \varepsilon$ por hipótesis, se tiene que, por el **Teorema 5.3**,

$$g(\chi_1)\cdots g(\chi_{r-1}) = J(\chi_1, \chi_2, \ldots, \chi_{r-1})g(\chi_1\chi_2\cdots\chi_{r-1}).$$

Multiplicando ambos lados de la igualdad por $g(\chi_r)$ se tiene que

$$g(\chi_1\chi_2\cdots\chi_{r-1})g(\chi_r) = g(\chi_r^{-1})g(\chi_r) = \chi_r(-1)p.$$

Aplicandolo a la ecuación anterior se tiene la prueba. □

Corolario 5.6 *Supongamos que χ_1, χ_2, ..., χ_r no son triviales pero que $\chi_1\chi_2\cdots\chi_r$ lo es. Entonces*

$$J(\chi_1, \chi_2, \ldots, \chi_r) = -\chi_r(-1)J(\chi_1, \chi_2, \ldots, \chi_{r-1}).$$

Demostración:

Para $r = 2$, definiendo que $J(\chi_1) = 1$ se tiene por el apartado **(c)** del **Teorema 5.1**.

Supongamos que $r > 2$. Usando la hipótesis de que $\chi_1\chi_2\cdots\chi_r = \varepsilon$ en la prueba del **Teorema 5.3** se llega a que

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = J_0(\chi_1, \chi_2, \ldots, \chi_r) + J(\chi_1, \chi_2, \ldots, \chi_r) \sum_{s\in(\mathbb{Z}/\mathbb{Z}p)^*} \psi(s).$$

Dado que $\sum_{s\in\mathbb{Z}/\mathbb{Z}p} \psi(s) = 0$, el sumatorio en la fórmula es igual a -1. Por el apartado **(c)** de la **Proposición 5.3.5** se tiene que

$$J_0(\chi_1, \chi_2, \ldots, \chi_r) = \chi_r(-1)(p-1)J(\chi_1, \cdots, \chi_{r-1}).$$

Por el **Corolario 5.5**, se tiene que

$$g(\chi_1)\cdots g(\chi_r) = \chi_r(-1)pJ(\chi_1, \cdots, \chi_{r-1}).$$

Poniendo estos resultados juntos se prueba el corolario. □

Teorema 5.4 *Asumiendo que χ_1, χ_2, ..., χ_r no son triviales, se tiene que:*

(a) *Si $\chi_1\chi_2\cdots\chi_r \neq \varepsilon$, entonces*

$$|\, J(\chi_1, \chi_2, \ldots, \chi_r)\,| = p^{\frac{r-1}{2}}.$$

(b) *Si $\chi_1\chi_2\cdots\chi_r = \varepsilon$, entonces*

$$|\, J_0(\chi_1, \chi_2, \ldots, \chi_r)\,| = (p-1)p^{\frac{r}{2}-1}.$$

y

$$|\, J(\chi_1, \chi_2, \ldots, \chi_r)\,| = p^{\frac{r}{2}-1}.$$

Demostración:

Por la **Proposición 5.2.2**, si $\chi \neq \varepsilon$, se tiene que $|\, g(\chi)\,| = \sqrt{p}$. El apartado **(a)** se tiene directamente por el **Teorema 5.3**.

El apartado **(b)** se tiene de forma similar por el apartado **(c)** de la **Proposición 5.3.5** y por el **Corolario 5.6**. □

5.4. La ecuación $x^n + y^n = 1$ en $\mathbb{Z}/\mathbb{Z}p$

Asumiendo que $p \equiv 1 \ (n)$, se va a investigar el número de soluciones de la ecuación $x^n + y^n = 1$ sobre el cuerpo $\mathbb{Z}/\mathbb{Z}p$. Los métodos vistos en la **Sección 5.3** se pueden aplicar directamente. Se tiene que

$$N(x^n + y^n - 1) = \sum_{a+b=1} N(x^n - a)N(y^n - b).$$

Sea χ un carácter de orden n. Por la **Proposición 5.1.5** se tiene que

$$N(x^n - a) = \sum_{i=0}^{n-1} \chi^i(a).$$

Combinando estos resultados nos lleva a

$$N(x^n + y^n - 1) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} J(\chi^i, \chi^j).$$

