Criba de Atkin-Berstein

Juan Luis Solórzano

8 de noviembre de 2024

Teorema 6.1

Sea $n \in 1 + 4\mathbb{Z}$,Si n es positivo y libre de cuadrados entonces p es primo si y solo si,

$$4x^2 + y^2 = p$$

tiene un número impar de soluciones (x, y)

Demostración.
Sea $n \in 1 + 4\mathbb{Z}$ y libre de cuadrados
Sea $\mathcal{S} = \{(x, y) : y > 0, 4x^2 + y^2 = n\}$
Sea T el conjunto de ideales de norma n en $\mathbb{Z}$
Para cada $(x, y) \in \mathcal{S}$ defínase $f(x, y) \in T$ como el ideal generado por $y + 2xi$
Paso 1 f es inyectiva, en efecto los otros generadores de $f(x, y)$ son:

$$-y - 2xi, \qquad -2x + yi, \qquad 2x - yi$$

pero ninguno tiene la forma: $y' + 2x'i$ con $y' > 0$
Paso 2 f es sobreyectiva :
Sean $I \in T$ y $a + ib \in \mathbb{Z}[i]$ un generador de I, entonces $a^2 + b^2 = n$
Notese que $a \neq 0 \neq b$ pues n es libre de cuadrados, tenemos entonces:

continua.

$$\begin{cases} I = f\left(\frac{-a}{2}, b\right) & \text{si } a \in 2\mathbb{Z} \text{ y } b > 0 \\ I = f\left(\frac{a}{2}, -b\right) & \text{si } a \in 2\mathbb{Z} \text{ y } b < 0 \\ I = f\left(\frac{b}{2}, a\right) & \text{si } a \in 2\mathbb{Z}+1 \text{ y } b > 0 \\ I = f\left(\frac{-b}{2}, a\right) & \text{si } a \in 2\mathbb{Z}+1 \text{ y } b < 0 \end{cases}$$

Paso 3 Si n es primo, entonces,
$\#T = 2 \Rightarrow \#\{(x,y) : x > 0, y > 0, 4x^2 + y^2 = n\} = \frac{\#\mathcal{S}}{2} = \frac{\#T}{2} = 1$
Si $n = p_1 p_2 \dots p_r$ con p_i primos distintos ,
El número de ideales de norma p_i es par para cada $1 \leqslant i \leqslant r$

$$\Rightarrow 2^r \mid \#T \Rightarrow 4 \mid \#T \Rightarrow \#\{(x,y) : x > 0, y > 0, 4x^2 + y^2 = n\} = \frac{\#\mathcal{S}}{2} = \frac{\#T}{2} \in 2\mathbb{Z}$$

□

Teorema 6.2

Sea $n \in 1 + 6\mathbb{Z}$. Si n es positivo y libre de cuadrados, entonces n es primo si y solo si,

$$3x^2 + y^2 = n$$

tiene un número impar de soluciones (x, y) con $x > 0$ y $y > 0$.

Demostración.
Sea $n \in 1 + 6\mathbb{Z}$ y libre de cuadrados.
Sea $\mathcal{S} = \{(x, y) : y > 0, 3x^2 + y^2 = n\}$.
Sea T el conjunto de ideales de norma n en $\mathbb{Z}[\omega]$, donde $\omega = \frac{-1+\sqrt{-3}}{2}$.
Para cada $(x, y) \in \mathcal{S}$, defínase $f(x, y) \in T$ como el ideal generado por $x + y + 2x\omega$.
De forma analoga a la prueba anterior se puede probar que:
Paso 1: f es inyectiva.
Paso 2: f es sobreyectiva.
Si n es primo, entonces $\#T = 2$, lo que implica que:

$$\#\{(x, y) : x > 0, y > 0, 3x^2 + y^2 = n\} = \frac{\#\mathcal{S}}{2} = \frac{\#T}{2} = 1.$$

Si n es un producto de primos, entonces $\#T$ es divisible por 4, lo que implica que el número de soluciones es par.

Teorema 6.3

Sea $n \in 11 + 12\mathbb{Z}$. Si n es positivo y libre de cuadrados, entonces n es primo si y solo si,

$$3x^2 - y^2 = n$$

tiene un número impar de soluciones (x, y) con $x > y > 0$.

El algoritmo

El teorema 6.1 nos permite encontrar primos de la forma $4k+1$ es decir $12k+1$ y $12k+5$
El teorema 6.2 nos permite encontrar primos de la forma $6k+1$ es decir $12k+1$ y $12k+7$
el teorema 6.3 nos permite encontrar prios de la forma $12k+1$
Podemos encontrar usando esos teoremas todos los primos mayores a 5

```python
def CribaAB(N):
    criba = [0]*(N+1)
    lim = int(N**0.5)+1

    for x in range(1,lim):
        for y in range(1,lim):
            # teorema 6.1
            # n = 4x**2 + y**2
            n = 4*x**2 + y**2
            # verificar si n es candidato a ser primo de la forma 4k +1
            if n<= N and (n%12 ==1 or n% 12 ==5 ):
                criba[n] = 1 - criba[n]

            # teorema 6.2
            # n = 3*x**2 +y**2
            n = 3*x**2 +y**2
            # verificar si n es candidato a ser primo de la forma 6k+1
            if n<= N and n % 12 == 7:
                criba[n] = 1 - criba[n]

            # teorema 6.3
            # n = 3*x**2-y**2
            n = 3*x**2-y**2
            if n<= N and n % 12 == 11:
                criba[n] = 1 - criba[n]
    #eliminar cuadrados de primos
    for p in range(5,lim, 2):
        if criba[p]:
            p2 = p**2
            for i in range(p2, N+1,p):
                criba[i] = 0
    primos = [2,3] + [i for i in range(5,N+1) if criba[i]]
    return primos
```

References

A. O. L. Atkin and D. J. Bernstein.

Prime sieves using binary quadratic forms.

Mathematics of Computation, 73(246):1023–1030, 2003.

Article electronically published on December 19, 2003.