Discrete tutorial

1. $\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b$.
2. $n \bmod 9 \equiv \{\text{sum of digits}\} \bmod 9$.
3. $k \mid a,b \Rightarrow \gcd(a,b) = k \gcd\left(\frac{a}{k}, \frac{b}{k}\right)$.
4. Find $x, y \in \mathbb{Z}$ s.t. $77x + 52y = 1$ — 2 steps
5. Show $\exists$ arbitrarily large pairs of numbers whose Euclidean Algorithm terminates in

(1) $$\gcd(a,b) = p_1^{\min(a_1,b_1)} * p_2^{\min(a_2,b_2)} * \dots * p_n^{\min(a_n,b_n)}$$
$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} * p_2^{\max(a_2,b_2)} * \dots * p_n^{\max(a_n,b_n)}$$
$$\therefore \text{lcm}(a,b)\gcd(a,b) = p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} + \dots + p_n^{a_n+b_n} = a \cdot b. \blacksquare$$

(2) Let $N \in \mathbb{N}$, $N = 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10^1 a_1 + a_0$. (where $a_0, a_1 \dots a_k$ = digits)
$$N = 10^k a_k - a_k + 10^{k-1} a_{k-1} - a_{k-1} + \dots + 10^1 a_1 - a_1 + a_0 - a_0 + (a_0 + a_1 + \dots + a_k)$$
$$= a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \dots + a_1(10-1) + \sum_{i=0}^{k} a_i$$

(3) $k \mid a, b$

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} = p_1^{a_1+k_1} p_2^{a_2+k_2} \dots p_n^{a_n+k_n}$$
$$b = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} = \text{"}$$
$$\gcd(a,b) = p_1^{\min(a_1+k_1,\, b_1+k_1)} p_2^{\min(a_2+k_2,\, b_2+k_2)} \dots p_n^{\min(a_n+k_n,\, b_n+k_n)}$$

e.g. $\min(a+3, b+3) = \min(a,b)$.

$$\gcd(a,b) = \left(p_1^{\min(a_1,b_1)} \cdot p_1^{k_1}\right) \cdot \left(p_2^{\min(a_2,b_2)} \cdot p_2^{k_2}\right) \dots \left(p_n^{\min(a_n,b_n)} \cdot p_n^{k_n}\right)$$

$= k \cdot \gcd\left(\frac{a}{k}, \frac{b}{k}\right)$. — exponents of primes in k.

In this case, $\min(a_1, b_1) = a_1, b_1$ here are $= k$.

(4) $77 = 52 \cdot 1 + 25$ — $25 = 77 - 52 \cdot 1$ — a/k, b/k.

$52 = 25 \cdot 2 + 2$ — $2 = 52 - 25 \cdot 2$

$25 = 2 \cdot 12 + 1$ — $1 = 25 - 12 \cdot 2$

$1 = 25 - 12(52 - 25 \cdot 2)$.

$1 = 25 - 12(52 - (77 - 52) \cdot 2)$.

$= 77 - 52 - 12 \times 52 - 24 \times (77 - 52)$.

$= 77 - 52 - 12 \times 52 - 24 \times 77 + 24 \times 52$.

$= -23 \times 77 + 11 \times 52$ ✗

= whatever blah blah ...

$= +25 \times 77 - 13 \times 52$.

Discrete : Tutorial

① Show $\mathbb{Z}/n\mathbb{Z}$ field $\Rightarrow$ n prime. $(\forall a \exists x : a = \frac{1}{x})$

② Show: prod of invertible elements in $\mathbb{Z}/n\mathbb{Z}$ is also invertible.

③ $100\hat{}100\hat{}100\hat{}1000 \bmod 7 = ?$

④ p prime, $1 \leq a \leq p-1$, show $[a], [2a], \ldots, [(p-1)a]$ are distinct residue classes.

⑤ Prove Fermat by considering $a(2a)(3a)\ldots(p-1)a$

⑥ $19^{101^{1000}} \bmod 20 = ?$

⑦ $\forall n \in \mathbb{N}$, def. $A_n = \{m \mid 1 \leq m \leq n, (m,n) = 1\}$ $(m,n) = \gcd(m,n)$..

$\varphi(n) := A_n$ is the Euler totient function.

Show $((m,n) = 1) \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$.

