10/5/25 : Cryptography & Sybere law

Prime numbers and their summery:

Definition: P is called prime number if and only if the is divisible by only 1 and p ownself.

Theorem of Arithmatic:

Definition:

$$100 = 2 \cdot 5 \cdot 5 \cdot 2$$

The Seive of Eratosthenes can be used to find all primes

Mersenne prime: form $2^p - 1$; palso prime like $p = 3$: $2^3 - 1 =$ ⊗ ∇ also prime.

Still now, there is no generalize eqn to find prime numbers.

How many primes numbers can be possible in a given triangle?

$f(n) = n^2 - n + 41$ given prime numbers where $n \leq 40$.

Actually what we need:

Goldbach's Conjecture:

The twin prime : differ 2 like 5, 7 and 11, 13

GCD:

if GCD 1 then those are relatively prime like 10, 17

Finding GCD using Prime factorization:

Least Common multiple (LCM):

Euclidean Algorithm:
GCD as a linear Combination:

Bezout's Theorem: $gcd(a,b) = sa+tb$ — Proof

using

linear Congruence: $ax \equiv b \pmod{m}$

Finding Inverse:

HW: Find an inverse of 101 modulo 9720
201 modulo 9720

exam ☆☆ Chinese Remainder Theorem: when devided by 3 r is 2, when 5, r is 3 when 7, r is 2 ; translated as congruence — Proof

$x \equiv 2 \pmod 3$,
$x \equiv 3 \pmod 5$,
$x \equiv 2 \pmod 7$

$x = a_n \pmod{m_n}$

Proof

exam ☆ Fermat's Little Theorem:

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

HW $x^{222} \bmod 11$