Viet

Discrete : Good Stuff.

Recall: • $a \equiv b \bmod n$ if $n \mid a-b$.

• congruence mod n is an equivalence relation on $\mathbb{Z}$.

• arith rules: $\left.\begin{array}{l} a \equiv b \bmod n \\ a' \equiv b' \bmod n \end{array}\right\} \Rightarrow \begin{cases} a \pm a' \equiv b \pm b' \bmod n \\ aa' \equiv bb' \bmod n \end{cases}$

In part. $a \equiv b \bmod n \Rightarrow a^k \equiv b^k \bmod n \wedge ka \equiv kb \bmod n$.

Example: Let $\overline{d_1 d_2 \ldots d_n} = N$, $d_1 \ldots d_n$ are digits.

mod 2: $N = \underbrace{10^{n-1}}_{0 \bmod 2} d_1 + \underbrace{10^{n-2}}_{0 \bmod 2} d_2 + \ldots + 10 d_{n-1} + \underbrace{d_n}_{?} \equiv d_n \bmod 2$. //same for mod 5

mod 3: $N = 10^{n-1} d_1 + 10^{n-2} d_2 + \ldots + 10 d_{n-1} + d_n \equiv d_1 + d_2 + \ldots + d_{n-1} + d_n \bmod 3$.

$(10 \equiv 1 \bmod 3) \Rightarrow (10^k \equiv 1^k \bmod 3)$

mod 9: same

mod 11: $N = \underbrace{10^{n-1}}_{\text{etc}} d_1 + \underbrace{10^{n-2}}_{\equiv 1 \bmod 11} d_2 + \ldots + \underbrace{10}_{\equiv -1 \bmod 11} d_{n-1} + d_n$

$(10 \equiv -1 \bmod n) \Rightarrow 10^k \equiv (-1)^k \bmod n$

$N \equiv \ldots + d_{n-2} - d_{n-1} + d_n \bmod 11$ — if even length, start w/ $\ominus$. odd, → start w/ $\oplus$

Ex: $100^{100} \bmod 7$? reductions address base and/or exponent.

(base) $100 \equiv 2 \bmod 7 \Rightarrow 100^{100} \equiv 2^{100} \bmod 7$

$2^{100} = 2^{10^{10}} \Rightarrow 2^{10} \equiv 1024 \bmod 7 = 2 \bmod 7$

$(2^{10})^{10} \equiv 2^{10} \bmod 7 \equiv 2 \bmod 7$.

usually works w/ prime mod (exponent) — recall Fermat's little theorem. $a^p \equiv a \bmod p$

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

$a^7 \equiv a \bmod 7 \quad \forall a \in \mathbb{Z}$

$a^6 \equiv 1 \bmod 7 \quad \forall a \in \mathbb{Z}: \gcd(a,7) = 1$

$100^{100} = 100^{6(\ldots)+r}$ $\gcd(100,7) = 1$ ok.

$\Rightarrow 100^{6(\ldots)+4} \equiv 100^4 \bmod 7 \equiv 2^4 \bmod 7 \equiv 2 \bmod 7$.

$\boxed{\mathbb{Z}/n\mathbb{Z}}$ Again.. congruence mod n, $n \in \mathbb{Z}^+$, is an equivalence relation on $\mathbb{Z}$

$\Rightarrow$ equivalence classes.

$[a] = \{c \in \mathbb{Z} : c \equiv a \bmod n\}$ All c that are congruent to $a \bmod n$.

$[0] = \{0, n, 2n, -n, -2n \ldots\}$ $= [n]$ (2 equi classes the same when representatives are the same!)

$[1] = \{1, n+1, 2n+1, -n+1, -2n+1 \ldots\}$

⚠ $[1] = [1-n]$

proof ② $\quad a|c \Rightarrow c = ac' \qquad ab \mid aq_1, bq_2 \quad$ ~~$1 = ax + by$.~~

$b|c \Rightarrow b|c = ac' \qquad ab|c^2$. ~~$aq_1 = bq_2$~~

$\gcd(a,b) = 1 \qquad b|c' \Rightarrow ab|ac' = c$ ■ $\qquad$ ~~$0 = aq_1 - bq_2$~~

$\hookrightarrow$ because $b \nmid a \wedge b|ac'$

Theorem: $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = a \cdot b$. $\quad \rightarrow$ no more common parts between a, b.

proof: $d = \gcd(a,b)$. $\quad d|a \Rightarrow a = da'$

$d|b \Rightarrow b = db'$ $\Big\}$ $\gcd(a', b') = 1$

(If $k = \gcd(a', b') > 1$, then,

$k|a' \Rightarrow kd|a'd = a$

$k|b' \Rightarrow kd|b'd = b$.

so kd greater than gcd ↯)

Now, show $\mathrm{lcm}(a,b) = da'b'$

(then $\gcd \cdot \mathrm{lcm} = d \cdot da'b' = ab$)

$da'b'$ is a common multiple of a and b.

~~$(a|da'b' \Rightarrow a|ab') \wedge (b|da'b' \Rightarrow b|ba')$~~

~~If m = common multiple of a and b, then $da'b'|m$.~~

~~(any other common multiple $> da'b'$)~~

~~$ab'|m \wedge a'b|m. \Rightarrow ab'a'b|m$~~

~~$dab' \times a'db'|m. \Rightarrow da'b'ab|m\,ab$~~

~~$\hookrightarrow da'b'|m$.~~

NOT VALID!

Bud's proof: $\left.\begin{matrix} a|m \\ d|a \end{matrix}\right\}$ $d|m \Rightarrow m = m'd$.

$a = da' \mid m = dm' \Rightarrow a'|m'$ $\Big\}$ $\Rightarrow$ $a'b'|m'$ $\quad$ relatively prime.

Same for b: $\Rightarrow b'|m'$

$\Rightarrow da'b'|m'd \Rightarrow da'b'|m$. ■

recall $\quad$ given a, b, $\rightarrow$ prime factorizations, "joint".

$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $\quad \alpha_1 \ldots \alpha_k \geq 0$

$b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ $\quad \beta_1 \ldots \beta_k \geq 0$

$\Rightarrow \gcd(a,b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$

$\mathrm{lcm}(a,b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$

$\gcd(a,b) \cdot \mathrm{lcm}(a,b) =$

$$\boxed{\prod p_k^{\min(\alpha_k, \beta_k)} \cdot \prod p_k^{\max(\alpha_k, \beta_k)} = \prod p_k^{\alpha_k + \beta_k}}$$

Discrete Cont'.

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

for $n > 0$ 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: $a \equiv b \bmod n \Leftrightarrow b \equiv a \bmod n$.

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). $a \equiv b \bmod n \wedge a' \equiv b' \bmod n \Rightarrow a \pm a' \equiv b \pm b' \bmod n$

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