Q1

Need to find the smallest positive solution to the system

$x \equiv 1 \mod 2$

$x \equiv 1 \mod 3$

$x \equiv 1 \mod 4$

$x \equiv 1 \mod 5$

$x \equiv 1 \mod 6$

$x \equiv 0 \mod 7.$

equivalent to finding s.l.n the system

$$\begin{cases} x \equiv 1 \pmod{60} \\ x \equiv 0 \pmod 7 \end{cases}$$

$$(2|x-1) \wedge (3|x-1) \wedge (4|x-1) \wedge (5|x-1) \wedge (6|x-1) \iff (60|x-1)$$

$\gcd(60,7) = 1$. By Chinese Remainder thm,

$$x = 7x_1 + 0$$

is a soln to the system of congruences.

where $x_1$ is a soln to $7x \equiv 1 \pmod{60}$

Euclidean Alg:

$$60 = 8 \times 7 + 4$$
$$7 = 1 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$
$$1 = 4 - 3 = 4 - (7-4) = 2 \times 4 - 7$$
$$= 2(60 - 8 \times 7) - 7 = 2 \times 60 + (-17)7$$

$x_1 = -17$ or $43$.

So $x = 7 \times 43 = 301$.

55 numbers chosen from the set $\{1, 2, -, 100\}$.

(Q3) 9 congruence classes of modulo 9.

$0, 1, 2, - , 8$

At least one congruence class must have 7 numbers out of 55.

$$a_1 < a_2 < - - < a_7.$$

<u>Claim</u>: $\exists\, i \in \{1, - 6\}$ s.t $a_{i+1} - a_i = 9$.

If not $\forall i$, $a_{i+1} - a_i \in \{18, 27, - - \}$.

$$\Rightarrow a_7 - a_1 \geq 6 \times 18 = 108 \quad \text{X}^c.$$

(Q2) $a, b \in \mathbb{Z}$. $a, b \geq 1$.

Assume $(36a + b)(a + 36b)$ is a power of 2, for some $a, b$

Assume $a < b$ and $\gcd(a, b) = 1$.

w.l.o.g

$$\Rightarrow \begin{aligned} 36a + b &= 2^m \qquad m < n \\ a + 36b &= 2^n \end{aligned}$$

$$\Rightarrow \begin{aligned} 35(a - b) &= 2^m - 2^n = 2^m\left[1 - 2^{n-m}\right] \\ 37(a + b) &= 2^m + 2^n = 2^m\left[1 + 2^{n-m}\right] \end{aligned}$$

$\Rightarrow$ Both $(a - b)$ & $(a + b)$ are divisible by $2^m$

$\Rightarrow$ Both $a$ & $b$ are divisible by $2^{m-1}$

$\Rightarrow$ Since $\gcd(a, b) = 1$, $m - 1 = 0$

$\Rightarrow$ $36a + b = 2$ which is impossible.

$\Rightarrow$

(Q4) No poly. with integer coefficients $P(x)$ with $P(7) = 5$ and $P(15) = 9$.

Assume there is a poly

$$P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

with integer coefficients and $P(7) = 5$ & $P(15) = 9$.

$$P(15) = a_0 + a_1 15 + a_2 (15)^2 + \dots + a_n (15)^n$$

$$P(7) = a_0 + a_1 7 + a_2 7^2 + \dots + a_n (7^n)$$

$$\Rightarrow 4 = P(15) - P(7) = a_1(15-7) + a_2(15^2 - 7^2) + \dots + a_n(15^n - 7^n)$$

$15^k - 7^k$ is divisible by 8 for all $k \geq 1$.

$$\Rightarrow 8 \mid 4 \quad \cancel{\times}^n$$

Q5 $\quad f: \{0,1,2,\dots\} \longrightarrow \{0,1,2,\dots\}$.

$\forall m,n \geq 0, \quad 2f(m^2+n^2) = (f(m))^2 + (f(n))^2$.

