Capítulo 1

Introducción a la Teoría Algebraica de Números.

1.1. Dominios Euclídeos. Anillos de Enteros.

Definición 1.1.1. Sea A un dominio de integridad, diremos que A es un dominio euclídeo si existe $\phi : A \to \mathbb{N}$ tal que verifique las siguientes propiedades:

1. $a \neq 0 \Rightarrow \phi(a) > 0$, ó, equivalentemente $a = 0 \iff \phi(a) = 0$
2. $b \neq 0 \Rightarrow a = qb + r$, donde $q, r \in A$ y, o bien $r = 0$ ó $\phi(r) < \phi(b)$

Diremos que un dominio de integridad $A \subset \mathbb{C}$ es un dominio norm-euclídeo o norma-euclídeo si la función ϕ es justo la norma euclídea usual en los complejos (al cuadrado).

Definición 1.1.2. Consideremos el conjunto $\mathcal{A} = \{z \in \mathbb{C} \,|\, \exists\, p \in \mathbb{Z}[x] \text{ mónico} \,|\, p(z) = 0\}$. Este conjunto se denomina el conjunto de los enteros algebraicos.

Teorema 1.1.3. *$\mathcal{A}$ con la suma y producto usuales de los números complejos es un anillo conmutativo.*

Demostración. Obviamente 0 y $1 \in \mathcal{A}$, ya que son raíces de los polinomios t y $t - 1$ respectivamente.

Veamos que si $z \in \mathcal{A}$ entonces $-z \in \mathcal{A}$. En efecto, sea $z \in \mathcal{A}$ entonces, existe un $p \in \mathbb{Z}[t]$ mónico con $p(z) = 0$. Entonces, es fácil comprobar que $-z$ es raíz del polinomio $p(-t)$, así, $-z \in \mathcal{A}$.

Veamos que la suma está. Tomemos $z_1, \omega_1 \in \mathcal{A} \Rightarrow \exists\, p, q \in \mathbb{Z}[t]$ mónicos tales que

$$p = (t - z_1) \dots (t - z_n)$$
$$q = (t - \omega_1) \dots (t - \omega_m)$$

Hacemos $r = \Pi_{i,j}(t - z_i - \omega_j) \in \mathbb{C}[t]$ mónico. Los coeficientes son polinomios simétricos en los z_i y ω_j, luego son polinomios con coeficientes enteros en los coeficientes de p y q, así pues, son necesariamente enteros. Claramente, $r(z_1 + \omega_1) = 0$ por construcción y $z_1 + \omega_1 \in \mathcal{A}$.

La idea de la multiplicación es esencialmente la misma, sólo que $r = \prod_{i,j}(t - z_i\omega_j)$.

De esta manera, se ve que este es un anillo. La conmutatividad viene heredada por la conmutatividad de $\mathbb{C}$. □

Antes de dar la siguiente definición, vamos a introducir unos pocos conceptos básicos de la Teoría de Galois. Se define una extensión de cuerpos sobre $\mathcal{K}$, y se denota $\mathcal{L} : \mathcal{K}$, a la terna $(\mathcal{K}, \mathcal{L}, \varphi)$ dónde $\mathcal{K}, \mathcal{L}$ son dos cuerpos y $\varphi : \mathcal{K} \to \mathcal{L}$ tal que $\varphi(\mathcal{K}) \subset \mathcal{L}$. Además, al cuerpo $\mathcal{L}$ se le puede dar una estructura de $\mathcal{K}-$espacio vectorial.

Los casos que nos interesan para este curso son las extensiones de $\mathbb{Q}$. Algunos ejemplos son $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{d}\right)$ con d libre de cuadrados, $\mathbb{Q}(\xi_p)$ dónde ${\xi_p}^p = 1$ y p es primo...

Definición 1.1.4. Se dice que $\mathcal{K}$ es un cuerpo de números si $\mathcal{K}$ es un cuerpo y:

1. $\mathbb{Q} \subset \mathcal{K} \subset \mathbb{C}$
2. $dim_{\mathbb{Q}}\ \mathcal{K}$ es finita.

Dado un cuerpo de números $\mathcal{K}$, llamaremos $O_{\mathcal{K}} = \mathcal{K} \cap \mathcal{A}$ al anillo de enteros o de números (se usan indiscriminadamente) de $\mathcal{K}$, es decir, a los enteros algebraicos contenidos en $\mathcal{K}$.

Ejercicio. Consideremos los anillos $\mathbb{Z}\left[\sqrt{-d}\right]$, que, es fácil comprobar que son anillos, si d es libre de cuadrados. Nos preguntamos, ¿para que $d \geq 1$ son estos anillos dominios euclídeos?

La función norma en estos anillos debería ser la norma euclídea usual al cuadrado en los números complejos, es decir, $N\left(a + b\sqrt{-d}\right) = a^2 + b^2 d$ (a este tipo de dominios euclídeos que funcionan con la norma compleja les llamaremos norma-Euclídeos o norm-Euclídeos). Esta aplicación verifica la primera condición de la definición de dominio euclídeo. Veamos cuándo cumple la segunda.

Vamos a aplicar el algoritmo de Euclides. Sean $a + b\sqrt{-d}$ y $\alpha + \beta\sqrt{-d}$ con $|a + b\sqrt{-d}|^2 > |\alpha + \beta\sqrt{-d}|^2$. Haciendo la división compleja habitual,

$$\frac{a + b\sqrt{-d}}{\alpha + \beta\sqrt{-d}} = q_1 + q_2\sqrt{-d}$$

para ciertos $q_1, q_2 \in \mathbb{Q}$. Vamos a truncar q_1 y q_2 a los enteros más próximos $\bar{q_1}$ y $\bar{q_2}$ de forma que $|\varepsilon_i| = |q_i - \bar{q_i}| < \frac{1}{2}$ para $i = \{1, 2\}$.

Así, $a + b\sqrt{-d} = \left(\alpha + \beta\sqrt{-d}\right)\left(\bar{q_1} + \bar{q_2}\sqrt{-d}\right) + r$ dónde r denota el resto de la división euclídea. Para que $\mathbb{Z}\left[\sqrt{-d}\right]$ sea un dominio euclídeo, $N(r) < N\left(\alpha + \beta\sqrt{-d}\right)$, o lo que es equivalente,

$$\begin{aligned} |r|^2 &= \left|a + b\sqrt{-d} - \left(\alpha + \beta\sqrt{-d}\right)\left(\bar{q_1} + \bar{q_2}\sqrt{-d}\right)\right|^2 \\ &= \left|a + b\sqrt{-d} - \left(\alpha + \beta\sqrt{-d}\right)\left(q_1 + \varepsilon_1 + (q_2 + \varepsilon_2)\sqrt{-d}\right)\right|^2 \\ &= \left|\left(\alpha + \beta\sqrt{-d}\right)\left(\varepsilon_1 + \varepsilon_2\sqrt{-d}\right)|^2 < |\alpha + \beta\sqrt{-d}\right|^2 \end{aligned}$$

O sea, habrá que ver para qué valores de d es $\left|\varepsilon_1 + \varepsilon_2\sqrt{-d}\right|^2 = {\varepsilon_1}^2 + d{\varepsilon_2}^2 < 1$. Haciendo unos cálculos, se puede ver fácilmente que esto ocurre para $d = 1, 2$, ya que $|\varepsilon_i| < 1/2$, luego ${\varepsilon_i}^2 < \frac{1}{4}$.

