Strong prime p

$$\left.\begin{aligned} p-1 &= 2rj \\ r-1 &= 2tm \\ p+1 &= 2sl \end{aligned}\right\}$$

$p = 3628273133$ $\qquad$ $p-1 = 3628273132$

The largest f

$= \cancel{36} \; \underbrace{28211} \times 128612$

p Not - strong prime as 28211 is the largest prime factor of $p-1$ which is not large.

$\bullet\; p = 2^{82589933} - 1$

Then $p+1$, the largest prime factor is $\underline{2}$.

- Testing a number whether it is a prime

Primality test

$$\boxed{\text{If } (a, p) \text{ then } a^{p-1} \equiv 1 \mod p.}$$

- n is composite if $a^{p-1} \not\equiv 1 \mod p$ for $(a, p) = 1$

E.g.,

$a = 2, \quad n = 341 = 11 \times 31$

$2^{11-1} = 2^{10} \equiv 1 \mod 11 \Rightarrow 2^{340} = (2^{10})^{34} \equiv 1 \mod 11$

$2^{31-1} = 2^{30} \equiv 1 \mod 31 \Rightarrow 2^{340} \equiv 1 \mod 31$

$11, 31 \mid 2^{340} - 1 \Rightarrow 341 = 11 \times 31 \mid 2^{340} - 1$

$\therefore 2^{341-1} \equiv 1 \mod 341$

$(2^{30})^{11} = 2^{330} \equiv 1 \mod 31$
$= 2^{330} \times 2^{10} \equiv 1 \mod 31$

Pseudoprime : A composite number n is said to be a pseudoprime to the base b ~~(where g~~ where $\gcd(b, n) = 1$ if $b^{n-1} \equiv 1 \pmod{n}$.

Carmichael number: A composite number which is a pseudoprime to base every $1 < b < n$ with $\gcd(b, n) = 1$

E.g., 561, 1105

$n = 561 = 3 \times 11 \times 17$

Chose $1 < b < 561$ so that $\gcd(b, 3) = 1$, $\gcd(b, 11) = 1$ & $\gcd(b, 17) = 1$ so that $\gcd(b, n) = 1$

$b^2 \equiv 1 \mod 3 \Rightarrow b^{560} \equiv 1 \mod 3$

$b^{10} \equiv 1 \mod 11 \Rightarrow b^{560} \equiv 1 \mod 11$

$b^{16} \equiv 1 \mod 17 \Rightarrow b^{560} \equiv 1 \mod 17$

Since 3, 11, 17 are coprime pairwise

$b^{561-1} = b^{560} \equiv 1 \mod 3 \times 11 \times 17$

561 is the smallest Carmichael number.

Choose $b=3$ for $n=341$

$3^{341-1} \equiv \overset{?}{56}$ mod 341

$\not\equiv 1$ mod 341

Fermat's primality test fails for 341

For this test the output is either get a composite number of test fails.

Wilson's Thm: $n \in \mathbb{N} \setminus \{1\}$ is a prime if & only if $(n-1)! \equiv -1 \pmod{n}$

Proof: Suppose $n = p$, a prime.

Then $\underbrace{1, 2, 3, \ldots, (p-1)}$ are units in $\mathbb{Z}_p$

(or $U(\mathbb{Z}_p) = \mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$)

In the group $\mathbb{Z}_p^\times$ every element has a unique inverse. Pair each with its inverse.

$\exists\ 1 < m < p$ s.t. $m^2 \equiv 1 \pmod{p}$. But $m \neq 1$, so $m \equiv -1$ mod p ($= p-1$, mod p)

So $(p-1)! = 1 \times 2 \times \cdots \times (p-1)$

$= m \pmod{p}$

$= -1 \pmod{p}$

Converse, Assume $(n-1)! \equiv -1 \pmod{n}$

Suppose n is not a prime. Let $n > d > 1$ & $d \mid n$.

Since $n \mid (n-1)! + 1$, $d \mid (n-1)! + 1$

on the other hand $d \mid (n-1)!$ (since $1 < d < n$)

Thus $d \mid 1$ a contradiction

So n must be a prime.

Miller-Rabin test:

Propn: Let p be an odd prime & write
$p-1 = 2^k q$ where $\gcd(2,q)=1$

Let $a \in \mathbb{N}$ s.t. $p \nmid a$. Then one of the following statements is true

① $a^q \equiv 1 \mod p$

② One of $a^q, a^{2q}, a^{2^2 q}, \ldots, a^{2^{k-1} q}$ is congruent to -1 modulo p.