Number Theory

Gauss - "Math is the queen of the Sciences and Number Theory is the queen of Math"

Prime Numbers - Integers 2 or greater that are only divisible by 1 and itself.

Fnd Thm Arith - All integers have a unique prime factorization

$175 = 5^2 \times 7^1$

① Slow prime test → trial div until $\sqrt{n}$. (must be included)

② Prime factorization

Question: Is n prime?

$n = 143$

Trial Division

$143 \% 2 = 1$ (not divis by 2)

$143 \% 3 = 2$ (" " 3

$143 \% 4 = 3$ (" " 4, can skip in computer) we usually run it

$\vdots$

$143 \% 11 = 0$ ✓ EADA! $143 = 11 \times 13$

If not prime, $xy = n$

$\sqrt{n}\sqrt{n} = n$ → if x, y exist either $x \leq \sqrt{n}$ or $y \leq \sqrt{n}$

if $x > \sqrt{n}$ and $y > \sqrt{n}$, $xy \neq n$.

Prime fact

$1008 = 8 \times 126 = 2^3 \times 126$

$= 2^3 \times 2 \times 63$

$= 2^3 \times 2 \times 7 \times 3^2$

$= \boxed{2^4 \times 3^2 \times 7}$

$2008 = 8 \times 251$

$= 2^3 \times 251$

Each # can be written as

$$\prod_{p_i \in Primes} p_i^{q_i}$$

How many integers in between 1 and n share no common factor with n? (LATER)

Fermat's Thm: if $gcd(a,p)=1$, $p \in Prime$, then

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

Start with $S = \{1, 2, 3, \ldots, p-1\}$

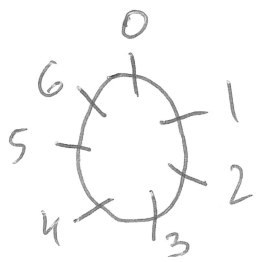
Create new set $T = \{a, 2a, 3a, \ldots a(p-1)\}$ mult each value by a

$gcd(a,p)=1$

p = Prime

Values in set T are equivalent values in set S mod p.

p=7	1	2	3	4	5	6
i=4	4	8	12	16	20	24
	↓	↓	↓	↓	↓	↓
	4	1	5	2	6	3



To prove formally.

Proof by contradiction assume T is not equiv S mod p.

Then since no item in T is $\equiv 0 \pmod p$ we must have 2 items equiv to each other mod p:

$\{a, 2a, 3a, \ldots a(p-1)\}$

$ai \equiv aj \pmod p$ $\quad 0 \le i, j < p$, $i \neq j$, $p > i > j \ge 0$

$ai - aj \equiv 0 \pmod p$

$a(i-j) \equiv 0 \pmod p$

$\Rightarrow p \mid (a(i-j))$

$\Rightarrow$ ~~$p \mid a$~~ or ~~$p \mid (i-j)$~~

Since $\gcd(p,a)=1$

$1 \le i-j \le p-1$

this contradicts $p \mid (i-j)$ so this is also not possible

> $a \mid b$ - "b is divisible by a", there exists an integer c such that $b = ac$.

Sets S, T equivalent mod P:

$$\prod_{i=1}^{p-1} a \cdot i \equiv \prod_{i=1}^{p-1} i \pmod p$$

$\prod_{i=1}^{p-1} a \cdot i$: product of everything in T

$\prod_{i=1}^{p-1} i$: product everything in S

$$a^{p-1} \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} i \pmod{p}$$

$$a^{p-1} \prod_{i=1}^{p-1} i - \prod_{i=1}^{p-1} i \equiv 0 \pmod{p}$$

$$\prod_{i=1}^{p-1} i \left(a^{p-1} - 1\right) \equiv 0 \pmod{p}$$

$$(p-1)! \left(a^{p-1} - 1\right) \equiv 0 \pmod{p}$$

$$\Longrightarrow p \mid \left((p-1)! \left(a^{p-1} - 1\right)\right)$$

$$\Longrightarrow p \nmid (p-1)! \quad \text{or} \quad p \mid \left(a^{p-1} - 1\right)$$

No p doesn't divide evenly into any of the terms

must be true!

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

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

for each integer base from 1 to $p-1$, the cycle length of the mod exp divides evenly into $p-1$.

4^0 4^1 4^2 4^3 4^4 4^5 4^6 4^7

1 4 2 | 1 4 2 | 1 4

3^0 3^1 3^2 3^3 3^4 3^5 3^6 3^7

1 3 2 6 4 5 | 1

→ Since 3 cycles through all non-zero remainders, we call it a generator or primitive roots.

How do I test this?

Calculate $49^{302} \mod 101$

What is the remainder when 49^{302} is divided by 101?

101 is prime, $\gcd(49,101)=1$, thus by Fermat's Thm, $49^{100} \equiv 1 \mod 101$

$$49^{302} = 49^{300} \times 49^2$$
$$= (49^{100})^3 \times (2401)$$
$$\equiv 1^3 \times 78 \mod 101$$
$$\equiv \boxed{78} \mod 101.$$

$$\begin{array}{r} 23 \text{ R } 78 \\ 101 \overline{)\,2401} \\ 202 \\ \hline 381 \\ -303 \\ \hline 78 \end{array}$$

---

for some n, if $\gcd(a,n)=1$ and $a^{n-1} \not\equiv 1 \pmod n$, I have proof n is composite.

Note: if $a^{n-1} \equiv 1 \pmod n$ that doesn't prove n is prime.

Miller-Rabin Primality Test