Test de primalidad de Pocklington

Ana Sofía Escobar

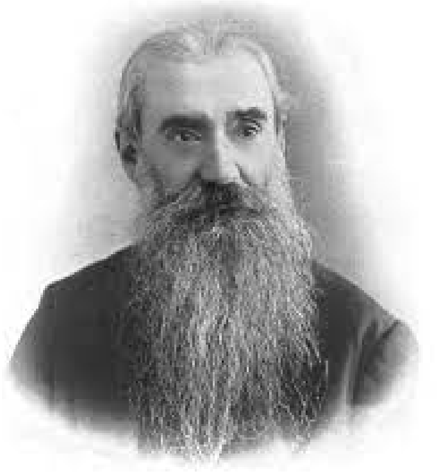
Universidad del Valle de Guatemala
Facultad de Ciencias y Humanidades
Teoría de Números

18 de noviembre de 2023

Contenido

Historia

- El test de primalidad de Pocklington fue propuesto por el matemático y físico inglés Henry C. Pocklington en 1914.
- Fue propuesto como una alternativa más eficiente al test de primalidad de Lucas, requiriendo solo la factorización parcial de $n-1$.



HENRY POCKLINGTON,

Test de primalidad de Lucas

Theorem (Test de Lucas)

Sea $n > 1$. Si para cada factor primo q de $n-1$ existe un entero a tal que

$$a^{n-1} \equiv 1 \pmod{n},$$

y

$$a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n};$$

entonces n es primo.

El Test de Lucas, también conocido como el Test de Lucas-Lehmer, es un método para verificar la primalidad de un número de Mersenne, que tiene la forma $2^p - 1$, donde p es un número primo.

Teoremas útiles

Theorem (Pequeño teorema de Fermat)

Sean $a \in \mathbb{Z}$ y p un número primo, y a no es divisible por p. Entonces,

$$a^p \equiv a \pmod{p}.$$

Theorem (Euler-Fermat)

Sean $a, n \in \mathbb{Z}$, con $n > 1$ siendo dos enteros tales que $(a, n) = 1$. Entonces,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Theorem (Test de primalidad)

Sea $N > 1$ un número entero, y supongamos que existen números naturales a y p tales que:

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

$$p \text{ es primo}, \; p|N-1 \text{ y } p > \sqrt{N}-1 \quad (2)$$

$$mcd\left(a^{(N-1)/p}-1, N\right) = 1 \quad (3)$$

Entonces, N es primo.

La Ecuación 1 se relaciona directamente con el teorema de Euler-Fermat. Si encontramos cualquier valor de a que no sea divisible por N y que haga que la Ecuación 1 sea falsa, podemos concluir inmediatamente que N no es primo.

Test de Pocklington

Demostración.

Supongamos que N no es primo. Esto significa que debe existir un primo q, donde $q \leq \sqrt{N}$, que divide a N.

.

Dado que $p > \sqrt{N} - 1 \geq q - 1$, $p > q - 1$, y dado que p es primo, $\mathrm{mcd}(p, q-1) = 1$.

.

Por lo tanto, debe existir un entero u, el cual es un inverso multiplicativo de p módulo $q - 1$, con la propiedad de que

$$up \equiv 1 \pmod{q-1}$$

y, por lo tanto, por el pequeño teorema de Fermat,

$$a^{up} \equiv a \pmod{q}$$

Test de Pocklington

Demostración.

Esto implica

$$1 \equiv a^{N-1} \pmod{q}$$

por hipotesis (1) ya que $q|N$.

$$1 \equiv (a^{N-1})^u \equiv a^{up((N-1)/p)} \equiv (a^{up})^{(N,1)/p} \pmod{q}$$

$$\Rightarrow 1 \equiv a^{(N-1)/p} \pmod{q}$$

Esto muestra que q divide al mcd en la hipotesis (3), y por lo tanto este mcd no es igual a 1, lo cual es una contradicción. □

Test de Pocklington: Problemas

Cuando se brinda p desde un principio a es simple de encontrar pero en caso contario, suele ser complicado encontrar un valor de p que satisfaga la ecuación (2) de la hipotesis:

- Generalmente es difícil encontrar un factor primo (p).
- Para muchos primos N, dicho p no existe.
- La eficiencia del Test depende de la elección del a.