Usamos ahora el **Teorema 5.1** para estimar este sumatorio.
Cuando $i = j = 0$ se tiene que

$$J(\chi^0, \chi^0) = J(\varepsilon, \varepsilon) = p.$$

Cuando $j + i = n$, se tiene que $\chi^i = (\zeta^j)^{-1}$ por lo tanto

$$J(\chi^i, \chi^{-i}) = -\chi^i(-1).$$

El sumatorio de estos términos es

$$-\sum_{j=1}^{n-1} \chi^j(-1).$$

Se puede notar que

$$\sum_{j=0}^{n-1} \chi^j(-1) = \begin{cases} n, & \text{si } -1 \text{ es una potencia } n\text{-ésima} \\ 0, & \text{en cualquier otro caso} \end{cases}$$

Entonces la contribución de esos términos es $1-\delta_n(-1)n$, donde $\delta_n(-1)$ es la *delta de Kronecker* que vale 1 si -1 es potencia n-ésima y 0 en caso contrario. Finalmente, si $i = 0$ y $j \neq 0$ o $i = 0$ y $j \neq 0$, entonces $J(\chi^i, \chi^j) = 0$. Por tanto,

$$N(x^n + y^n - 1) = p + 1 - \delta_n(-1)n + \sum_{\substack{i,j=1 \\ i+j\neq n}}^{n-1} J(\chi^i, \chi^j).$$

Hay $(n-1)^2 - (n-1) = (n-1)(n-2)$ de esos términos y todos tienen valor absoluto igual a $\sqrt{p}$. Todo esto nos lleva a la siguiente proposición.

Proposición 5.4.1

$$|\, N(x^n + y^n - 1) + \delta_n(-1)n - (p+1)\,| \leq (n-1)(n-2)\sqrt{p}.$$

Para valores altos de p la estimación anterior muestra la existencia de muchas soluciones no triviales.

5.5. Un resultado para las ecuaciones más generales

Todas las ecuaciones que se han considerado hasta ahora han sido casos especiales de

$$a_1\chi_1^{l_1} + a_2\chi_2^{l_2} + \cdots + a_r\chi_r^{l_r} = b, \tag{5.3}$$

donde $a_1, \ldots, a_r \in (\mathbb{Z}/\mathbb{Z}p)^*$, $b \in \mathbb{Z}/\mathbb{Z}p$. Sea N el número de soluciones. El objetivo es dar una fórmula y una estimación para N. Los métodos usados son idénticos con los métodos desarrollados en secciones previas.

Para empezar tenemos que,

$$N = \sum_{\sum_{i=1}^r a_i u_i = b} N(x_1^{l_1} - u_1)N(x_2^{l_2} - u_2)\cdots N(x_r^{l_r} - u_r). \tag{5.4}$$

Se va a asumir que l_1, l_2, ..., l_r con divisores de $p-1$, aunque no es necesario. Variemos χ_l de forma que recorra todos los caracteres de orden l_i. Entonces,

$$N(x_i^{l_i} - u_i) = \sum_{\chi_i} \chi_i(u_i).$$

Sustituyendo en la **ecuación** (5.4) se tiene que

$$N = \sum_{\chi_1,\chi_2,\cdots,\chi_r} \left(\sum_{\sum_{i=1}^r a_i u_i = b} \chi_1(u_1)\chi_2(u_2)\cdots\chi_r(u_r) \right). \tag{5.5}$$

Se puede ver que la suma interior está estrechamente relacionada con las sumas de Jacobi que se han considerado anteriormente.

Es necesario tratar los casos $b = 0$ y $b \neq 0$ por separado.

Si $b = 0$, sea $t_i = a_i u_i$. Entonces la suma interior se puede expresar de la siguiente forma

$$\chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_r(a_r^{-1})J_0(\chi_1,\chi_2,\ldots,\chi_r).$$

Si $b \neq 0$, sea $t_i = b^{-1}a_i u_i$. Entonces la suma interior se puede expresar de la siguiente forma

$$\chi_1\chi_2\cdots\chi_r(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_r(a_r^{-1})J(\chi_1,\chi_2,\ldots,\chi_r).$$

En ambos casos, si $\chi_1 = \chi_2 = \cdots = \chi_r = \varepsilon$ el término vale p^{r-1} dado que

$$J_0(\varepsilon,\varepsilon,\ldots,\varepsilon) = J(\varepsilon,\varepsilon,\ldots,\varepsilon) = p^{r-1}.$$

Si algunos pero no todos los χ_i son iguales a ε, entonces el término vale 0. En el primer caso, el valor es cero a menos que $\chi_1\chi_2\cdots\chi_r = \varepsilon$. Todo esto es a una consecuencia de la **Proposición 5.3.5**.