⑦ Show for p prime, $\varphi(p^k) = p^k(1 - \frac{1}{p})$

① $[a] \in \mathbb{Z}/n\mathbb{Z}$ invertible $\Leftrightarrow$ $(a,n) = 1$.

$n = ab$, $\Rightarrow (a,n) = a \Rightarrow [a] \notin \mathbb{Z}/n\mathbb{Z}$ not invertible.

② $[a][x_a] = [1] \Rightarrow [ax_a] = [1]$.

Consider $[a_1], [a_2], \ldots, [a_n] = [a_1 a_2 \ldots a_n]$ } multiply

$[x_{a_1}], [x_{a_2}], \ldots, [x_{a_n}] = [x_{a_1} x_{a_2} \ldots x_{a_n}]$ }

$[x_{a_1} a_1 x_{a_2} a_2 x_{a_3} a_3 \ldots x_{a_n} a_n] = [x_{a_1} a_1][x_{a_2} a_2] \cdots [x_{a_n} a_n]$

$= 1 \cdot 1 \cdot \ldots \cdot 1 = 1$

Note: $a a^{-1} = 1 \wedge b b^{-1} = 1$, $\Rightarrow a b a^{-1} b^{-1} = 1 \Rightarrow (aa^{-1})(bb^{-1}) = 1$ OK.

③ $10^{100^{100^{1000}}} \bmod 7$.

$10 \bmod 7 = 3 \bmod 7$. $p \not\mid 7 \rightarrow$ prime. So, Fermat applic.

$a^{p-1} \equiv 1 \bmod p$, $a^p \equiv a \bmod p$.

$3^{100^{100^{1000}}} \equiv 3^{4^{100^{1000}}} \bmod 7 \equiv 4^{100^{1000}} \bmod 7 \equiv 4^{4^{1000}} \bmod 7 \equiv 4^{1000} \bmod 7$

$\equiv 4^4 \bmod 7 \equiv 4 \bmod 7$.

④ basically need to show that $[na] \neq [ma]$ when $n \neq m$, $1 \leq n$, $m \leq p-1$.

Suppose $[na] = [ma]$

$[na] - [ma] = [na - ma] = [0] \bmod p$. This means $p \mid na - ma$

$= p \mid (n-m)a$.

So $p \mid a \vee p \mid n-m$. but a, n, m less than p (by construction).

⑤ Notice: Every $a \not\equiv 0 \bmod p$ is invertible (because it's coprime to p).

$[a^{r_1}][2a^{r_2}][3a^{r_3}] \dots [(p-1)a^{r_{p-1}}]$

Basically, somewhere in this residue contains r_1 and r_1^{-1},

r_2 and r_2^{-1}

↳ Can pair off all possible residues, ~~a~~.

$[1][1] \dots [1] \equiv 1 \bmod p$.

↳ $a^{p-1}\underbrace{(p-1)!} \equiv 1 \bmod p \Rightarrow a^{p-1} \equiv 1 \bmod p$.

all the a's get grouped together → ↳ product of all residues, multiplies to 1.

odd power, -1

→ even power, 1.

⑥ $19^{101^{1000}} \bmod 20 \equiv (-1)^{101^{1000}} \bmod 20 \equiv 1 \bmod 20$

⑦ $\varphi(m)$ = number of things coprime to m.

$\varphi(mn) = \varphi(m)\varphi(n)$.

$|A_{mn}| \longrightarrow |A_m||A_n|$. Set up a bijection. exercise.

↳ $A_{mn} \longrightarrow A_m \times A_n$

$ab. \longleftarrow (a,b)$ ok. injective. show surjective

⑧ $\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.

Elements from 1 to p^k which are not coprime to p^k.

$p, 2p, 3p, \dots, p^{k-1}p$.

$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$ ∎

Congruences "The same w/o being equal". Almost equality → equi relation.

fix $n > 0$ integer.

$a \equiv b \bmod n$ → a and b have the same remainder upon division by n.

i.e. $n \mid a - b$ → makes sense.

Equivalence relation : ① Reflexive : $a \equiv a \bmod n$. a has same remainder as a.

(Try to prove this) ② Sym : $a \equiv b \bmod n \iff b \equiv a \bmod n$.

③ Trans : $a \equiv b \bmod n$, $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$.

→ Congruence mod n is an equivalence relation on $\mathbb{Z}$.