Así, hemos probado que $\mathbb{Z}[i]$ y $\mathbb{Z}\left[\sqrt{-2}\right]$ son dominios euclídeos. Sin embargo, hay algunos anillos de números más que también son dominios euclídeos.

Teorema 1.1.5. *El anillo $O_{\mathcal{K}}$ dónde $\mathcal{K} = \mathbb{Q}\left(\sqrt{d}\right)$ es $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si, y sólo si, $d \equiv 1\ (\mod 4)$ y $\mathbb{Z}\left[\sqrt{d}\right]$ si, y sólo si, $d \equiv 3\ (\mod 4)$ ó $d = 2$. Además, si $d < 0$ libre de cuadrados, entonces $O_{\mathcal{K}}$ es un anillo norma-Euclídeo si, y sólo si, es un anillo euclídeo. Además, los valores de d para los que es euclídeo son $d = -1, -2, -3, -7, -11$.*

Demostración. La demostración, aunque no es esencialmente complicada, excede las competencias de esta sección. Se puede buscar dicha prueba en [1]. □

Ejercicio. Las unidades de $\mathbb{Z}[i]$ y $\mathbb{Z}\left[\sqrt{-2}\right]$ Vamos a calcular las unidades de estos anillos. Primero, vamos a valernos de una proposición importante:

Proposición 1.1.6. *Un elemento u en un dominio norma-euclídeo $A \subset \mathbb{C}$ es una unidad $\iff N(u) = 1$.*

Demostración. En esta demostración se utiliza fuertemente que la norma euclídea es multiplicativa, es decir, $|ab| = |a||b|$ para $a, b \in A$. Es algo que no ocurre con todas las normas que se puedan definir sobre un dominio euclídeo. Por ejemplo, si defino la norma $\phi = 2|\ |^2$, verifica todas las hipótesis de norma en un anillo, pero NO es multiplicativa. Así, nos restringimos a los dominios norma-euclídeos. Así, consideremos la norma euclídea N para esta demostración.

$\Rightarrow$ Supongamos que u es una unidad. Entonces, existe un elemento $v \in A$ tal que $uv = 1_A$. Tomando normas, $N(uv) = N(u)N(v) = N(1_A) = 1$. Como $N(a) \in \mathbb{N}$ para todo $a \in A$, debe ser que $N(u) = 1$.

$\Leftarrow$ Recíprocamente, supongamos que existe un elemento $u \in A$ con $N(u) = 1$. Como $u \neq 0_A$, existen $q, r \in A$ tales que $1_A = qu + r$ con $N(r) < N(u) = 1$, así, sólo queda que $N(r) = 0$ y $1_A = qu$, o sea, u es una unidad. □

Calculemos ahora las unidades de $\mathbb{Z}[i]$ y $\mathbb{Z}\left[\sqrt{-2}\right]$:

1. Para calcular las unidades en $\mathbb{Z}[i]$, sabemos que la norma euclídea utilizada es la norma compleja usual (al cuadrado). O sea, para que un elemento $a + bi$ sea una unidad, se necesita que $a^2 + b^2 = 1 \iff a = \pm 1$ y $b = 0$ ó $a = 0$ y $b = \pm 1$. Así, las únicas unidades en $\mathbb{Z}[i]$ serán $u = \pm 1, \pm i$.

2. Las unidades de $\mathbb{Z}\left[\sqrt{-2}\right]$ se calculan igual, resultando que $a^2 + 2b^2 = 1 \iff a = \pm 1$ y $b = 0$. Así, las unidades en este anillo son $u = \pm 1$.

Dominios de Ideales Principales. Dominios de Factorización Única. La idea detrás de los dominios euclídeos es obtener un algoritmo de "división", para intentar parecernos lo máximo posible a un cuerpo, sin serlo. Es decir, un dominio euclídeo es lo más parecido dentro de los anillos a un cuerpo sin llegar a serlo realmente. Ser un dominio euclídeo es una condición muy fuerte, ya que $DE \Rightarrow DIP$ y $DE \Rightarrow DFU$. Vamos a probar estos hechos:

Proposición 1.1.7. *Todo dominio euclídeo A es también un dominio de ideales principales.*

Demostración. Sea $I \neq \langle 0 \rangle \subset A$, entonces, existe un elemento $d \in I$ con norma minimal para I. Para todo $p \in I$, existen $q, r \in D$ tales que $p = qd + r$ con $N(d) > N(r)$, si $r \neq 0$, entonces $r = p - qd \in I$ ya que I es un ideal de A. Y, como la norma de d es minimal, es una contradicción y debe ser que $r = 0$ y $p = qd$ para todo $p \in I$, lo que demuestra que $I = \langle d \rangle$, o sea, un ideal principal. □

Proposición 1.1.8. *Todo dominio de ideales principales A es también un dominio de factorización única.*

Demostración. Vamos a ver que todo elemento de A admite una factorización en irreducibles de A.

Primero veamos que es imposible que haya una sucesión $\{a_n\}_{n\in\mathbb{N}}$ dónde $a_{n+1} \mid a_n$ sin ser asociados. Una vez hecho esto, podemos factorizar un elemento $a \in A$, ya que sabemos que este proceso termina necesariamente.

Supongamos que una sucesión de ese estilo existe, entonces los a_i generan una cadena de ideales $\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \dots$. La unión de estos ideales es algún ideal $\langle a\rangle$. Así, $a \in \langle a_n\rangle$ para algún $n \in \mathbb{N}$ lo que implica que $\langle a_i\rangle = \langle a_n\rangle \forall i \geq n$, lo que es una contradicción.

Ahora vamos a ver que esta factorización es única.

Cada irreducible p genera un ideal $\langle p\rangle$ maximal, porque si $\langle p\rangle \subsetneq \langle a\rangle \subsetneq A$ para algún ideal $\langle a\rangle$, entonces $p = aq$ para algún $q \in A$ no unidad, lo cual contradice que p sea irreducible. Así, $A/\langle p\rangle$ es un cuerpo.

