PROBLEM I Prove that solution of equation

$$x^2+y^2=z^4, \gcd(x,y)=1, x>0, y>0, z>0, 2\mid x$$

is

$$\begin{cases} x=4ab(a^2-b^2) \\ y=|a^4+b^4-6a^2b^2| \\ z=a^2+b^2 \end{cases}$$

where $a>0, b>0, \gcd(a,b)=1, a\not\equiv b \mod 2$.

SOLUTION . On one hand, we know x, y, z^2 is solution of Pythagorean equation, so there exists $s, t \in \mathbb{N}^+, s>t, \gcd(s,t)=1, s\not\equiv t \mod 2$, such that

$$\begin{cases} x=2st \\ y=s^2-t^2 \\ z^2=s^2+t^2 \end{cases}$$

For convinence we dismiss the condition $s>t$ and let $y=|s^2-t^2|$ instead. Now s, t are symmetry, so without loss of generality assume $2\mid s$, then (s,t,z) is solution of Pythagorean equation, so $\exists a, b \in \mathbb{N}^+, \gcd(a,b)=1, a\not\equiv b \mod 2, a>b$, such that

$$\begin{cases} s=2ab \\ t=a^2-b^2 \\ z=a^2+b^2 \end{cases}$$

So $x=2st=2\times 2ab\times(a^2-b^2)=4ab(a^2-b^2)$, and $y=|s^2-t^2|=|4a^2b^2-a^4-b^4+2a^2b^2|=|a^4+b^4-6a^2b^2|$, and $z=a^2+b^2$.

On the other hand, it is easy to check that for $x=4ab(a^2-b^2), y=|a^4+b^4-6a^2b^2|, z=a^2+b^2$ we have $x^2+y^2=z^4$. And since $\gcd(a,b)=1$ we get $\gcd(x,y)\mid\gcd(2,y)^2\gcd(a,y)\gcd(b,y)\gcd(a+b,y)\gcd(a-b,y)=\gcd(2,a^4+b^4)^2\gcd(a,b^4)\gcd(b,a^4)\gcd(a+b,4a^4)\gcd(a-b,4a^4)$. Since $a\not\equiv b \mod 2$ we get $\gcd(2,a^4+b^4)=1$. Easily to know $\gcd(a,b^4)=\gcd(b,a^4)=1$. And $\gcd(a\pm b,4a^4)\mid\gcd(a\pm b,2)^2\gcd(a\pm b,a)^4=1$. Finally we get $\gcd(x,y)=1$. Easy to check $x,y,z>0$ and $2\mid x$.

All in all, they are all solution of the given equation. □

PROBLEM II Find a method to judge whether a number can be divided by $37, 101$.

SOLUTION . Noting $1000\equiv 1 \mod 37$, so we can use 1000-binary. Assume $n=\sum_{k=0}^m a_k 1000^k$ and $0\le a_k<1000$. Then $n\equiv\sum_{k=0}^m a_k \mod 37$. So $37\mid n \iff 37\mid\sum_{k=0}^m a_k$.

For 10-binary, we can combine them as group of three. Assume $n=\sum_{k=0}^t b_k 10^k, 0\le b_k<10$. Let $s=\left\lceil\frac{t}{3}\right\rceil$ and let $b_k=0$ for $k>t$. Then $n=\sum_{k=0}^s(b_{3k}+10b_{3k+1}+100b_{3k+2})1000^k$. Then $37\mid n \iff 37\mid\sum_{k=0}^s b_{3k}+10b_{3k+1}+100b_{3k+2}$.

Noting $100\equiv -1 \mod 101$, so we can consider 100-binary for 101. Assume $n=\sum_{k=0}^m a_k 100^k$ and $0\le a_k<100$. Then $n\equiv\sum_{k=0}^m(-1)^k a_k \mod 101$. So $101\mid n \iff 101\mid\sum_{k=0}^m(-1)^k a_k$.

For 10-binary, we can combine them as group of two. Assume $n = \sum_{k=0}^{t} b_k 10^k, 0 \le b_k < 10$. Let $s = \lceil \frac{t}{2} \rceil$ and let $b_k = 0$ for $k > t$. Then $n = \sum_{k=0}^{s}(b_{2k} + 10b_{2k+1})100^k$. Then $101 \mid n \iff 101 \mid \sum_{k=0}^{s}(-1)^k(b_{2k} + 10b_{2k+1})$. □

PROBLEM III Assume $2 \nmid a$, then $a^{2^n} \equiv 1 \mod 2^{n+2}$.