Poniéndolo todo junto con el **Teorema 5.4** se obtiene que

Teorema 5.5 *En las condiciones anteriores:*

(a) *Si $b = 0$ entonces*

$$N = p^{r-1} + \sum_{(\chi_1^{l_1},\chi_2^{l_2},\ldots,\chi_r^{l_r})=(\varepsilon,\varepsilon,\ldots,\varepsilon)} \chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_r(a_r^{-1})J_0(\chi_1,\chi_2,\ldots,\chi_r).$$

donde $\chi_i \neq \varepsilon$ $\forall i$ y $\chi_1\chi_2\cdots\chi_r = \varepsilon$. Si M es el número de esas r-tuplas, entonces

$$|N - p^{r-1}| \leq M(p-1)p^{\frac{r}{2}-1}.$$

(b) *Si $b \neq 0$ entonces*

$$N = p^{r-1} + \sum_{(\chi_1^{l_1},\chi_2^{l_2},\ldots,\chi_r^{l_r})=(\varepsilon,\varepsilon,\ldots,\varepsilon)} \chi_1\chi_2\cdots\chi_r(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots\chi_r(a_r^{-1})J(\chi_1,\chi_2,\ldots,\chi_r).$$

donde $\chi_i \neq \varepsilon$ $\forall i$. Si M_0 es el número de esas r-tuplas con $\chi_1\chi_2\cdots\chi_r = \varepsilon$ y M_1 es el número de esas r-tuplas con $\chi_1\chi_2\cdots\chi_r \neq \varepsilon$, entonces

$$|N - p^{r-1}| \leq M_0 p^{\frac{r}{2}-1} + M_1 p^{\frac{r-1}{2}}.$$

Se puede destacar una consecuencia inmediata del **Teorema 5.5**. Sean a_1, a_2, ..., a_r y $b \in \mathbb{Z}$ y se considera la congruencia

$$a_1 x_1^{l_1} + a_2 x_2^{l_2} + \cdots a_r x_r^{l_r} \equiv b \ \ (p).$$

Entonces, para primos p suficientemente grandes, la congruencia tiene muchas soluciones. De hecho, el número de soluciones tiende a infinito a medida que aumenta p.

5.6. Aplicaciones: Ley de Reciprocidad Cuadrática

Anteriormente en este capítulo se ha investigado el número de soluciones de la ecuación $x^n + y^n = 1$ en el cuerpo $\mathbb{Z}/\mathbb{Z}p$. Es natural preguntarse la misma pregunta sobre la ecuación $x_1^2 + \cdots + x_r^2 = 1$. La respuesta puede ser encontrada fácilmente usando los resultados de la **Sección 5.3**.

Sea χ un carácter de orden 2 ($\chi(a) = \left(\frac{a}{p}\right)$ en nuestra notación anterior). Entonces

$$N(x^2 = a) = 1 + \chi(a).$$

Por tanto,

$$N(x_1^2 + \cdots + x_r^2 - 1) = \sum_{a_1 + \cdots + a_r = 1} N(x_1^2 - a_1) N(x_2^2 - a_2) \cdots N(x_r^2 - a_r).$$

Multiplicando y usando la **Proposición 5.3.5** nos lleva a que

$$N(x_1^2 + \cdots + x_r^2 - 1) = p^{r-1} + J(\chi, \chi, \ldots, \chi).$$

Dado que χ es un carácter de orden 2, se tiene que si r es impar, $\chi^r = \chi$ y si r es par, $\chi^r = \varepsilon$.