Rules : (arith). $a \equiv b \bmod n \wedge a' \equiv b' \bmod n \Rightarrow a \pm a' \equiv b \pm b' \bmod n$

$\Rightarrow aa' \equiv bb' \bmod n$

Discrete : Tutorial.

① $(a, b) = 1$, $\Rightarrow b \mid a^{\varphi(b)} - 1$.

② $x \equiv 1 \bmod 3$, $\equiv 4 \bmod 5 \equiv 6 \bmod 7$.

Prove ① : Suppose $\varphi(b) = k$. List coprime elements :

$s_1, s_2, \dots, s_k$.

Consider the b residues of the $(as_1), (as_2) \dots (as_i)$

Soit $r_i \equiv as_i \bmod b$. $\gcd(b, r_i) = 1$ ← montrer que.

Supposons $\exists p$ primaire, $p \mid r_i \wedge p \mid b$.

$as_i = k(b) + r_i$ ↘ $\Rightarrow p \mid as_i$. $\gcd(as_i, b) = 1$. ⇒ contradiction.

Donc, $\gcd(b, r_i) = 1$.

Supposons $r_i \equiv r_j \bmod b$, $i \neq j$. Donc, $b \mid as_i - as_j$ Normal! $as_i \bmod b \equiv as_j \bmod b$.

$\Rightarrow b \mid as_i - as_j \Rightarrow b \mid s_i - s_j$ contradiction

Donc, r_i sont des permutations de s_i. $(as_1, as_2 \dots as_k)$ ↘

Soit : $as_1\, as_2 \dots as_k = a^k(s_1 s_2 \dots s_k) \equiv (r_1 \dots r_k) \equiv s_1 \dots s_k$.

$0 \equiv a^k(s_1 \dots s_k) - (s_1 \dots s_k) \bmod b$

$0 \equiv (a^k - 1)(s_1 \dots s_k) \bmod b$.

Donc, $b \mid (a^k - 1)(s_i \dots s_k)$ Mais $\gcd(s_i, b) = 1$.

donc, $b \mid a^k - 1$, $k = \varphi(b)$. ∎

① $\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 5 \\ x \equiv 6 \bmod 7 \end{cases} \Rightarrow x = 7j + 6$.

$x \equiv 4 \bmod 5 \Rightarrow 7j + 6 \equiv 4 \bmod 5$.

$7j \equiv 3 \bmod 5$.

$2j \equiv -2 \bmod 5$

$j \equiv -6 \bmod 5$, $j \equiv 4 \bmod 5$, $j = 5k + 4$

$x = 7(5k+4) + 6 = 35k + 34$. $\Rightarrow 35k + 34 \equiv 1 \bmod 3$.

$35k + 1 \equiv 1 \bmod 3$, $35k \equiv 0 \bmod 3$. $\equiv 2k \equiv 0 \bmod 3$.

$k \equiv 0 \bmod 3$, $k = 3 \cdot l + 0$.

$x = 35 \cdot (3l) + 34 = 105l + 34$ $\quad x \equiv 34 \bmod 105$

③ Solve ① $12x + 31y \equiv 2 \bmod 127$

② $2x + 89y \equiv 23 \bmod 127$

① $- 6 \times$ ② $\rightarrow -503y \equiv -136 \bmod 127$.

$5y \equiv 118 \bmod 127$.

Euclidean Alg: $1 = -2 \cdot 127 + 51 \cdot 5$. 51 inverse de 5.

$\rightarrow \bmod 127$: $\rightarrow 1 \equiv 51 \cdot 5 \bmod 127$.

$5 \cdot 5\, y \equiv 51 \cdot 118 \bmod 127$.

$y \equiv 49 \bmod 127$.

② $2x \equiv 23 - 89y \bmod 127 \Rightarrow 2x \equiv 23 - 89(49) \bmod 127$.

$2x \equiv 107 \bmod 127$.

Need to find linear sum of 2 and 127: (Eucl. Alg).

$1 = 127 - 63 \cdot 2$. $\bmod 127$

$1 \equiv -63 \cdot 2 \bmod 127$. $\quad 1 \equiv 2 \cdot 64 \bmod 127$

$64 \cdot 2x \equiv 64 \cdot 107 \bmod 127$.

$x \equiv 117 \bmod 127$.