① $3x^2 - y! = 2022$

mod 2 : $3x^2$ can be $\boxed{0}$ or 1

$y!$ will be $\boxed{0}$ when $y \geqslant 2$

2022 is $\boxed{0}$ ×

mod 3

$3x^2$ is 0

$y!$ is 0 when $y \geqslant 3$

202 is 0 ×

mod 4 $3x^2$ can be 0 or 3

$3 \cdot 0^2 \equiv 0$, $3 \cdot 1^2 \equiv 3$, $3 \cdot 2^2 \equiv 0$, $3 \cdot 3^2 \equiv 3$

$y!$ is 0 when $y \geqslant 4$

2022 is 2

$0 - 0 \not\equiv 2$

$3 - 0 \not\equiv 2$

no solution

Try $y = 1, 2, 3$

$3x^2 = y! + 2022$

$= 2023, 2024, 2028$

$x^2 = \frac{2023}{3}, \frac{2024}{3}, \frac{2028}{3}$

$\frac{2023}{3} \to \notin \mathbb{Z}$, $\frac{2024}{3} \to \notin \mathbb{Z}$, $\frac{2028}{3} \to 676$

$x = 26$ $\quad \boxed{(26, 3)}$

Alternatively, mod 9 works as well.

---

(2) (a) $ax \equiv c \pmod{m}$ no sol. or

(m, a) sol. in $\mathbb{Z}_m$

(b) $ax + by \equiv c \pmod{m}$ no sol.

or $m \cdot (m, a, b)$ sol. $0 \leq x, y \leq m-1$.

(a) From the lectures :

- no sol. if $(m,a) \nmid c$ ✓

→ • unique sol. mod $\frac{m}{(m,a)}$ if $(m,a) \mid c$.

If we say $t \bmod \frac{m}{(m,a)}$ is the

unique solution.

In $\mathbb{Z}_m$, this corresponds to

$$t,\ t+\frac{m}{(m,a)},\ t+2\cdot\frac{m}{(m,a)},\ \dots,\ t+\left((m,a)-1\right)\cdot\frac{m}{(m,a)}$$

$\Rightarrow$ There are (m,a) sol. in $\mathbb{Z}_m$.

(b) $ax+by \equiv c \pmod m$

Fix a y

- $ax \equiv c-by \pmod m$ has no

sol. in $\mathbb{Z}_m$ or $\boxed{(m,a) \text{ sol. in } \mathbb{Z}_m}$.

for how many fixed values of y, this is the case?

$ax \equiv c - by \pmod{m}$ has sol.

when $(m,a) \mid c - by$, i.e.

$by \equiv c \pmod{(m,a)}$.

- This has $((m,a), b)$ solutions y in $\mathbb{Z}_{(m,a)}$.

- When we lift these solutions to $\mathbb{Z}_m$, there will be

$\boxed{((m,a), b) \cdot \dfrac{m}{(m,a)} \text{ solutions } y.}$

$\Rightarrow \# \text{ sol.} = ((m,a), b) \cdot \dfrac{m}{(m,a)} \cdot (m,a)$

$$= \big((m,a),\ b\big)\cdot m$$

$$\parallel$$

$$= (m,a,b)\cdot m$$

③ $s_i = \dfrac{i^2+i}{2}$

(a) $m = 2^n$, then $\{s_0, s_1, \dots, s_{m-1}\}$ is CSR mod m

Observation: $\{s_0, s_1, \dots, s_{m-1}\}$ is a CSR mod m if and only they are all distinct mod m.

WTS: $s_i \not\equiv s_j \pmod m$ when $i \neq j$

Assume $i \neq j$ and $s_i \equiv s_j \pmod m$

$\Rightarrow s_i - s_j \equiv 0 \pmod m \Rightarrow m \mid s_i - s_j$.

$$s_i - s_j = \frac{i^2 + i - j^2 - j}{2} = \frac{(i-j)(i+j+1)}{2}$$

$\Rightarrow \quad 2^n \;\Big|\; \dfrac{(i-j)(i+j+1)}{2}$

$\Rightarrow \quad 2^{n+1} \;\big|\; (i-j)(i+j+1)$

both of them
cannot be even

$\Rightarrow \quad 2^{n+1} \mid i-j \quad$ or $\quad 2^{n+1} \mid i+j+1$

$0 \leq i, j \leq 2^n - 1 \qquad 1 \leq i+j+1 \leq 2^{n+1}-1$ $\times$

$-(2^n-1) \leq i-j \leq 2^n - 1$

$\Downarrow$

$i-j=0 \Rightarrow i=j$, $\quad \cancel{\quad}$

(b) $m = k \cdot 2^n \qquad k \geqslant 3$ odd.

At least 2^{n+1} of $s_0, s_1, \ldots, s_{m-1}$
are divisible by k

$\{s_0, s_1, \ldots, s_{m-1}\}$ is not CSR.

$k \mid s_i \qquad k \mid \frac{i^2+i}{2}$

$k \mid i^2 + i = i(i+1)$

$i \equiv 0, -1 \pmod{k} \Rightarrow k \mid s_i$

$s_0, \; s_{k-1}, s_k, \; s_{2k-1}, s_{2k}, \; s_{3k-1}, s_{3k}$

$\ldots \; s_{(2^n-1)\cdot k-1}, \; s_{(2^n-1)k}, \; s_{2^n k-1}$

$\Downarrow$

at least 2^{n+1} s_i divisible by k.