.

Por ejemplo, $N = 17$ no tiene un p adecuado porque $N - 1 = 2^4$, y $p = 2 < \sqrt{N} - 1$, lo que no cuple la desigualdad en (2).

Test Generalizado de Pocklington

Corollary (Test Generalizado de Pocklington)

Factorice $N-1$ como $N-1 = AB$, donde A y B son primos relativos, $A > \sqrt{N}$, la factorización prima de A es conocida, pero la factorización de B no necesariamente es conocida.
Si para cada factor primo p de A existe un entero a_p tal que

$$a_p^{N-1} \equiv 1 \pmod{N}$$

y

$$\gcd(a_p^{(N-1)/p} - 1, N) = 1,$$

entonces N es primo.

Test Generalizado de Pocklington

Demostración.

Sea p un primo que divide a A, y sea p^e la potencia máxima de p que divide a A. Sea q un factor primo de N. Para el a_p del teorema, sea $b \equiv a_p^{(N-1)/p^e} \pmod{q}$. Esto implica que $b^{p^e} \equiv a_p^{N-1} \equiv 1 \pmod{q}$, y debido a que $mcd(a_p^{(N-1)/p} - 1, N) = 1$, también $b^{p^{e-1}} \equiv a_p^{(N-1)/p} \not\equiv 1 \pmod{q}$.

.

Esto significa que el orden de $b \pmod{q}$ es p^e. Así, p^e divide a $(q-1)$. Esto se cumple para cada factor de potencia primo p^e de A, lo que implica que A divide a $(q-1)$. Y entonces $q > A \geq \sqrt{N}$.

.

Si N fuera compuesto, necesariamente tendría un factor primo menor o igual a $\sqrt{N}$. Se ha demostrado que no existe tal factor, lo que prueba que N es primo.

$\square$

Ejemplo

Ejercicio: Determinar si $N = 27457$ es un número primo.

.

Primero, buscamos factores primos pequeños de $N - 1$. Notese que $N - 1 = 2^6 \cdot 3 \cdot 143 = 27546$. Debemos determinar si $A = 192$ y $B = 143$ cumplen las condiciones del Corolario. $A^2 = 36864 > 27457 = N$, así que $A > \sqrt{N}$. Por lo tanto, hemos factorizado lo suficiente de $N - 1$ para aplicar el Corolario. También debemos verificar que $\gcd(A, B) = 1$.

.

Finalmente, para cada factor primo p de A, usar prueba y error para encontrar un a_p que satisfaga las condiciones del corolario.

.

Ejemplo

Para $p = 2$, probar $a_2 = 2$. Elevar $2^{13728} \equiv 1 \pmod{27457}$, pero $\gcd(2^{13728} - 1, 27457) = 27457$. Entonces, $a_2 = 2$ satisface la primera pero no la segunda condicion del corolario. Probar $a_2 = 5$ en su lugar: $5^{13728} \equiv 1 \pmod{27457}$, y $\gcd(5^{13728} - 1, 27457) = 1$. Entonces, $a_2 = 5$ satisface cambas condiciones.

.

Para $p = 3$, probar $a_3 = 2$: $2^{9152} \equiv 1 \pmod{27457}$, y $\gcd(2^{9152} - 1, 27457) = 1$. Entonces, $a_3 = 2$ satisface cambas condiciones.

.

Por lo tanto N=27457 es primo y note a los dos pares (p, a_p) $(2, 5)$ y $(3, 2)$.

¿Preguntas?

Referencias

[1] **Caldwell, C. K.**
Primality proving 3.1: N-1 tests and Pepin's test for Fermats.
Disponible en: https://t5k.org/prove/prove3_1.html

[2] **Șuteu, D.**
Primality testing algorithms.
trizenx, 17 de septiembre de 2023.
Disponible en: https://trizenx.blogspot.com/2020/01/primality-testing-algorithms.html

[3] **Wikipedia contributors.**
Pocklington Primality test.
Wikipedia, 29 de octubre de 2023.
Disponible en:
https://en.wikipedia.org/wiki/Pocklington_primality_test