Supongamos ahora que un elemento de A tuviera dos factorizaciones

$$p_1 \dots p_r = q_1 \dots q_s$$

Consideramos los ideales $\langle p_i\rangle$ y $\langle q_i\rangle$. Reordenando si fuera necesario, digamos que p_1 genera un ideal "minimal" en el sentido de que $\langle p_1\rangle$ no contuviera estrictamente a ninguno de los otros ideales. Queremos ver que $\langle p_1\rangle = \langle q_i\rangle$ para algún i. Supongamos que no. Entonces, $\langle p_1\rangle$ no contiene a ninguno de los q_i, así q_i es no nulo módulo $\langle p_1\rangle$ para todo i, lo cuál es una contradicción porque el lado izquierdo de la ecuación es 0 módulo (p_1).

Sin pérdida de generalidad, ahora supongamos que $\langle p_1\rangle = \langle q_1\rangle$ si fuera necesario. Esto quiere decir que $p_1 = u_1 q_1$ para alguna unidad $u_1 \in A$. Cancelando (podemos hacerlo porque estamos en un dominio de integridad), nos da que $p_2 \dots p_r = u_1 q_2 \dots q_s$. Aplicando este razonamiento iterativamente llegamos a la conclusión de que $p_i = u_i q_i$, con $u_i \in \mathcal{U}(A)$ unidades, y que la factorización es esencialmente única, es decir, A es un DFU. □

Ahora que hemos probado que todo dominio euclídeo es, además, un DIP y un DFU, podemos pasar a resolver las ecuaciones diofánticas, que son ecuaciones sobre los números enteros. En general, resolver este tipo de ecuaciones es muy difícil con los métodos usuales de resolución, dado que $\mathbb{Z}$ no es un cuerpo, mucho menos algebraicamente cerrado. Así que en vez de eso, emplearemos elementos de la Teoría de Números Algebraica.

1.2. Ecuaciones diofánticas no lineales.

Ejercicio. $\mathbb{Z}[i]$ y la ecuación $x^3 = y^2 + 1$. La primera pregunta que puede surgirnos es, ¿existen dos números a y $b \in \mathbb{Z}$ tales que a sea un cubo perfecto y b sea un cuadrado perfecto y los separe una unidad? Esta pregunta es equivalente a pensar, ¿existen x e $y \in \mathbb{Z}$ tales que $x^3 = y^2+1$? En principio, resolver esta ecuación en los números enteros es complejo, y tendremos que entenderla como una ecuación en los enteros Gaussianos, $\mathbb{Z}[i]$, dónde i es solución de t^2+1. En este anillo, el polinomio anterior, que en $\mathbb{Z}$ es irreducible (ya que no tiene raíces enteras), descompone completamente. Es decir, queremos resolver la ecuación $x^3 = (y+i)(y-i)$.

Primero, es fácil ver que x e y deben tener paridades distintas. Veamos que y debe ser par y x impar. En efecto, si $x = 2q$ e $y = 2k+1$, entonces 8 debería dividir a $4k^2+4k+2$, pero se ve por inducción que no es así. Observemos que si $y+i$ e $y-i$ son coprimos en $\mathbb{Z}[i]$, entonces ambos deberán ser cubos perfectos. Vamos a probar este hecho. Supongamos que no lo fueran, entonces $\exists r \in \mathbb{Z}[i]$ de manera que $r \mid y+i$ y $r \mid y-i$. Esto implica que $r \mid 2y$ (la suma) y que $r \mid 2i$ (la diferencia). Sin embargo, $N(2i) = 4$, es decir, que r debe tener norma $1, 2$ ó 4.

1. Vamos a descartar automáticamente que $N(r) = 4$, porque entonces r sería asociado de $2i$, es decir, existe una unidad $u \in \mathbb{Z}[i]$ tal que $r = u2i$.

2. Vamos a ver que tampoco hay ningún elemento r con norma 2 que divida a $y+i$ e $y-i$. En efecto, sí que hay elementos de norma 2 en $\mathbb{Z}[i]$, que son $1+i$ y todos sus asociados (es equivalente a resolver $\alpha^2+\beta^2=2$). Sin embargo, como $2 \mid y$, $2 \nmid y+i, y-i$, así que, $1+i \mid 2i$ pero $1+i \nmid y+i, y-i$. Luego, no hay elementos de norma 2 dividiendo a ambos (de hecho, no dividen a ninguno).

3. Sólo queda que los elementos de orden 1 dividan a $y+i$ y a $y-1$ simultáneamente. Esto es que las unidades ± 1 y $\pm i$ dividan a ambos, o sea, que en efecto, son coprimos.

Así, acabamos de ver que tanto $y+i$ como $y-i$ deben ser coprimos, luego, ambos son cubos perfectos. En efecto, existe un $\alpha+i\beta \in \mathbb{Z}[i]$ tal que $(\alpha+i\beta)^3 = y+i$. Desarrollando esto, queda:

$$\begin{cases} y = \alpha^3 - 3\alpha\beta^2 \\ 1 = 3\alpha^2\beta - \beta^3 \end{cases} \tag{1.1}$$

Fijémonos en la segunda ecuación. El segundo lado de la ecuación es divisible entre β, esto quiere decir que $\beta = \pm 1$ (recordemos que α y β son números enteros). Es claro que si $\beta = 1$, entonces no tiene solución, ya que queda $2 = 3\alpha^2$, que es una ecuación sin soluciones enteras, pues $3 \nmid 2$. Si $\beta = -1$, entonces la ecuación queda $0 = 3\alpha^2$, o sea, $\alpha = 0$ ya que estamos en un dominio de integridad. Así, queda que $y = 0$ y deberá ser $x = 1$.

Ejercicio. $\mathbb{Z}\left[\sqrt{-2}\right]$ y la ecuación $x^3 = y^2 + 2$. Otra pregunta que nos puede resultar interesante, y que se resuelve recurriendo a dominios euclídeos es, ¿existen un cuadrado y un cubo perfectos en los números enteros tales que el cubo sea el cuadrado más dos unidades? Es decir, resolver esta ecuación diofántica $x^3 = y^2 + 2$. Aquí recurriremos al anillo $\mathbb{Z}\left[\sqrt{-2}\right]$, que, como hemos visto antes, también es un dominio euclídeo con norma $N\left(a+b\sqrt{-2}\right) = a^2+2b^2$. Observemos que x e y deben tener la misma paridad, y, además, que ambos son impares, ya que, si $x = 2k$ e $y = 2q$, entonces la ecuación es equivalente a $8k^3 = 4q^2 + 2 = 2\left(2q^2+1\right)$ y es claro que $2q^2+1$ nunca es un múltiplo de 4. Así, x e y deben ser impares.

Es fácil ver que las únicas unidades en este anillo son ± 1, ya que no hay más números enteros a, b con $a^2 + 2b^2 = 1$.