Soln: $m=0,\ n=0$

$2f(0) = 2f(0)^2$

$\Rightarrow f(0)(1-f(0)) = 0$

$\Rightarrow f(0)=0$ or $f(0)=1$

$f(0)=0$, $\quad m=1,\ n=0$

$2f(1) = f(1)^2 + 0$

$f(1)(f(1)-2) = 0$

$f(1)=0,\ f(1)=2$.

$f(0)=0,\ f(1)=0$

$f(0)=0,\ f(1)=2$

$f(0)=1$, $\quad m=1,\ n=0$

$2f(1) = f(1)^2+1$

$f(1)^2 - 2f(1) + 1 = 0$

$(f(1)-1)^2 = 0$

$f(1)=1$.

$f(0)=1,\ f(1)=1$

$f(0)=0,\ f(1)=0,\quad m=n=1 \Longrightarrow 2f(2)=0 \Rightarrow f(2)=0$

$f(0)=0,\ f(1)=2,\quad m=n=1 \Longrightarrow 2f(2)=8 \Rightarrow f(2)=4$.

$f(0)=1,\ f(1)=1,\quad m=n=1 \Longrightarrow 2f(2)=2 \Rightarrow f(2)=1$.

(a) $f(0)=0,\ f(1)=0,\ f(2)=0$

(b) $f(0)=1,\ f(1)=1,\ f(2)=1$

(c) $f(0)=0,\ f(1)=2,\ f(2)=4$.

$(0,0) \longrightarrow 0$

$(1,0) \longrightarrow 1$

$(1,1) \longrightarrow 2$ ⟵ 3 missing

$(2,0) \longrightarrow 4$

$(2,1) \longrightarrow 5$

$(5,0) \longrightarrow (3,4) \longrightarrow 3.$ ⟵ 6 & 7 missing

$(2,2) \longrightarrow 8$

$(3,0) \longrightarrow 9$

$(3,1) \longrightarrow 10$

$(10,0) \longrightarrow (6,8) \longrightarrow 6$

$(5,5) \longrightarrow (7,1) \longrightarrow 7$

$f(4) = 8$

$f(5) = 10$

$f(3)^2 + f(4)^2 = f(5)^2 + f(0)^2$

$\Rightarrow f(3) = 6$

$f(8) = 16$

$f(9) = 18$

$f(10) = 20$

$f(n) = 2n, \quad n \leq 10$

$(5k)^2 + 0^2 = (3k)^2 + (4k)^2.$ identity.

$(5k)^2 + 0^2 = (3k)^2 + (4k)^2$

$(5k+1)^2 + 2^2 = (3k-1)^2 + (4k+2)^2$

$(5k+2)^2 + 1^2 = (3k+2)^2 + (4k+1)^2$

$(5k+3)^2 + 1^2 = (3k+1)^2 + (4k+3)^2$

$(5k+4)^2 + \quad = (3k+4)^2 + (4k+2)^2$

If $k \geq 2$ then the first term on the left is greater than any of two terms on the right.

Assume that $f(k) = 2k$, for $k < n$.

need to show $f(n) = 2n$.

Let $n = 5m + j$, $0 \leq j \leq 4$.

Use the above identities, then we can write

$n^2 + m_1^2 = m_2^2 + m_3^2$. and

$(f(n))^2 + (f(m_1))^2 = 2f(n^2 + m_1^2) = 2f(m_2^2 + m_3^2) = f(m_2)^2 + f(m_3)^2$

$\Rightarrow (f(n))^2 + (f(m_1))^2 = (f(m_2))^2 + (f(m_3))^2$.

$\Rightarrow f(n)^2 + (2m_1)^2 = (2m_2)^2 + (2m_3)^2$

$\Rightarrow f(n)^2 = 4(m_2^2 + m_3^2 - m_1^2) = 4n^2$

$\Rightarrow f(n) = 2n$.

So by induction $f(n) = 2n$ for all $n \in \mathbb{N}$.

By similar argument $f(n) = 0$ for all $n$ in Case (a)

and $f(n) = 1$ for all $n$ " (b)

Q6 h $ax+by=c$, $a,b,c \in \mathbb{Z}$ has a sol$^n$ in integers $x$ and $y$ iff $\gcd(a,b)/c$.

