

## Teorema de Proth

Sea  $N$  un número de Proth, es decir de la forma  $N = k2^n + 1$  con  $k$  impar y  $k < 2^n$ , entonces si para algún número entero  $a$  se cumple que:

$$a^{\frac{N-1}{2}} \equiv -1 \pmod{N} \quad (1)$$

entonces  $N$  es un número primo llamado primo de Proth. Este test funciona en la práctica porque si  $N$  es primo, el 50 % de los valores de  $a$  cumplen con la condición indicada arriba.

**Dem:**

### Generalización del test de Pocklington

Factorizar  $N - 1$  como  $N - 1 = AB$ , donde  $A$  y  $B$  son coprimos y  $A > \sqrt{N}$ . La factorización de  $A$  se conoce, pero la de  $B$  no es necesaria. Entonces si para cada factor  $p$  primo de  $A$  existe  $a_p$  tal que

$$a_p^{N-1} \equiv 1 \pmod{N} \quad (2)$$

$$\gcd\left(a_p^{\frac{N-1}{p}} - 1, N\right) = 1 \quad (3)$$

entonces  $N$  es primo.

Tenemos que  $N - 1 = k2^n$ , entonces para  $A = 2^n$  y  $B = k$  se cumplen los requisitos del enunciado. Lo primero como  $k$  es impar y  $k < 2^n$  tenemos que  $A$  y  $B$  son coprimos y además  $A > \sqrt{N}$ . Además el único factor primo de  $A$  es 2, veamos un  $a_2$  tal que cumpla (2) y (3).

Sabemos que existe un  $a$  tal que cumple (1) entonces,

$$\begin{aligned} a^{\frac{N-1}{2}} + 1 &\equiv 0 \pmod{N} \\ \left(a^{\frac{N-1}{2}} + 1\right) \left(a^{\frac{N-1}{2}} - 1\right) &\equiv 0 \pmod{N} \\ a^{N-1} - 1 &\equiv 0 \pmod{N} \end{aligned} \quad (4)$$

$a$  cumple (2). Por otro lado

$$\begin{aligned} a^{\frac{N-1}{2}} - 1 &\equiv -2 \pmod{N} \\ (k2^{n-1}) \left(a^{\frac{N-1}{2}} - 1\right) &\equiv (k2^{n-1})(-2) \pmod{N} \\ (k2^{n-1}) \left(a^{\frac{N-1}{2}} - 1\right) &\equiv -k2^n \pmod{N} \\ (k2^{n-1}) \left(a^{\frac{N-1}{2}} - 1\right) &\equiv 1 \pmod{N} \end{aligned} \quad (5)$$

por tanto

$$\begin{aligned}
(k2^{n-1}) \left( a^{\frac{N-1}{2}} - 1 \right) &= 1 + xN \\
(k2^{n-1}) \left( a^{\frac{N-1}{2}} - 1 \right) + (-x)N &= 1 \\
\gcd \left( a^{\frac{N-1}{p}} - 1, N \right) &= 1
\end{aligned} \tag{6}$$

así  $a_2 = a$  cumple (2) y (3), y por tanto  $N$  es primo.

Veamos que además si  $N$  fuera primo, entonces existen un 50 % de probabilidades de encontrar dicho  $a$ .

### Criterio de Euler

Si  $N$  es primo entonces

$$a^{\frac{N-1}{2}} \equiv \begin{cases} 1 \pmod{N}, & \text{si } \exists x \text{ tal que } x^2 \equiv a \pmod{N}, \\ -1 \pmod{N}, & \text{en otro caso.} \end{cases} \tag{7}$$

Efectivamente si  $N$  es primo, entonces por el pequeño teorema de Fermat tenemos que para cualquier  $a$  coprimo con  $N$  ( $a \in \{1, \dots, N-1\} \subset \mathbb{Z}/N\mathbb{Z}$ ) se cumple

$$\begin{aligned}
a^{N-1} &\equiv 1 \pmod{N} \\
a^{N-1} - 1 &\equiv 0 \pmod{N} \\
\left( a^{\frac{N-1}{2}} - 1 \right) \left( a^{\frac{N-1}{2}} + 1 \right) &\equiv 0 \pmod{N}
\end{aligned} \tag{8}$$

de la última ecuación sacamos que por ser módulo un primo  $N$ , uno de los dos factores han de ser congruentes con cero. Definimos los siguientes conjuntos:

$$\begin{aligned}
A &= \left\{ a \in \mathbb{Z}/N\mathbb{Z} \mid a^{\frac{N-1}{2}} - 1 \equiv 0 \pmod{N} \right\}, \\
B &= \left\{ a \in \mathbb{Z}/N\mathbb{Z} \mid a^{\frac{N-1}{2}} + 1 \equiv 0 \pmod{N} \right\}.
\end{aligned}$$

Si  $a \equiv x^2 \pmod{N}$  entonces  $a^{\frac{N-1}{2}} - 1 \equiv x^{N-1} - 1 \equiv 0 \pmod{N}$ , por lo que todos los residuos cuadráticos están contenidos en  $A$ . Además por el Teorema de Lagrange tenemos que tanto  $A$  como  $B$  no pueden tener más de  $\frac{N-1}{2}$  de soluciones distintas, es decir  $|A|, |B| \leq \frac{N-1}{2}$ , mientras que  $|A| + |B| = p-1$  por (8), esto es si y sólo si  $|A| = |B| = \frac{N-1}{2}$ .