La ecuación anterior, dentro de $\mathbb{Z}\left[\sqrt{-2}\right]$ es equivalente a $x^3 = \left(y+\sqrt{-2}\right)\left(y-\sqrt{-2}\right)$ y el método de resolución es idéntico al anterior. Supongamos que existiera un $r \in \mathbb{Z}\left[\sqrt{-2}\right]$ con $r \mid y+\sqrt{-2}$ y $r \mid y-\sqrt{-2}$. Entonces, debe dividir a la suma y a la diferencia. En particular, $r \mid 2\sqrt{-2} \Rightarrow r \mid \sqrt{-2}$, ya que $2 \nmid y$. Pero, en este anillo, $\sqrt{-2}$ es irreducible, pues su norma euclídea, 2 es irreducible en $\mathbb{Z}$. Así, deben ser ambos cubos perfectos. En particular, $\left(\alpha+\sqrt{-2}b\right)^3 = y+\sqrt{-2}$. Desarrollando esto, queda:

$$\begin{cases} y = \alpha^3 - 6\alpha\beta^2 \\ 1 = 3\alpha^2\beta - 2\beta^3 \end{cases} \tag{1.2}$$

De nuevo, $1 = 3\alpha^2\beta - 2\beta^3$ es divisible por β, o sea, $\beta = \pm 1$. Si $\beta = -1$ la ecuación no tiene sentido ya que $3 \nmid -1$. Luego, $\beta = 1$ y $\alpha = \pm 1$. Así, $y = \pm 5$ y $x = 3$ como queríamos ver.

Algunas disquisiciones. ¿Qué pasaría si el anillo en el que trabajamos no es un dominio euclídeo? En efecto, la gran ventaja de los dominios euclídeos es, precisamente, que existe el algoritmo de Euclides para la división. Las implicaciones de esto son determinantes. La existencia de un máximo común divisor y de la coprimalidad de elementos dotan a estos

anillos de una estructura muy rica para trabajar en álgebra. Si A fuera un Dominio de Ideales Principales pero no un Dominio Euclídeo, las cosas se complican, pues, aunque sí exista el máximo común divisor, en estos anillos "no sabemos dividir" (y con esto me refiero a que es muy difícil hallar dicho máximo común divisor, al menos más difícil que en los dominios euclídeos donde la norma sea computable).

Los anillos en los que hemos trabajado a lo largo de esta sesión han sido todos anillos de números (o de enteros), que son un tipo de anillos especiales en los que se verifica una propiedad que, en general, no es cierta: Si A es un anillo de números, entonces A es un DFU $\iff$ A es un DIP. La demostración de este hecho no es trivial, y no la veremos. En cualquier caso, cuando trabajemos con anillos de enteros que sean DFU automáticamente obtendremos un DIP, con todas las características de estos.

Sin embargo, es evidente que los argumentos anteriores se caen si trabajamos con anillos de enteros que no sean DFU. Por ejemplo, ¿qué enteros x, y satisfacen la ecuación $x^3 = y^2 + 5$. En efecto, lo lógico sería trabajar en el anillo $\mathbb{Z}\left[\sqrt{-5}\right]$, pero, claro, este anillo, lejos de ser Dominio Euclídeo, no es ni siquiera un DFU, ya que $6 = 2 \times 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ y es fácil ver que ni 2 divide a $\left(1 \pm \sqrt{-5}\right)$ (ni viceversa), ni 3 divide a $\left(1 \pm \sqrt{-5}\right)$ (ni viceversa), probando que este anillo NO es un DFU.

Las técnicas que se emplean en Teoría Algebraica de Números para abordar este tipo de problemas pasan por dotar a los ideales de los anillos con una norma, y en caso de que se pueda hacer esto sin problemas, diremos que el anillo es un Dominio de Dedekind.

Capítulo 2

Introducción a la Teoría Elemental de Números.

2.1. Algunos resultados principales en Teoría Elemental de Números.

Teorema 2.1.1 (Teorema Chino de los Restos)**.** *Sean $n, m \in \mathbb{Z}$ coprimos. Entonces, la aplicación*

$$\gamma : \mathbb{Z}/(nm)\,\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$$[a]_{nm} \mapsto ([a]_n, [a]_m)$$

es un isomorfismo de anillos.

Demostración. Primero hay que ver que γ está bien definida. Tomemos $a, b \in [a]_{nm}$, entonces, tenemos que $a \equiv b \mod nm$, luego $a - b = knm \iff a = knm + b$ para cierto $k \in \mathbb{Z}$. Si reducimos módulo n y m respectivamente:

$$\begin{aligned} a &\equiv b \mod n \\ a &\equiv b \mod m \end{aligned}$$

Así, la aplicación está bien definida. Para ver que es un morfismo de anillos, no hay más que ver que las proyecciones son morfismos de anillos, y las operaciones en anillos producto se hacen coordenada a coordenada. Primero, observemos que $\mathbf{card}\,(\mathbb{Z}/(nm)\,\mathbb{Z}) = \mathbf{card}\,(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = nm$. Así que para probar que esta aplicación es un isomorfismo de anillos, hay que ver que $\ker\gamma = [0]_{nm}$. Supongamos que hubiera algún $[a]_{nm} \in \mathbb{Z}/(nm)\,\mathbb{Z}$ con $\gamma([a]_{nm}) = ([0]_n, [0]_m)$. Esto implicaría que a es un múltiplo de n y de m, luego, a es múltiplo de nm, y $a \equiv 0 \mod nm$ y el núcleo es trivial, probando así el teorema. □

Teorema 2.1.2 (Pequeño Teorema de Fermat)**.** *Si p es un número primo, entonces para cada $a \in \mathbb{Z}/p\mathbb{Z}$ se tiene que $a^{p-1} \equiv 1 \mod p$.*

Demostración. Veremos la demostración clásica que no pasa por teoría de grupos. Consideremos un elemento $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$ y la aplicación

$$mlt_a : \mathbb{Z}/p\mathbb{Z}^\times \to \mathbb{Z}/p\mathbb{Z}^\times$$

$$b \mapsto ab$$

Es claro que es una biyección. Consideremos ahora

$$\prod_{b\in\mathbb{Z}/p\mathbb{Z}^\times} a \equiv \prod_{b\in\mathbb{Z}/p\mathbb{Z}^\times} ab \mod p \Rightarrow 1 \equiv a^{p-1} \mod p$$

ya que $\prod_{b\in\mathbb{Z}/p\mathbb{Z}^\times} a$ es invertible. □

Observación 2.1.3. *Evidentemente, la biyección del teorema anterior NO es un morfismo, ya que no respeta el producto. Es claro que* $mlt_a(bc) = a\cdot bc \neq mlt_a(b)\cdot mlt_a(c) = ab\cdot ac$.

