Quiz 10

Last time Fermats "little theorem" 🤔

If p is a prime number, then $p \mid a^p - a$ for every positive int of a

ex what is the ~~number~~ remainder of 3^{50} after division by 7

P=7 so $7 \mid a^7 - a$, for all a, take $a = 3^7$: $7 \mid (3^7)^7 - 3^7 = 3^{49} \cdot 3^7$

$a = 3$, $7 \mid 3^7 - 3$

$\rightarrow 7 \mid 3^{49} - 3 \rightarrow 7 \mid 3(3^{49} - 3) = 3^{50} - 2$ Sometimes wrong steps

$\rightarrow 7 \mid 3^{50} - 2$ remainder is 2

Lemma If p is a prime, then $p \mid \binom{p}{k}$ for all $k = 1, \dots p-1$

Proof:: $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ $\xrightarrow{\text{simply top/bottom}}$ $\frac{(p-k+1)(\cdots)(p-1)(p)}{k!}$

$\Rightarrow k! \binom{p}{k} = p(p-1) \cdots (p-k+1)$

$\Rightarrow$ that is $p \mid k! \binom{p}{k}$

According to euclid theorem $p \mid k!$ or $p \mid \binom{p}{k}$

let's say $p \mid k!$ meaning $p \mid k! = 1 \cdot 2 \cdots k$

but $k < p$ or $p \mid j$ for some $1 \le j \le k < p$

hence contradiction

So $p \mid \binom{p}{k}$

Proof (FLT) Induction on a

→ Base Case:: $a = 1$ true since $p \mid 1^p - 1 = 0$

→ Induction Step:: $p \mid (a+1)^p - (a+1)$

• expand Binomially $(a+1)^p - (a+1)$

↳ $a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1 - a - 1$

$a^p - a$: div by p, induction hyp

$\binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$: By Lemma

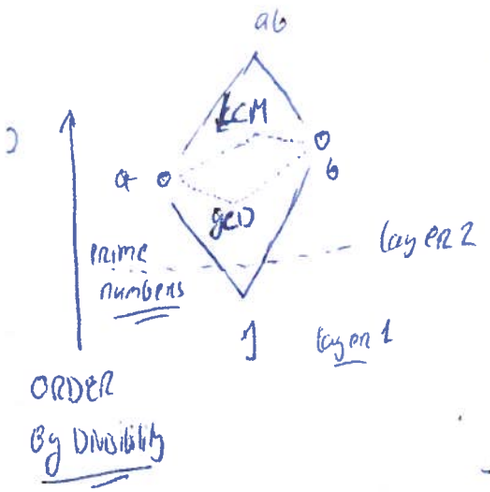
hence Induction proven □

Greatest Common divisors & Least common Multiples

GCD ab : positive INTegers

LCM gcd (a,b) = gCDivisor of a,b

LCM (a,b)



Relatively Prime

If a & b have a gCD = 1, they are known as relatively prime.

ex ~~if 6 & 8~~ using ab that are Distinct prime numbs, so they also relatively primes

⟷

Exs: gCD(6,8) : 2
LCM (6,8) : 24

} see that 6·8 = 2·24 hence you can see LCM is derived from GCD

Convention gCD (a,0) = a for a ≥ 0

LCM (a,0) = 0

⟷

Proposition ① if a|b then gcd (a,b) = a

② gCD(a, b) = gCD (a, b-a) assuming b > a else gcd (a-b, b)

Example of R.P (8,25) both not prime, but gCD (8,25) = 1

Lets take a large numbers gCD(240, 420)

using lemma ② = gCD (240, 420 - 240) (420 - 240 = 180)

↳ gCD (240 - 180, 180) (240 - 180 = 60)

↳ gCD (60, 180) = 60

} Basis of EuclD alg will do detail later

Proof of Proposition:- d = gCD(a,b)