SOLUTION. We will prove $a^{2^n} - 1 = (a^2 - 1)\prod_{k=1}^{n-1}(a^{2^k} + 1)$ first. Prove it by MI to n. When $n = 1$ there is nothing to do. Assume it holds for certain n, consider $n+1$, we get $a^{2^{n+1}} - 1 = (a^{2^n} + 1)(a^{2^n} - 1) = (a^{2^n} + 1)(a^2 - 1)\prod_{k=1}^{n-1}(a^{2^k} + 1) = (a^2 - 1)\prod_{k=1}^{n}(a^{2^k} + 1)$. So we get it holds for every $n \in \mathbb{N}^+$.

Since $2 \nmid a$, assume $a = 2b + 1$, then $a^2 - 1 = 4b^2 + 4b = 4b(b+1)$. Noting $2 \mid b(b+1)$, we get $8 \mid a^2 - 1$. And easily $2 \mid a^{2^k} + 1, \forall k \in \mathbb{N}$. So we get $8 \times \prod_{k=1}^{n-1} 2 \mid a^{2^n} - 1$, i.e., $2^{n+2} \mid a^{2^n} - 1$. Finally we get $a^{2^n} \equiv 1 \mod 2^{n+2}$. □

PROBLEM IV Let p be a prime and s, t be integers and $t \le s$. Prove that $(u + p^{s-t}v : 0 \le u \le p^{s-t} - 1, 0 \le v \le p^t - 1)$ is a Complete residue system of p^s.

SOLUTION. Since there are p^{s-t} different u and $p^t - 1$ different v, there are p^s different elements in total. So we only need to prove any two of them are not equal $\mod p^s$.

Assume $u_1 + p^{s-t}v_1 \equiv u_2 + p^{s-t}v_2 \mod p^s$, we need to prove $(u_1, v_1) = (u_2, v_2)$. Consider $\mod p^{s-t}$, we get $u_1 \equiv u_2 \mod p^{s-t}$. Since $|u_1 - u_2| \le p^{s-t} - 1$, we easily get $u_1 = u_2$. Then $p^{s-t}v_1 \equiv p^{s-t}v_2 \mod p^s$. So $v_1 \equiv v_2 \mod p^t$. For the same reason since $|v_1 - v_2| \le p^t - 1$ we get $v_1 = v_2$. So we proved any two of them are not equal $\mod p^s$.

So $(u + p^{s-t}v : 0 \le u \le p^{s-t} - 1, 0 \le v \le p^t - 1)$ is a Complete residue system of p^s. □

PROBLEM V Assume $m_1, \cdots, m_k$ is k integers coprime to each other. Assume $A_1, A_2, \cdots, A_k$ is Complete residue of $m_1, \cdots, m_k$ respectively. Let $m = \prod_{t=1}^{k} m_t$ and $M_t := \frac{m}{m_t}, t = 1, \cdots, k$. Prove that $A := \{\sum_{t=1}^{k} M_t x_t : x_t \in A_t, t = 1, \cdots, k\}$ is a Complete residue of m.

SOLUTION. Easily $|A_t| = m_t$, so there is m different $(x_1, \cdots, x_k)$. So we only need to prove for different $(x_1, \cdots, x_k)$ the value of $\sum_{t=1}^{k} M_t x_t \mod m$ is different.

Assume $\sum_{t=1}^{k} M_t x_t \equiv \sum_{t=1}^{k} M_t y_t$ and $x_t, y_t \in A_t, t = 1, \cdots, k$. Now we need to prove $(x_1, \cdots, x_k) = (y_1, \cdots, y_k)$. Noting for $i \ne j$ we have $m_i \mid M_j$. So we consider $\mod m_i$, we get $M_i x_i \equiv M_i y_i \mod m_i$. Then $m_i \mid M_i(x_i - y_i)$. Since $\gcd(m_i, m_j) = 1$ for $i \ne j$, we get $\gcd(m_i, M_i) = 1$. So $m_i \mid x_i - y_i$. Since $x_i, y_i \in A_i$ and A_i is Complete residue of m_i, we get $x_i = y_i$. So $(x_1, \cdots, x_k) = (y_1, \cdots, y_k)$.