En primer caso se va a suponer que r es impar. Entonces, aplicando el **Teorema 5.3** se tiene que

$$J(\chi, \chi, \ldots, \chi) = g(\chi)^{r-1}.$$

Dado que χ es de orden 2, entonces $\chi = \overline{\chi}$ y por tanto, tal y como se ha visto anteriormente, se tiene que

$$g(\chi)^2 = \chi(-1)p.$$

De esto se sigue que

$$J(\chi, \chi, \ldots, \chi) = \chi(-1)^{\frac{r-1}{2}} p^{\frac{r-1}{2}}.$$

Ahora se va suponer que r es par. Usando el **Corolario 5.6**, se puede encontrar que

$$J(\chi, \chi, \ldots, \chi) = -\chi(-1)^{\frac{r}{2}} p^{\frac{r-2}{2}}.$$

Finalmente, se debe recordar que

$$\chi(-1) = (-1)^{\frac{p-1}{2}}.$$

Entonces se tiene la siguiente proposición:

Proposición 5.6.1 *En las condiciones anteriores:*

(a) *Si r es impar, entonces*

$$N(x_1^2 + x_2^2 + \cdots + x_r^2 - 1) = p^{r-1} + (-1)^{\frac{r-1}{2} \cdot \frac{p-1}{2}} p^{\frac{r-1}{2}}.$$

(b) *Si r es par, entonces*

$$N(x_1^2 + x_2^2 + \cdots + x_r^2 - 1) = p^{r-1} + (-1)^{\frac{r}{2} \cdot \frac{p-1}{2}} p^{\frac{r}{2}-1}.$$

Con todo lo visto hasta ahora podemos llevar nuestros métodos al caso más general posible, que es de la forma

$$a_1 \chi_1^{l_1} + a_2 \chi_2^{l_2} + \cdots + a_r \chi_r^{l_r} = b,$$

donde $a_1, \ldots, a_r, b \in \mathbb{Z}/\mathbb{Z}p$ y $l_1, l_2, \ldots, l_r \in \mathbb{Z}_{>0}$ como ya vimos en la **Sección 5.5**.

Ahora usaremos las sumas de Jacobi para dar otra demostración de la *Ley de Reciprocidad Cuadrática*. Sea q un primo impar distinto de p y χ un carácter de orden 2 en $\mathbb{Z}/\mathbb{Z}p$.

Entonces, por el **Corolario 5.5**, se tiene que

$$g(\chi)^{q+1} = (-1)^{\frac{p-1}{2}} pJ(\chi, \chi, \ldots, \chi),$$

donde hay q componentes en la suma de Jacobi.

Dado que $q+1$ es par, se tiene que

$$g(\chi)^{q+1} = (g(\chi)^2)^{\frac{q+1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q+1}{2}} p^{\frac{q+1}{2}}.$$

Sustituyendo en la fórmula se puede encontrar que

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} = J(\chi, \chi, \ldots, \chi).$$

Por otro lado, se sabe que

$$J(\chi, \chi, \ldots, \chi) = \sum_{t_1+t_2+\cdots+t_q=1} \chi(t_1)\chi(t_2)\cdots\chi(t_q).$$

Si $t = t_1 = t_2 = \cdots = t_q$, entonces $t = \frac{1}{q}$, y el término correspondiente del sumatorio vale

$$\chi\left(\frac{1}{q}\right)^q = \chi(q)^{-q} = \chi(q).$$

Si no todos los t_i son iguales, entonces hay q q-tuplas diferentes que se obtienen de $(t_1, t_2, \ldots, t_q)$ por permutaciones cíclicas.

Por lo tanto, los términos correspondientes del sumatorio todos tienen el mismo valor. Entonces

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv \chi(q) \pmod{q}.$$

Dado que $\chi(q) = \left(\frac{q}{p}\right)$ y $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q}$, se tiene que

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}$$

y por tanto,

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Lo que nos prueba la *Ley de Reciprocidad Cuadrática*. ■

Bibliografía

[1] M.W. Baldoni, C. Ciliberto & G.M. Piacentini Cattaneo: *Elementary number theory, cryptography and codes*. Springer (2009).

[2] H. Cohen: *A course in computational number theory*. Springer (1993).

[3] G. H. Hardy & E.M. Wright: *An Introduction to the Theory of Numbers*. Oxford Science Publications (1938).

[4] K. Ireland & M. Rosen: *A Classical Introduction to Modern Number Theory*. Springer (1982).

[5] N. Koblitz: *A course in number theory and cryptography*. Springer (1987).

[6] J. Serre: *A course in Arithmetic*. Springer (1973).

[7] N. Smart: *Cryptography: an introduction*. MGraw-Hill (2003).