Este es un resultado clásico de la Teoría de Números, y, si bien es cierto, es bastante fuerte, uno puede preguntarse, ¿y qué pasaría para anillos modulares más generales, $\mathbb{Z}/n\mathbb{Z}$, dónde n no es un número primo? Euler, más tarde, dio una generalización de este teorema, pero antes, vamos a definir la función φ de Euler.

Definición 2.1.4. Sea $n\in\mathbb{Z}$, definimos la función $\varphi:\mathbb{Z}\to\mathbb{Z}$ de Euler como

$$\varphi(n) = \mathbf{card}\left(\{m\in\mathbb{Z} : \operatorname{mcd}(n,m) = 1, m < n\}\right)$$

.

Proposición 2.1.5. *Dado* $n\in\mathbb{Z}$, *entonces* $\mathbf{card}\left(\mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right)\right) = \varphi(n)$.

Demostración. Veamos que si $a\in\mathbb{Z}/n\mathbb{Z}$ es invertible, entonces $mcd(a,n) = 1$. Supongamos lo contrario, entonces existen $b,c\in\mathbb{Z}/n\mathbb{Z}$ no nulos tales que $ab\equiv 1 \mod n$ y $ac\equiv 0 \mod n$. Esto es una contradicción, ya que

$$\begin{aligned}(ac)\, b &\equiv 0 \mod n\\ (ab)\, c &\equiv 1c \mod n\end{aligned}$$

Sin embargo, $c\not\equiv 0$, así hemos llegado a una contradicción.

El recíproco es trivial, ya que si $\operatorname{mcd}(a,n) = 1$, entonces existen $u,v\in\mathbb{Z}$ tales que $au+nv = 1$, luego $nv = 1-au$, o sea $au\equiv 1 \mod n$. □

Proposición 2.1.6. *La función* φ *de Euler tiene las siguientes propiedades.*

a *Si* $p\in\mathbb{Z}$ *es un número primo, entonces* $\varphi(p^\alpha) = p^{\alpha-1}(p^\alpha - 1)$ *con* $\alpha\geq 1$.

b *Si* $\operatorname{mcd}(m,n) = 1$, *entonces* $\varphi(nm) = \varphi(n)\varphi(m)$ *(se dice que una función que satisface esta propiedad es multiplicativa).*

Demostración. El primer apartado se sigue fácilmente de que si p es un número primo, los únicos posibles valores de $\operatorname{mcd}(p^\alpha, m) = 1, p, p^2, \ldots, p^\alpha$, y la única manera de que sea distinto de 1 es que m sea un múltiplo de p^k para todo $1\leq k\leq\alpha$, y fijo k, hay justo $p-1$ múltiplos de p^k.

b se obtiene como un corolario del Teorema Chino de los Restos. Si $n,m\in\mathbb{Z}$ con $\operatorname{mcd}(n,m) = 1$, entonces sabemos que $\varphi(nm) = \mathbf{card}\left(\mathcal{U}\left(\mathbb{Z}/(nm)\,\mathbb{Z}\right)\right) = \mathbf{card}\left(\mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}\right)\right) = \varphi(n)\varphi(m)$. □

Observación 2.1.7. *Podemos definir que una función* f *es completamente (o totalmente) multiplicativa si dados* $a,b\in dom(f)$ *se tiene que* $f(ab) = f(a)(b)$.

La función que nos interesa ahora, es la función φ *de Euler, que es una función aritmética (cuyo dominio es* $\mathbb{N}$ *y toma valores en* $\mathbb{Q}$, $\mathbb{R}$ *ó* $\mathbb{C}$*).* $\mathbb{N}$ *tiene propiedades interesantes que nos permiten explotar el potencial de las funciones multiplicativas, como la coprimalidad de elementos y la existencia de unidades (aunque esto sea algo que más bien hereda de* $\mathbb{Z}$, *ya que* $\mathbb{N}$ *no es un anillo, aunque las operaciones aritméticas sí estén definidas). Como podemos factorizar todos*

los naturales como producto único de potencias de primos, hallar el valor de la función φ de Euler en cualquier natural resulta sencillo. Sin embargo, podemos observar que la función φ de Euler, en efecto, no es totalmente multiplicativa:

$$\varphi(4) = 2 \neq \varphi(2)\varphi(2) = 1$$

Teorema 2.1.8 (Pequeño Teorema de Euler-Fermat)**.** *Si $n \in \mathbb{Z}$, entonces, se tiene que $a^{\varphi(n)} \equiv 1$ mód n.*

Demostración. La demostración es, esencialmente, la misma que para el caso de primos. Como en $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ todos son unidades, el homomorfismo $mlt_a(x) = ax$ es una biyección. En el caso de $\mathbb{Z}/n\mathbb{Z}$ sólo sucede con los $a \in \mathbb{Z}/n\mathbb{Z}$ tales que $\text{mcd}(a, n) = 1$, y hay justo $\varphi(n)$ de ellos. □

Observación 2.1.9. *Si nos fijamos en la demostración del Pequeño Teorema de Euler-Fermat, vemos que, en realidad, estamos dando una especie de "pre-teorema" de Lagrange para grupos abelianos. Evidentemente, este argumento no sirve para grupos no abelianos, ¿por qué?*

2.2. La Ley de Reciprocidad Cuadrática

En aritmética modular, nos interesa resolver ecuaciones del tipo $x^2 = a \mod n$ para $a, n \in \mathbb{Z}$. Sobre todo, este caso es interesante si n es un número primo. ¿Cómo sabemos si estas ecuaciones modulares tienen solución sin tener que explorar todos los casos dónde x recorre los elementos de $\mathbb{Z}/n\mathbb{Z}$?

Definición 2.2.1. Dados p primo y $a \in \mathbb{Z}/p\mathbb{Z}$, definimos el símbolo de Legendre como

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si\ a \equiv 0 \mod p \\ 1 & si\ x^2 \equiv a \mod p\ tiene\ solucion \\ -1 & en\ caso\ contrario \end{cases} \tag{2.1}$$

Proposición 2.2.2 (Criterio de Euler)**.** *Si p es un primo impar y $a \in \mathbb{Z}/p\mathbb{Z}$ no nulo, entonces*

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

Demostración. Supongamos que $\left(\frac{a}{p}\right) = 1$ y tomemos un generador g de $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$. Entonces, si $a \equiv b^2 \mod p$ y $b \equiv g^k \mod p$, entonces $a \equiv g^{2k} \mod p$, luego, $a^{\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1 \mod p$.

Supongamos ahora que $\left(\frac{a}{b}\right) = -1$. Entonces $a \equiv g^{2k+1}$, y, por tanto, $a^{\frac{p-1}{2}} \equiv g^{\frac{(2k+1)(p-1)}{2}} \equiv g^{\frac{2pk+p-2k-1}{2}} \equiv g^{k(p-1)} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Proposición 2.2.3. *El símbolo de Legendre es totalmente multiplicativo.*

Demostración. Utilizando la proposición anterior, $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = (a)^{\frac{p-1}{2}} (b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, probando que es multiplicativo.