So finally we get A is Complete residue of m. □

PROBLEM VI Let $H = \frac{3^{n+1}-1}{3-1}$. Let $I = \{(x_0, \cdots, x_n) : x_k \in \{-1, 0, 1\}, k = 0, \cdots, n\}$. Let $f : I \to N := [-H, H] \cap \mathbb{Z}$, and $f(x_0, \cdots, x_n) = \sum_{k=0}^{n} x_k 3^k$. Prove that f is bijection. Thus, we can use $n+1$ weights and a balance to weigh all integer weights between 1 and H.

SOLUTION. First we prove f is well-defined. i.e., $\forall (x_0, \cdots, x_n) \in I, -H \le \sum_{k=0}^{n} x_k 3^k \le H$. Since $x_k = -1, 0, 1$, we get $\sum_{k=0}^{n} x_k 3^k \le \sum_{k=0}^{n} 1 \times 3^k = \frac{3^{n+1}-1}{3-1} = H$. For the same reason, we get $\sum_{k=0}^{n} x_k 3^k \ge -H$.

Second we will prove f is injection. Assume $x, y \in I$ and $f(x) = f(y)$, i.e., $\sum_{k=0}^{n} x_k 3^k = \sum_{k=0}^{n} y_k 3^k$, we need to prove $x = y$. If $x \neq y$, then assume $m = \min\{t : x_t \neq y_t\}$. Then $x_t = y_t, \forall t < m$. So $\sum_{k=m}^{n} x_k 3^k = \sum_{k=m}^{n} y_k 3^k$. Consider $\mod 3^{m+1}$, we get $x_m 3^m \equiv y_m 3^m \mod 3^{m+1}$, i.e., $x_m \equiv y_m \mod 3$. But $x_m, y_m \in \{-1, 0, 1\}$ and $x_m \neq y_m$, contradiction! So $x = y$ and thus f is injection.

Finally we prove f is surjection. Since $|I| = 3^{n+1}$, and $|N| = 2H + 1 = 3^{n+1}$, we get $|I| = |N| < \infty$. Noting we have proved f is injection, so f is surjection.

All in all, f is bijection.

Now we use $n+1$ weights, $3^0, 3^1, \cdots, 3^n$. For every integer $n : 1 \leq n \leq H$, we know there is a $x \in I$ such that $f(x) = n$. Let $L := \{t : x_t = 1\}$ and $R = \{t : x_t = -1\}$, put the thing to weigh on right, and put weights in R on right, then put weights in L on left, we can weigh this thing out if it's weight is n. □

PROBLEM VII Assume $m_1, \cdots, m_k$ is k integers coprime to each other. Assume $A_1, A_2, \cdots, A_k$ is Complete residue of $m_1, \cdots, m_k$ respectively. Let $m = \prod_{t=1}^{k} m_t$ and $M_t := \prod_{i=1}^{t-1} m_i, t = 1, \cdots, k$. Prove that $A := \{\sum_{t=1}^{k} M_t x_t : x_t \in A_t, t = 1, \cdots, k\}$ is a Complete residue of m.

SOLUTION. Easily $|A_t| = m_t$, so there is m different $(x_1, \cdots, x_k)$. So we only need to prove for different $(x_1, \cdots, x_k)$ the value of $\sum_{t=1}^{k} M_t x_t \mod m$ is different.

Assume $\sum_{t=1}^{k} M_t x_t \equiv \sum_{t=1}^{k} M_t y_t$ and $x_t, y_t \in A_t, t = 1, \cdots, k$. Now we need to prove $(x_1, \cdots, x_k) = (y_1, \cdots, y_k)$. Noting for $i < j$ we have $m_i \mid M_j$. If $(x_1, \cdots, x_k) \neq (y_1, \cdots, y_k)$, then let $i = \min\{t : x_t \neq y_t\}$. Then $\sum_{t=i}^{k} M_t x_t = \sum_{t=i}^{k} M_t y_t$. Consider $\mod m_i$, we get $M_i x_i \equiv M_i y_i \mod m_i$. Then $m_i \mid M_i(x_i - y_i)$. Since $\gcd(m_i, m_j) = 1$ for $i > j$, we get $\gcd(m_i, M_i) = 1$. So $m_i \mid x_i - y_i$. Since $x_i, y_i \in A_i$ and A_i is Complete residue of m_i, we get $x_i = y_i$. So $(x_1, \cdots, x_k) = (y_1, \cdots, y_k)$.

So finally we get A is Complete residue of m. □