

Primality Tests

ANISHA JOSEPH

Primality Tests

Decide whether a number is prime or composite.

Pseudoprimes

Proposition 14.1. (*Fermat Primality Test*) *Let $n > 1$ be an odd integer. Choose an integer b with $1 < b < n$. (Often, we choose $b = 2$.) If $b^{n-1} \not\equiv 1 \pmod{n}$ then n is composite.*

Proof. If n is prime, then Fermat's theorem says that $b^{n-1} \equiv 1 \pmod{n}$, which we have assumed does not happen. Therefore, n cannot be prime. \square

Pseudoprimes

Example. Let's show that 209 is not prime. We start by noting that $2^4 \equiv 16 \pmod{209}$. By successive squaring, we have

$$\begin{aligned} 2^8 &\equiv 16^2 \equiv 47 \pmod{209} \\ 2^{16} &\equiv 47^2 \equiv 119 \pmod{209} \\ 2^{32} &\equiv 119^2 \equiv 158 \pmod{209} \\ 2^{64} &\equiv 158^2 \equiv 93 \pmod{209} \\ 2^{128} &\equiv 93^2 \equiv 80 \pmod{209}. \end{aligned}$$

Therefore,

$$2^{208} \equiv 2^{128} \cdot 2^{64} \cdot 2^{16} \equiv 80 \cdot 93 \cdot 119 \equiv 36 \not\equiv 1 \pmod{209}.$$

The fact that we showed 209 is composite without factoring it or finding any prime divisors is the key to why this method is fast.

b-pseudoprime

Definition 14.2. A composite integer $n > 1$ is called a ***b*-pseudoprime** if $b^{n-1} \equiv 1 \pmod{n}$.

For example, 341 is a 2-pseudoprime. The number 91 is a 3-pseudoprime because $3^{90} \equiv 1 \pmod{91}$ but $91 = 7 \times 13$. However, we can use the Fermat Test to check that 341 and 91 are composite, without factoring, by computing

$$3^{340} \equiv 56 \pmod{341} \quad \text{and} \quad 2^{90} \equiv 64 \pmod{91}.$$

hhhh

Fermat's pseudoprimes

A composite number p is called a Fermat pseudoprime to a base a if it satisfies Fermat's Little Theorem for that base, meaning:

$$a^{p-1} \equiv 1 \pmod{p}$$

Eg: 561

For $a=2$, $2^{561-1} \equiv 1 \pmod{561}$

Carmichael number

Definition 14.3. A composite $n > 1$ is called a **Carmichael number** if $b^{n-1} \equiv 1 \pmod{n}$ for all integers b with $\gcd(b, n) = 1$.

Example. 561 and 1729 are Carmichael numbers. Let's prove this for $561 = 3 \times 11 \times 17$. Fermat's theorem says that if $b \not\equiv 0 \pmod{17}$ then $b^{16} \equiv 1 \pmod{17}$. Therefore,

$$b^{560} \equiv (b^{16})^{35} \equiv (1)^{35} \equiv 1 \pmod{17}.$$

Similarly, when $b \not\equiv 0 \pmod{11}$, Fermat's theorem tells us that $b^{10} \equiv 1 \pmod{11}$, so

$$b^{560} \equiv (b^{10})^{56} \equiv (1)^{56} \equiv 1 \pmod{11}.$$

Finally, when $b \not\equiv 0 \pmod{3}$, Fermat tells us that $b^2 \equiv 1 \pmod{3}$, which implies that $b^{560} \equiv 1 \pmod{3}$. We now have, whenever $\gcd(b, 561) = 1$, that $b^{560} - 1$ is a multiple of 3, 11, and 17. Therefore, it is a multiple of $561 = 3 \times 11 \times 17$. This is exactly the statement that

$$b^{560} \equiv 1 \pmod{561}$$

for all integers b with $\gcd(b, 561) = 1$, so 561 is a Carmichael number.

Euler pseudoprimes

A composite number p is called an Euler pseudoprime to base a if it satisfies:(Satisfies Euler's criterion)

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

They "fool" the Euler criterion primality test, making them appear to be prime under this test.

Eg: 561 for base a=2