También es claro que el símbolo de Legendre es totalmente multiplicativo, ya que, al factorizar el número $a = (-1)^{\varepsilon} 2^k p_1^{k_1} \dots p_n^{k_n}$, podemos factorizar el símbolo de Legendre como los productos de los correspondientes símbolos de Legendre de los primos en la factorización y elevarlos a las potencias correspondientes. □

Proposición 2.2.4 (Criterio de Gauss). $\left(\frac{a}{p}\right) = (-1)^m$ *dónde*

$$m = \mathbf{card}\left(\left\{1 \leq k \leq \frac{p-1}{2} : ka \mod p > p/2\right\}\right)$$

y p es un primo impar.

Demostración. Vamos a considerar $U = \left\{1 \leq k < \frac{p}{2}\right\}$ y definimos la aplicación

$$\tau : U \to U$$

$$k \mapsto \pm ak$$

dónde el signo se escoge de manera que $\pm ak \mod p > \frac{p}{2}$. Es claro que τ está bien definida porque p es impar.

Vamos a ver que también es una biyección. Si tomamos $k_1, k_2 \in U$ tales que $\pm k_1 a \equiv \pm k_2 a$ mód p entonces $k_1 \equiv \pm k_2 \mod p$, y sólo es posible si $k_1 \equiv k_2$. Vamos a probar este hecho: si, en efecto fuera $k_1 \equiv -k_2 \mod p$, entonces $p \mid k_1 + k_2$, pero tenemos que $2 \leq k_1 + k_2 < p$, lo que es una contradicción. Luego debe ser $k_1 \equiv k_2 \mod p$.

Ahora,

$$\prod_{k \in U} k \equiv \prod_{k \in U} \tau(k) \equiv \prod_{k \in U} \pm ak \mod p$$

luego,

$$\prod_{k \in U} k \equiv (-1)^m a^{\frac{p-1}{2}} \prod_{k \in U} k \mod p$$

y así tenemos que $(-1)^m \equiv a^{\frac{p-1}{2}}$.

En efecto, $m = \mathbf{card}(U)$ ya que m es la cantidad de veces que tenemos que escoger el signo negativo, ya que si $ka \mod p > \frac{p}{2}$ entonces $-ka \mod p < \frac{p}{2}$ y $-ka \in U$. □

Teorema 2.2.5 (Ley de Reciprocidad Cuadrática). *Sean p y q dos números primos impares. Entonces:*

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

Demostración de Liouville. Sea ξ_p una raíz p-ésima de la unidad. Consideramos el polinomio

$$x^p - y^p = \prod_{n=0}^{p-1} \left(\xi_p^n x - \xi_p^{-n} y\right)$$

desarrollando, obtenemos la siguiente igualdad

$$\frac{x^p - y^p}{x - y} = x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^p = \prod_{n=1}^{p-1} \left(\xi_p^n x - \xi_p^{-n} y\right)$$

Evaluamos este polinomio en $x = y = 1$ y la igualdad queda

$$p = \prod_{n=1}^{p-1} \left(\xi_p^n - \xi_p^{-n}\right) = (-1)^{\frac{p-1}{2}} \prod_{n=1}^{\frac{p-1}{2}} \left(\xi_p^n - \xi_p^{-n}\right)^2$$

Y, elevando a $\frac{q-1}{2}$ ambos lados de la igualdad, queda que:

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

Hasta ahora, hemos trabajado en $\mathbb{Z}[\xi_p]$, pero ahora vamos a trabajar en $\mathbb{Z}[\xi_p]/\langle q\rangle$, es decir, vamos a reducir esa ecuación módulo q. Primero, por el Criterio de Euler, sabemos que $\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \mod q$, y, por otro lado, $\left(\xi_p^n - \xi_p^{-n}\right)^q \equiv \xi_p^{nq} - \xi_p^{-nq} \mod q$.

Así, la ecuación queda

$$\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{n=1}^{\frac{p-1}{2}} \frac{\xi_p^{nq} - \xi_p^{-nq}}{\xi_p^n - \xi_p^{-n}} \mod q$$

Es claro que, en el numerador en el denominador habrá algunas que se repitan, ya que al elevar una raíz p-ésima a un número, es lo reducir el exponente $\mod p$. Por lo tanto, el numerador recorrerá las mismas raíces que el denominador, salvo el signo. En efecto, si $nq > \frac{p}{2}$, entonces $-nq < \frac{p}{2}$ y podemos sacar factor común (-1) en esos casos y cancelar ese elemento del numerador con el correspondiente del denominador. ¿Cuál es, al final de todo esto, el exponente del (-1)? Justamente será el m definido en el Criterio de Gauss.

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

Ahora, por el Criterio de Gauss, $(-1)^m = \left(\frac{q}{p}\right)$ con lo que tenemos

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

Pasando $\left(\frac{q}{p}\right)$ al otro lado, y dándonos cuenta de que, en realidad, ahora estamos trabajando con números enteros, y no con enteros modulares, la ecuación queda

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

□

Y uno se puede preguntar, ¿Qué pasa con los casos $\left(\frac{-1}{p}\right)$ y $\left(\frac{2}{p}\right)$? Vamos a demostrar ahora las dos leyes suplementarias.

Teorema 2.2.6 (1ª Ley Suplementaria)**.** $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Demostración. Es un corolario inmediato del Criterio de Euler. □

Teorema 2.2.7 (2ª Ley Suplementaria)**.** $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Demostración. Vamos a considerar ξ_8 una raíz primitiva 8-ésima de la unidad. Por el criterio de Euler, sabemos que $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$. Hay que interpretar cuál es el número de la derecha.

Para ello, consideremos $\chi = \xi_8 + \xi_8^{-1} = \sqrt{2}$. En $\mathbb{Z}[\xi_8]$ se cumple que

$$\chi^p = \left(\xi_8 + \xi_8^{-1}\right)^p \equiv \xi_8^p + \xi_8^p \equiv \begin{cases} \chi & p \equiv \pm 1 \mod 8 \\ -\chi & p \equiv \pm 3 \mod 8 \end{cases}$$

Puesto que $\sqrt{2} = \chi$, entonces calculamos

$$2^{\frac{p-1}{2}} = \chi^{p-1} = \chi^p \chi^{-1} = \left(\xi_8 + \xi_8^{-1}\right)^p \chi^{-1} \equiv \left(\xi_8^p + \xi_8^p\right) \chi^{-1} \equiv \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

Esta formulación es equivalente a decir que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, como queríamos ver. □

2.2.1. Algunas Aplicaciones de la Ley de Reciprocidad Cuadrática.

Teorema 2.2.8. *Existen infinitos primos de la forma $p = 4n + 1$.*

Demostración. Supongamos $\{p_1, \ldots, p_k\}$ los únicos primos de la forma $p_i \equiv 1 \mod 4$. Sea $a = 4p_1 \ldots p_k$ y consideremos el número $a^2 + 1$. En efecto, existirá un p primo impar con $p \mid a^2 + 1$, es decir, $a^2 \equiv -1 \mod p$ Sin embargo, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \iff p = 4n + 1$. Es claro, además, que $p \notin \{p_1, \ldots, p_k\}$, ya que si lo estuviera, $a^2 \equiv 0 \mod p$, lo que es una contradicción.