In mod $m = 2^n \cdot k$, which congruence classes are divisible by k

$$\underbrace{k, 2k, 3k, \ldots, 2^n \cdot k}_{2^n \text{ of them}}$$

2^{n+1} s_i should correspond to these 2^n congruence classes

$\Rightarrow s_i \equiv s_j$ for some i, j.

4

$x \equiv 15 \pmod{16}$

$x \equiv 16 \pmod{17}$

$3x \equiv 3 \pmod{18}$

$\downarrow$

$x \equiv 1 \pmod{6}$

$x \equiv 1 \pmod{2}$ $\quad$ $x \equiv 1 \pmod{3}$

$x \equiv 1 \pmod{3}$

$x \equiv 16 \pmod{17}$

$x \equiv 15 \pmod{16}$ $\quad$ $x \equiv 1 \pmod{2}$

compatible

$3k+1$

$3k+1 \equiv 16 \pmod{17}$

etc

$x \equiv 1 \pmod{3}$

$x \equiv 16 \pmod{17}$

$x \equiv 15 \pmod{16}$

$x \equiv 15 \pmod{16}$

$x \equiv 16 \pmod{17}$

$\rightarrow$

$x \equiv -1 \pmod{16}$

$x \equiv -1 \pmod{17}$

$\downarrow$

$x \equiv -1 \pmod{\underset{\overset{\shortparallel}{272}}{16 \cdot 17}}$

$x = 272k - 1$

$\underbrace{272}\, k - 1 \equiv 1 \pmod{3}$

$2k \equiv 2 \pmod{3}$

$k \equiv 1 \pmod{3}$

$x = 272 \cdot (3\ell + 1) - 1$

$= \boxed{816\ell + 271}$

5. $100 \le n \le 999$

$$n^2 = \overline{\ldots\ldots n}$$

$$n^2 \equiv n \pmod{1000}$$

$$n^2 - n \equiv 0 \pmod{1000} \quad 1000 \to 2^3 \cdot 5^3$$

$$n \cdot (n-1) \equiv 0 \pmod{1000}$$

$$n \cdot (n-1) \equiv 0 \pmod 8 \qquad n(n-1) \equiv 0 \pmod{125}$$

$$8 \mid n(n-1) \qquad 125 \mid n(n-1)$$

$$8 \mid n \qquad 8 \mid n-1 \qquad 125 \mid n \qquad 125 \mid n-1$$

$$\boxed{n \equiv 0, 1 \pmod 8} \qquad \boxed{n \equiv 0, 1 \pmod{125}}$$

$2 \cdot 2 = 4$ solutions in mod 1000.

- $n \equiv 0 \pmod 8$, $n \equiv 0 \pmod{125}$

$$\Downarrow$$

$$n \equiv 0 \pmod{1000} \qquad \times$$

- $n \equiv 1 \pmod 8$, $n \equiv 1 \pmod{125}$

$$\Downarrow$$

$$n \equiv 1 \pmod{1000} \qquad \times$$

- $n \equiv 0 \pmod 8$, $n \equiv 1 \pmod{125}$

$$125k + 1 \equiv 0 \pmod 8$$

$$5k + 1 \equiv 0 \pmod 8$$

solve

$$k \equiv 3 \pmod 8$$

$$125k + 1 = 125 \cdot (8\ell + 3) + 1$$

$$= 1000\ell + \boxed{376}$$

• $n \equiv 1 \pmod 8$ $\quad n \equiv 0 \pmod{125}$

$125k \equiv 1 \pmod 8$

$5k = 8m + 1$

$5k - 8m = 1$

$5k \equiv 1 \pmod 8$ solve

$k \equiv 5 \pmod 8$

$125k = 125(8\ell + 5)$

$= 1000\ell + \boxed{625}$

6 n powerful if $\boxed{p \mid n \Rightarrow p^2 \mid n}$

All the exponents are at least two

in the prime factorisation

Inf. many a s.t

$a, a+1, a+2$ not powerful.

$2 \mid n \quad 4 \nmid n \longrightarrow 2 \pmod 4$

$3 \mid n \quad 9 \nmid n \quad \rightarrow \quad 3$ or $6 \pmod 9$

$5 \mid n \quad 25 \nmid n \quad \rightarrow \quad 5, 10, 15, 20 \pmod{25}$

$a \equiv 2 \pmod 4$ $\quad$ a not powerful

$a \equiv 2 \pmod 9 \rightarrow a+1$ not powerful

$a \equiv 3 \pmod{25} \rightarrow a+2$ not powerful

Φ

There is a unique solution

$t \pmod{900}$.

$t, t+900, t+2\cdot 900, t+3\cdot 900, \ldots$

they all satisfy the condition

back at $\boxed{12:23}$

n pseudo prime

$2^n \equiv 2 \pmod{n}$

WTS: $2^{2^n - 1} \equiv 2 \pmod{2^n - 1}$

WTS: $2^{2^n - 2} \equiv 1 \pmod{2^n - 1}$

WTS: $2^{2^n - 2} - 1 \equiv 0 \pmod{2^n - 1}$

WTS: $2^n - 1 \mid 2^{2^n - 2} - 1$.

$2^n - 2 \equiv 0 \pmod{n} \Rightarrow 2^n - 2 = n \cdot k$

WTS: $2^n - 1 \mid 2^{nk} - 1$

$\downarrow$

$(2^n)^k - 1 = (2^n - 1)(\ldots\ldots)$ ✓

$2^n \mid 2^{nk} - 1$