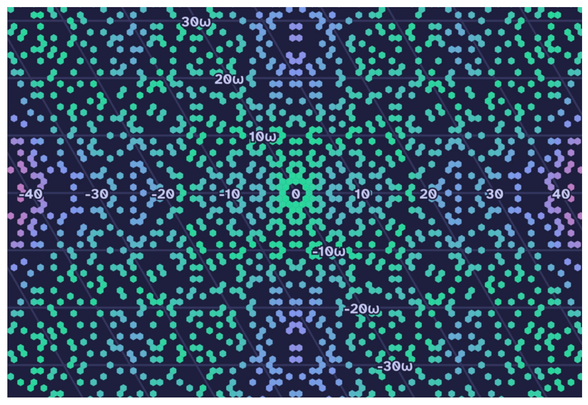
Números Primos En Otros Lugares

Mauricio Yahir Peña González[1]
Facultad de Ciencias Físico Matemático, Universidad Autónoma de Nuevo León
mauricioyairgzz@gmail.con[1]

Introduccion

Desde pequeños nos enseñan que los numeros primos son estos numeros especiales que solo se pueden dividir por 1 y por ellos mismos ¿Pero este mismo concepto se podra extender a otro tipo de numeros? La respuesta es que si, y para ello primero tenemos que recordar las propiedades que tienen los numeros primos.



Grafica ilustrativa de los primos en el Anillo $\mathbb{Z}[\omega]$

¿Que propiedades tienen los numeros primos?

Las siguientes propiedades de los numeros primos son las que nos interesa extender.
1) Factorización Única.
2) $p|\alpha\beta$, entonces $p|\alpha$ o $p|\beta$.
3) Irreducible.

Anillo de Enteros Cuadráticos $\mathbb{Z}[\sqrt{d}]$

Los Anillos de la forma $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ donde d no es 1, ni divisible por el cuadrado de un primo son ejemplos fundamentales en Álgebra Conmutativa.
Estos Anillos son Dominios de Integridad, pero no siempre son de Factorización Única.
En ellos los conceptos de elemento primo e irreducible pueden no coincidir.

Definiciones

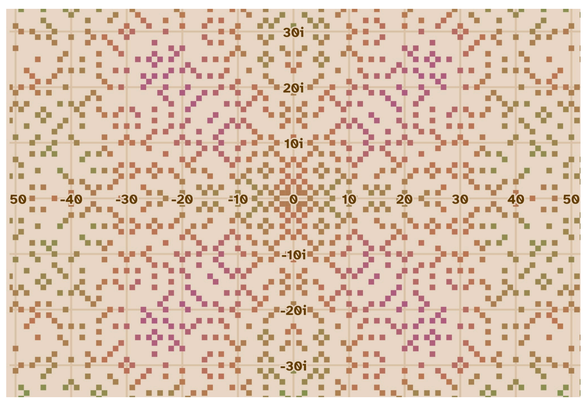
Conjugado: $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$.
Norma: $N(a + b\sqrt{d}) = a^2 - db^2$.
Unidad: u tal que $N(u) = \pm 1$.
Irreducible: No puede escribirse como producto de dos elementos no unidades.
Primo: p divide a un producto $\alpha\beta$ implica que divide a uno de ellos.

Diferencia entre Primo e Irreducible

Existe una diferencia entre Primo e Irreducible cuando no estamos en un Dominio de Factorización Única, un ejemplo clásico de esto es en $\mathbb{Z}[\sqrt{-5}]$ ya que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
Para efectos prácticos, de ahora en adelante solo trabajaremos con Dominios de Factorización Única.

Ejemplos cuando $d < 0$, $\mathbb{Z}[i]$ y $\mathbb{Z}[\omega]$

Empezando con $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ conocido como el Anillo de Enteros Gaussianos, aquí $i = \sqrt{-1}$, tenemos la propiedad $i^2 = -1$ y con la Norma vemos que hay 4 Unidades, estas son $1, -1, i$ y $-i$, por último el criterio para identificar elementos Primos es:
Todos los elementos Primos de $\mathbb{Z}[i]$ son de la forma
1) $a + bi$, con $N(a + bi) = p$.
2) $p \equiv 3 mod 4$.
Aquí p es un numero primo en $\mathbb{N}$.