Así, hemos creado un número primo p, de la forma $p = 4n+1$ adicional a los de la lista. □

Teorema 2.2.9. *Existen infinitos primos de la forma $p = 4n - 1$.*

Demostración. Supongamos $\{p_1, \ldots, p_k\}$ los únicos primos de la forma $p_i \equiv -1 \mod 4$. Sea $a = 4p_1 \ldots p_k$, y consideremos $a - 1$. En efecto, existirá, al menos, un primo p de la forma $p = 4n - 1$ dividiendo a $a - 1$. Si no fuera así, todos los primos serían de la forma $p = 4n + 1$, y al multiplicarlos, y ponerlos con sus correspondientes exponentes, quedaría un 1 en vez de un -1. Lo cuál es una contradicción. □

Proposición 2.2.10. *Sea p un número primo. Son equivalentes:*

1. $p = a^2 + b^2$
2. $p = 2$ *ó* $p \equiv 1 \mod 4$

Demostración. $\Rightarrow$ sabemos que $p = a^2 + b^2$. Sin embargo, no puede ser $p \equiv 3 \mod 4$, ya que $3 \equiv a^2 + b^2 \mod 4$ es una contradicción, ya que $\{0, 1\}$ son los únicos cuadrados módulo 4. Contradicción.

Así, los únicos posibles casos son $p = 4k + 1$ ó $p = 2$.

$\Leftarrow$ Evidentemente, el caso en que $p = 2$ es trivial, ya que $2 = 1^2 + 1^2$.

Supongamos que $p = 4k + 1$. Entonces, existe un $a \in \mathbb{Z}$ tal que $p \mid a^2 + 1$, luego $p \mid (a + i)(a - i)$. Sin embargo, $p \nmid a \pm i$, luego, p no es irreducible y de ahí se sige el argumento. □

2.3. El Teorema Débil del Número Primo de Dirichlet.

Vamos a introducir ahora las raíces de la unidad y los polinomios ciclotómicos.

Definición 2.3.1. Sea $n \in \mathbb{Z}$ un número natural positivo. Definimos $\xi_n \in \mathbb{C}$ a un número complejo que verifica ${\xi_n}^n = 1$, y lo denominaremos como "raíz n-ésima de la unidad". Diremos que una raíz n-ésima de la unidad es primitiva si para todo $1 \leq k < n$ se tiene que ${\xi_n}^k \neq 1$.

Definimos el n-ésimo polinomio ciclotómico como $\Phi_n = \Pi(t - \xi_n)$ dónde ξ_n es una raíz n-ésima primitiva de la unidad.

Proposición 2.3.2. *Si $n \in \mathbb{Z}$ es un número compuesto, entonces $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Además, si d_1 y d_2 son factores distintos de n, entonces $mcd(\Phi_{d_1}, \Phi_{d_2}) = 1$.*

Demostración. Las soluciones de $x^n - 1 = 0$ es el conjunto de todos los números complejos ξ tales que $\xi^n = 1$. Si $d \mid n$ y ξ_d es raíz d-ésima de la unidad, entonces $xi_d^n = \left(\xi_d^d\right)^{\frac{n}{d}} = 1^{\frac{n}{d}} = 1$, luego, también es raíz n-ésima de la unidad y el polinomio $x - \xi_d$ debe dividir a $x^n - 1$.

Para ver la otra parte del teorema observemos que si ξ_{d_1} es una raíz d_1-ésima de la unidad, y $d_1 \neq d_2$, entonces no puede ser una raíz d_2-ésima de la unidad. □

Proposición 2.3.3. *$\Phi_n(x) \in \mathbb{Z}[x]$ y mónico para todo $1 \leq n \in \mathbb{N}$*

Demostración. Vamos a demostrar por inducción este hecho. El caso $n = 1$ es trivial, ya que $\Phi_1(x) = x - 1$, que es, en efecto, un polinomio de coeficientes enteros y mónico.

Supongamos este hecho para todo $m < n$. Sea $\Phi_n(x)$. Sabemos, por la proposición anterior que $x^n - 1 = \prod_{d|n} \Phi_d(x)$, y, despejando, queda

$$\frac{x^n - 1}{\prod_{d|n} \Phi_d(x)} = \Phi_n(x)$$

Ahora, si hacemos la división de estos polinomios, como el producto de polinomios es mónico, quedará que $\Phi_n(x)$ tiene coeficientes enteros y es mónico. □

Proposición 2.3.4. *Sea $n \in \mathbb{Z}$, entonces*

$$\sum_{d|n} \varphi(d) = n$$

Demostración. Sabemos, por la proposición anterior, que

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Luego,

$$\deg\left(x^n - 1\right) = \deg\left(\prod_{d|n} \Phi_d(x)\right)$$

y $\deg\left(\Phi_d(x)\right) = \varphi(d)$, luego,

$$n = \sum_{d|n} \varphi(d)$$

como queríamos ver. □

Lema 2.3.5. *Si para un $p \in \mathbb{Z}$ primo existe un $a \in \mathbb{Z}$ tal que $p \mid \Phi_n(a)$ pero*

$$p \nmid \prod_{\substack{d \mid n \\ d < n}} \Phi_d(a)$$

entonces $p \equiv 1 \mod n$.

Demostración. Primero, sabemos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$, así que, evaluando obtenemos que $a^n - 1 = \prod_{d|n} \Phi_d(a) \Rightarrow p \mid a^n - 1$. Esto quiere decir que $ord\left(a, (\mathbb{Z}/p\mathbb{Z})^*\right) \mid n$, o sea, $a^n \equiv 1$ mód p. La idea es demostrar que este orden es, justamente, n y no ninguno de sus divisores.

Por el Pequeño Teorema de Fermat-Euler, sabemos que $ord\,(a, \mathbb{Z}/p\mathbb{Z}) \mid p-1$, y, por hipótesis, para cada $d \mid n, d < n$ tenemos que

$$\prod_{k|d} \Phi_k\,(a) = a^d - 1 \not\equiv 0 \mod p$$

, luego, $ord\,(a, (\mathbb{Z}/p\mathbb{Z})^*) \neq d$, es decir, que $ord\,(a, (\mathbb{Z}/p\mathbb{Z})^*) = n$ y tiene que ser $n \mid p-1$, o sea, $p - 1 = rn$ para algún $r \in \mathbb{Z}$, lo que prueba que $p = rn + 1$ como queríamos ver. □

Empleando este lema, vamos a demostrar el Teorema Débil del Número Primo de Dirichlet.

