Number Theory

Wednesday, January 21, 2026 6:57 PM

Recall: Divisibility by 3 and 9

1] Divisibility by 11

$5386 = 5\times10^3 + 3\times10^2 + 8\times10 + 6 \pmod{11}$

$\equiv 5(-1)^3 + 3(-1)^2 + 8(-1) + 6$

$\equiv -5 + 3 - 8 + 6$

$\equiv -4$

$\equiv 7 \pmod{11}$

Alternate +/− R to L

e.g. 53145376 (− + − + from right to left)

$\equiv 1$

e.g. 15335244

2] Divisibility by 7:

$5314762 = 5\times10^6 + 3\times10^5 + 1\times10^4 + 4\times10^3 + 7\times10^2 + 6\times10 + 2$

$\equiv 1 \quad -2 \quad -3 \quad -1 \quad 2 \quad 3 \quad 1 \pmod 7$

$-2 + 1 - 3 - 4 + 0 - 3 + 2$

$\equiv -2 \equiv 5 \pmod 7$

5314762 (− − +)

1587587

9

3] Primes :

See P02

4] Thrm: The Fundamental Theorem of Arithmetic (FAT)

Every $n > 1$ is either prime or can be represented uniquely as a product of primes.

e.g. $n = 100 = 2^2 \cdot 5^2$

5] Thrm : there are infinitly many primes

Proof:

Suppose we have a finite number of primes,

$$p_1, p_2, p_3, \ldots, p_n$$

let $q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$

then $p_i \nmid q$ for all $i = 1 \ldots n$

$\therefore q$ is a prime by the FTA.

6] Thrm: Number of primes

Let $\pi(x)$ = number of primes $\leq x$

then $\pi(x) \cong \frac{x}{\ln x}$

i.e $\frac{x}{\ln x} < \pi(x) < \frac{x}{\ln x - 1.084}$

by Gauss

by Lagrange

7] Thm: the multiplicative inverse a^{-1} exists in $\mathbb{Z}_n$ if and only if $\gcd(n, a) = 1$

8] To find $a^{-1} \pmod n$

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

by EEA, we can write $1 = s \cdot n + t \cdot a$

$\Rightarrow 1 \equiv 0 + t \cdot a \pmod n$

$\therefore a^{-1} \equiv t \pmod n$

9] Exer.

Find $13^{-1} \pmod{54}$

Soln:

$54 = 4 \cdot 13 + 2$

$13 = 6 \cdot 2 + 1$ ← gcd

$2 = 2 \cdot 1 + 0$

$\Rightarrow 1 = 13 - 6 \cdot 2$

$= 13 - 6(54 - 4 \cdot 13)$

$= -6 \cdot 54 + 25 \cdot 13$

$\therefore 1 = \underbrace{-6}_{s} \cdot 54 + \underbrace{25}_{t} \cdot 13$

$\Rightarrow 1 \equiv 0 + 25 \cdot 13 \pmod{54}$

$\therefore 13^{-1} \equiv 25 \pmod{54}$