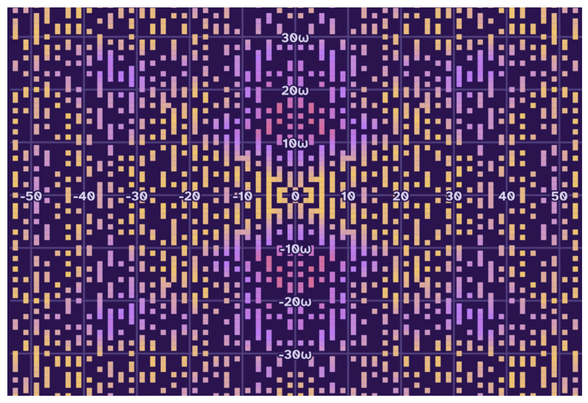


Grafica ilustrativa de los primos en el Anillo $\mathbb{Z}[i]$

De forma similar tenemos a $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$, conocido como el Anillo de Einsenstein, aquí $\omega = \frac{-1}{2} + \frac{\sqrt{-3}}{2}$, tenemos la propiedad $\omega^2 = -1 - \omega$ y con la Norma vemos que hay 6 Unidades, estas son $1, -1, \omega, -\omega, 1 + \omega$ y $-1 - \omega$, por último su criterio es:
Todos los elementos Primos de $\mathbb{Z}[\omega]$ son de la forma
1) $a + b\omega$, con $N(a + b\omega) = p$.
2) $p \equiv 2 mod 3$.

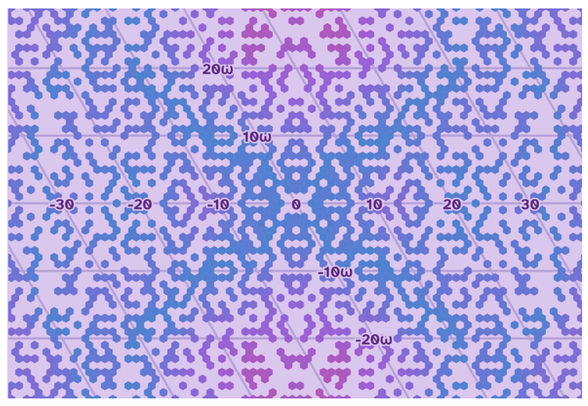
Ejemplos cuando $d > 0$, $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\phi]$

Empezando por $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$, aquí tenemos infinitas Unidades que se obtienen al resolver la ecuación de Pell $a^2 - 2b^2 = 1$, esta se obtienen de igualar la Norma a 1, al encontrar la solución mínima a la ecuación de Pell obtenemos la Unidad Fundamental la cual es $1 + \sqrt{2}$ y todas las demás son potencias de esta, por último su criterio es:
Todos los elementos Primos de $\mathbb{Z}[\sqrt{2}]$ son de la forma
1) $a + b\sqrt{2}$, con $N(a + b\sqrt{2}) = p$.
2) $p \equiv 3 mod 8$.
3) $p \equiv 5 mod 8$.



Grafica ilustrativa de los primos en el Anillo $\mathbb{Z}[\sqrt{2}]$

Siguiendo con $\mathbb{Z}[\phi] = \{a + b\phi | a, b \in \mathbb{Z}\}$, aquí tenemos infinitas Unidades, la Unidad Fundamental es ϕ y todas las demás son potencias de esta, tiene la propiedad $\phi^2 = 1 + \phi$, su criterio es:
Todos los elementos Primos de $\mathbb{Z}[\phi]$ son de la forma
1) $a + b\phi$, con $N(a + b\phi) = p$.
2) $p \equiv 2 mod 5$.
3) $p \equiv 3 mod 5$.



Grafica ilustrativa de los primos en el Anillo $\mathbb{Z}[\phi]$

Aplicaciones

Las primeras aplicaciones de toda esta teoría fueron las soluciones a distintas ecuaciones que se simplificaban en alguno de estos anillos, un ejemplo clásico es el siguiente:
Un primo p se puede escribir como $x^2 + y^2 = p$ si y solo si se factoriza en $\mathbb{Z}[i]$.

Aunque este tema no solamente se limita a aplicaciones teóricas, sino que también tenemos aplicaciones en criptografía con la criptografía basada en ideales y en curvas elípticas con multiplicación compleja

Biliografía

An Introduction to the Theory of Numbers Hardy, G. H., y Wright, E. M. (2008). An Introduction to the Theory of Numbers (6th ed.). Oxford University Press.
Algebraic Number Theory Cox, D. A. (2012). Algebraic Number Theory. Wiley.
Contemporary Abstract Algebra Gallian, J. A. (2021). Contemporary Abstract Algebra (10th ed.). Cengage Learning.