Teorema 2.3.6 (Teorema Débil del Número Primo de Dirichlet)**.** *Para todo $n \in \mathbb{Z}$, existen infinitos primos en la sucesión $\{kn+1\}_{n\in\mathbb{N}}$*

Demostración. Sea $k \geq 2$ y supongamos que $\{p_1, \ldots, p_s\}$ es el conjunto de todos los números primos en la sucesión $\{kn+1\}_{n\in\mathbb{N}}$. Vamos a considerar $N = k \times p_1 \times \cdots \times p_s$ y construimos el polinomio

$$Q\,(x) = \prod_{\substack{d \mid N \\ d < N}} \Phi_d\,(x)$$

Es claro que $\mathrm{mcd}\,(Q, \Phi_N) = 1$, ya que las raíces de Φ_N son todas las raíces N-ésimas primitivas de la unidad y las raíces de Q son todas las raíces n-ésimas no-primitivas, o, dicho de otra manera, para cada $d \mid nN, d < N$, todas las raíces d-ésimas primitivas son raíces de Q. Como Q y Φ_n están en $\mathbb{Q}\,[x]$, podemos hallar $U, V \in \mathbb{Q}\,[x]$ tales que se da la identidad de Bezout:

$$UQ + V\Phi_N = 1$$

Consideremos ahora un $a \in \mathbb{Z}$ tal que

$$aU, aV \in \mathbb{Z}\,[x] \tag{2.2}$$

Podemos escoger a de manera que

$$\Phi_N\,(a) \notin \{0, 1, -1\} \tag{2.3}$$

ya que hay infinitos a satisfaciendo (2.2) pero sólo hay, a lo sumo, $3\varphi\,(N)$ que satisfagan (2.3).

Así, existe un número primo $p \in \mathbb{Z}$ tal que $p \mid \Phi_N\,(a)$. Así, $a^N \equiv 1 \mod p$, luego, no puede ser $p \mid a$. Queremos ver que $p \nmid Q\,(x)$. Supongamos que sí, entonces $p \mid aU\,(a)\,Q\,(a) + aV\,(a)\,\Phi_N\,(a) = a$, lo cuál es una contradicción. Por el lema anterior, debe ser que $p \equiv 1 \mod N$, y como $n \mid N$, entonces debe ser $p \equiv 1 \mod n$. Ahora, $p \notin \{p_1, \ldots, p_s\}$, ya que $p \geq N + 1 > p_i$ para todo $i = 1, \ldots, s$. □

Como hemos visto, esta demostración es esencialmente existencialista, es decir, sólo prueba que existen infinitos primos, pero no da una manera de obtenerlos. Vamos a ver una demostración, en esencia, diferente, de que hay infinitos primos de la forma $kn + 1$ que nos va a brindar un "algoritmo" para crear números primos en esa sucesión. Para ello, necesitamos un teorema preeliminar.

Teorema 2.3.7. *Sea $n \geq 1$, p primo. Entonces, si $p \mid \Phi_n\,(a)$ para algún $a \in \mathbb{Z}$, entonces $p \mid n$ ó $p \equiv 1 \mod n$.*

Demostración. Si $p \mid \Phi_n(a)$ entonces $p \mid a^n - 1 \iff a^n \equiv 1 \mod p$. Esto quiere decir que $ord([a], (\mathbb{Z}/p\mathbb{Z})^*) \mid n$. Vamos por casos.

Primero, supongamos que $ord([a], (\mathbb{Z}/p\mathbb{Z})^*) = d < n$ con $d \mid n$. Entonces, debe ser $a^d \equiv 1 \mod p \iff p \mid a^d - 1$ y esto implica que $p^2 \mid a^n - 1 = \Phi_n(a)\left(a^d - 1\right) \ldots$. Por el mismo razonamiento, si $p \mid \Phi_n(a)$, entonces $p \mid \Phi_n(a+p)$ y, empleando el mismo argumento, $p^2 \mid (a+p)^n - 1$. Por lo tanto, $p^2 \mid na^{n-1}p \iff p \mid na^{n-1}$, y, como $p \nmid a$, entonces debe ser $p \mid n$.

Supongamos ahora que $ord([a], (\mathbb{Z}/p\mathbb{Z})^*) =$, entonces, por el Pequeño Teorema de Fermat, $n \mid p - 1$, luego $p \equiv 1 \mod n$, como queríamos ver. □

Vamos a probar ahora el Teorema Débil del Número Primo de Dirichlet utilizando este teorema anterior.

Demostración. Supongamos que hay un número finito de primos, $\{p_1, \ldots, p_k\}$ de la forma $p_i \equiv 1 \mod n$.

Consideremos $\Phi_n(np_1 \ldots p_n) \in \mathbb{Z}$. Entonces, existirá un p primo tal que $p \mid \Phi_n(np_1 \ldots p_n)$. De esta manera, $p \mid (np_1 \ldots p_n)^n - 1 \Rightarrow (np_1 \ldots p_n)^n \equiv 1 \mod p$. De aquí obtenemos que $p \nmid 1$, y por el Teorema anterior, debe ser que $p \equiv 1 \mod n$, y, por otro lado, que $p \nmid p_i$ para todo $p_i \in \{p_1, \ldots, p_k\}$. Contradicción. □

Fijémonos en qué hemos hecho exactamente en la prueba de este Teorema: hemos construido, a partir de una lista de primos finita, conocida previamente, un número entero, $\Phi_n(np_1 \ldots p_n)$, que es divisible por algún primo que no esté en esa lista (de hecho, hemos probado algo más fuerte, y es que todos sus divisores primos NO pertenecen a esa lista). Podemos imaginarnos esto como una "máquina de crear primos". En efecto, la prueba clásica de Euclides de que existen infinitos números primos utiliza un argumento muy similar a este. Si tuviéramos capacidad de cálculo suficiente, podríamos factorizar fácilmente el número $\Phi_n(np_1 \ldots p_n)$, pero eso es problema de los que estudian álgebra computacional; en realidad, a nosotros sólo nos importa que tenemos una manera explícita de crear primos de la forma $kn + 1$.

Bibliografía

[1] UNIQUE FACTORIZATION AND QUADRATIC FIELDS (MA2316, SECOND WEEK) - Vladimir Dotsenko

[2] Sur la loi de réciprocité dans la théorie des résidus quadratiques, J. math. pure appl. (I), 12 (1847), 95-96 - J. Liouville