7. Teoría de números

La teoría de números es una de las ramas de la matematicas que estudia los números naturales ($\mathbb{N}$) y los enteros, de los enteros ($\mathbb{Z}$) estudia sus propiedades.

Recordemos que:
- Los numeros enteros son $\{..., -1, 0, 1, ...\}$
- Nuestra definición de naturales no invluye 0 por defecto

7.1. Conjetura de Goldbash

En teoría de números cambian las definiciones con respecto a las matemáticas tradicionales. Goldbash dice que
- Para los números pares, los pares mayores a 2 $\mathbb{P} + \mathbb{P}$, se pueden extraer de la suma de dos números primos, ej. $3 > 2 \Leftrightarrow 3 = 2 + 1$
- Para los números impares mayores a 5 $\mathbb{P} + \mathbb{P} + \mathbb{P}$, todos son igualables a la suma de tre números primos, ej $7 = 2 + 2 + 3$

7.2. Teorema de Fermat

Partiendo de Pitágoras $a^2 + b^2 = c^2$, Fermat exploró qué sucede con las expresiones al ser de grado n de la forma $a^n + b^n = c^n$. El dice que es imposible encontrar 3 números enteros positivos tal que $a^n + b^n = c^n$ cuando $n > 2$.

7.3. Ejemplos de demostraciones

La forma para representar $2^2 = 4$ podemos dibujar 4 puntos en un cuadrado, haciendo gráficamente un cuadrado con 4 puntos, si es 3^2 hacemos un cuadrado de 9 puntos.

Asi como vemos que existen números cuadrados pueden existir números *triangulares*, en el caso de los números cuadrados es n^2, para los triangulares tenemos $\{3, 6, 10, 15, ...\}$, en la teoría de números debemos buscar una función que pueda modelar la representación.

$$\frac{(n)(n+1)}{2}$$

Debemos de hacer el análisis que logre describir la serie de números para resolver los problemas que se nos presenten. La teoría de números se emplea en distintos tipos de entrada.

No vamos a estar haciendo en loops sumas, series, que pueden moldearse en una función que permite describir para cualquier posición t el valor.

7.3.1. Suma

Otro ejemplo de fórmula, la fórmula que describe cualquier suma consecutiva de números

$$\frac{n(1+n)}{2}$$

Es decir, vamos a empezar a demostrar de forma inductiva, por medio de una función.

7.3.2. Paridad de enteros

Partiendo de $n \in \mathbb{Z}$, podemos definir:
- Par: $2n$
- Impar: $2n + 1$

Y podemos analizar las propiedades:
- par + par = par
- par + impar = impar
- impar + impar = par
- par $\times$ par = par
- impar $\times$ impar = impar

Y podemos demostrar, por ejemplo par $\times$ par = par de la forma:

$$
\begin{aligned}
(2n+1)(2n+1) & \\
&= (2n+1)^2 \\
&= 4n^2 + 4n + 1 \\
&\therefore \text{impar}
\end{aligned}
$$

7.3.3. Divisores

Sea $a, b \in \mathbb{Z}$ tal que $a \neq 0$ y se dice que a debe ser *divisor* de $b \Rightarrow K$, donde $K \in \mathbb{Z}$ que satisface $b = ka$. Si depejamos $k = \frac{b}{a}$.

El teorema de divisor lleva, naturalmente, a los números primos.

7.3.4. Divisor trivial

Con *trivial* hablamos de proposiciones que no es necesario demostrar, la sola proposición lo demuestra.

El divisor trivial es

Entonces los primos son aquellos que tienen divisores triviales.

7.3.5. Teorema fundamental de la aritmética

Cada entero puede ser factorizado por el producto de números primos, por ejemplo $6 = 3 \times 2$.

7.3.6. Primos de Mersenne

Aquellos números que están derivados de la expresión $M(p) = 2^p - 1$, donde $p \in \mathbb{P}$. Con los primeros 20 primos de la teoría de la aritmética, hallar los 20 primeros números primos de Mersenne.

El código resultante, delegando la generación de los números primos al *crate* `primes`, es:

```rust
use primes::{PrimeSet, Sieve};

fn main() {
    for p in Sieve::new().iter().take(20) {
        println!("{}", 2u128.pow(p as u32) - 1);
    }
}
```

Con la salida del programa:

```
   Compiling primos v0.1.0 (/Users/alejandro/repos/primos)
    Finished dev [unoptimized + debuginfo] target(s) in 0.40s
     Running `target/debug/primos`
3
7
31
127
2047
8191
131071
524287
8388607
536870911
2147483647
137438953471
2199023255551
8796093022207
140737488355327
9007199254740991
576460752303423487
2305843009213693951
147573952589676412927
23611832414348226068 47
```