If $(x_0,y_0)$ is a integer sol$^n$ then

$$x' = x_0 + \frac{bk}{d}, \quad y' = y_0 - \frac{ak}{d}, \quad d = \gcd(a,b)$$

are also ~~a~~ sol$^n$ for each $k \in \mathbb{Z}$., and integer sol$^n$s are of this form.

(⇒) $\gcd(a,b)/a$ & $\gcd(a,b)/b$

$\Rightarrow \gcd(a,b) / ax+by$

$\Rightarrow \gcd(a,b)/c$.

(⇐) ~~Assume c~~ $\gcd(a,b)$.

$= sa+tb$ for some $s,t \in \mathbb{Z}$

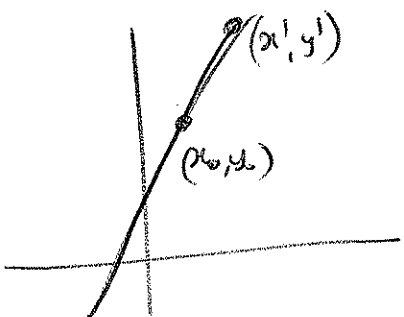
$\gcd(a,b)/c \Rightarrow c = q\gcd(a,b)$

$$\Rightarrow c = q(sa+tb).$$
$$= (qs)a + (qt)b$$
$$= xa + yb.$$

$x = qs$, $y = qt$.

II $ax'+by' = a\left(x_0 + \frac{bk}{d}\right) + b\left(y_0 - \frac{ak}{d}\right)$

$= ax_0 + by_0 = c$




$$\frac{y'-y_0}{x'-x_0} = \frac{-a}{b} = \frac{-\frac{a}{d}}{b/d}$$

$$\Rightarrow y' = y_0 - \frac{a}{d}k, \quad x' = x_0 + \frac{b}{d}k.$$

Q1: $a_1,\dots,a_n \in \mathbb{Z}$ $\gcd(a_1,\dots,a_n)=1$, $S \subseteq \mathbb{Z}$ with

(1) $\forall i=1\dots n$, $a_i \in S$

(2) $\forall i,j$, $a_i - a_j \in S$

(3) $\forall x,y \in S$, if $x+y \in S$ then $x-y \in S$.

(4) $0 \in S$ $[\because 0 = a_1 - a_1 \in S$ by (2)$]$

(5) $\forall x \in S$, $-x \in S$ $[0+x \in S \Rightarrow 0-x = -x \in S]$.

(6) $\forall x,y \in S$, $x-y \in S \Rightarrow x+y \in S$ $\left[\begin{array}{l} y \in S \Rightarrow -y \in S \quad (5) \\ x+y = x-(-y) \in S \quad (3) \end{array}\right]$

ignore (7) $\forall i$, $ma_i \in S$ for all $m \in \mathbb{Z}$.

$$(a_i - a_j) + a_j \in S \xRightarrow{(3)} (a_i - a_j) - a_j = a_i - 2a_j \in S.$$

If $(a_1,\dots,a_n)$ generates $S$ then $(a_1, a_2-a_1, \dots, a_n-a_1)$ which again generates $S$.

Apply this step to $(|a_1|, |a_2|, \dots, |a_n|)$ and assuming that $|a_1|$ is the smallest of these numbers, we obtain another n-tuple $(|a_1|, |a_2|-|a_1|, \dots, |a_n|-|a_1|)$ the sum of whose entries is smaller. Because we cannot have infinite decent, we eventually reach an n-tuple with the first entry equal to 0. In the process we did not change greatest common divisor of the entries. Ignoring the zero entries, we can repeat the procedure until there is only one non-zero number left. This number must be 1.

$$\gcd(x,y) = \gcd(x, y-x)$$

Now $0, 1 \in S \Rightarrow -1 \in S$.

by ③ $1 + (-1) \in S \Rightarrow 1 - (-1) = 2 \in S$.

Inductively we find that all positive, and also all negative integers are in $S$.

$$S = \mathbb{Z}.$$