① a|b, a|a } ⇒ a is common divisor then a ≤ d } → a = d

② ↳ also d|a ⇒ d ≤ a }

if x|16, x|4 then x ≤ d but if z|4 in d ≤ a

ⅱ) $d_1 = gCD(a,b)$ $d_2 = gCD(a, b-a)$

$\begin{cases} d_1 | a \\ d_1 | b \end{cases} \Rightarrow \begin{cases} d_1 | a \\ d_1 | b-a \end{cases} \rightarrow d_1 \le d_1$

$\begin{cases} d_2 | a \\ d_2 | b-a \end{cases} \Rightarrow \begin{cases} d_2 | a \\ d_2 | b \end{cases} \rightarrow d_2 \le d_1$

} $d_1 = d_2$

Finding GCD :: Given a, b : positive integer

[1 Prime fact
2 Euclid]

① Via Prim factorizations

$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$

$b = q_1^{\beta_1} \cdots q_m^{\beta_m}$

$p_1 \cdots p_n$ } Distinct prime

$q_1 \cdots q_m$ } Distinct Integers

$\alpha_1 \cdots \alpha_k$

$\beta_1 \cdots \beta_k$

$gCD(a,b) = R_1^{\phi_1} \cdots R_L^{\phi_L}$ } ex max $2^2 3^2$ is a gCD

random ex

$24 = 2^3 \cdot 3$

$42 = 2 \cdot 3 \cdot 7$

$gcd = 2 \cdot 3$

→ $R_1 \cdots R_L$ common prime

→ ϕ_j $(j = 1 \cdots L)$ smaller of the exponents of R_j in both a & b

---

Variation $gCD(24, 12345000)$

easy known Prime factor

hard unknown prime factorize

[JUST ONE Explicit Factorization]

Check 12345000 : Divisible by 3 ✓

Divisible by 2 ✓

" " 4 ✓

" " 8 ✗

So $gCD = 12$

Variation 2 (Joint prime factorization)

account for primes that show in a but not b by 0 representation in pow

$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$

$b = p_1^{\beta_1} \cdots p_n^{\beta_n}$

$p_1 \cdots p_n$ distinct primes dividing a or b

$\alpha_1 \cdots \alpha_n \geq 0$

$\beta_1 \cdots \beta_n \geq 0$

} → $24 = 2^3 \cdot 3 \cdot 7^0$

$42 = 2 \cdot 3 \cdot 7$

So $gCD(a,b) = p_1^{\text{Power}(\min\{\alpha,\beta\})} \cdots p_n^{\text{Power}(\min\{\alpha,\beta\})}$

Bonus $LCM(a,b) = p_1^{\text{Power}(\max\{\alpha,\beta\})} \cdots p_n^{\text{Power}(\max\{\alpha,\beta\})}$

---

② VIA Euclid

$gcd_{(a,b)}$ Given (a,b) Say $a > b$

$a = bq_1 + R_1 \quad 0 \leq R_1 < b$ } R = remainder

$gcd_{(a,R_1)}$

$gcd(b, R_2)$: $b = R_2 q_2 + R_2$

$gcd_{(R_{n-1}, R_n)}$ $R_{n-1} = R_n q_{n+1} + R_{n+1}$ } when $R_{n+1} = 0$ STOP

When you hit zero $gCD(r_{n-1}, r_n)$ then answer $= r_n$

Remarks : { The alg stops in finitely many steps since $b > r_1 > r_2 > \cdots > r_n$ [logarithmically in b] }

Ex $a = F_{n+1}$ $b = F_n$

① $F_{n+1} = F_n + F_{n-1}$ $\quad gcd(F_{n+1}, F_n)$

② $F_n = F_{n-1} + F_{n-2}$ $\quad gcd(F_n, F_{n-1})$

⋮ ⋮

(n) $F_2 = F_1 + 0$ $\quad gcd(F_2, F_1) = 1$

Invertibility & equivalence Class