

1. Find a complete set of residues modulo 7 so that...
- (a) ...each residue is even

It suffices to find a set S of seven even numbers so that for each $0 \leq i < 6$, some element of S is congruent to $i \pmod{7}$. For instance, $S = \{0, 2, 4, 6, 8, 10, 12\}$ has

$$\begin{aligned}0 &\equiv 0 \pmod{7} \\8 &\equiv 1 \pmod{7} \\2 &\equiv 2 \pmod{7} \\10 &\equiv 3 \pmod{7} \\4 &\equiv 4 \pmod{7} \\12 &\equiv 5 \pmod{7} \\6 &\equiv 6 \pmod{7}\end{aligned}$$

- (b) ...each residue is odd

We can take $S = \{1, 3, 5, 7, 9, 11, 13\}$ because

$$\begin{aligned}7 &\equiv 0 \pmod{7} \\1 &\equiv 1 \pmod{7} \\9 &\equiv 2 \pmod{7} \\3 &\equiv 3 \pmod{7} \\11 &\equiv 4 \pmod{7} \\5 &\equiv 5 \pmod{7} \\13 &\equiv 6 \pmod{7}\end{aligned}$$

- (c) ...each residue is prime

We can take $S = \{2, 3, 5, 7, 11, 13, 29\}$ because

$$7 \equiv 0 \pmod{7}$$

$$29 \equiv 1 \pmod{7}$$

$$2 \equiv 2 \pmod{7}$$

$$3 \equiv 3 \pmod{7}$$

$$11 \equiv 4 \pmod{7}$$

$$5 \equiv 5 \pmod{7}$$

$$13 \equiv 6 \pmod{7}$$

2. Prove that if $m > 4$ is composite, then

$$(m-1)! \equiv 0 \pmod{m}$$

Since m is composite, we can write $m = pq$ where $1 < p \leq q \leq m-1$. If m is not the square of a prime, we can assume $p < q$. In that case $(m-1)! = (m-1)(m-2)\cdots q\cdots p\cdots 2\cdot 1$ in which case $m = pq \mid (m-1)!$ and hence, $(m-1)! \equiv 0 \pmod{m}$.

Now suppose that $m = p^2$ for some prime p . Since $m > 4$, $p = \sqrt{m} > 2$. But then $2p < p^2 = m$, so $2p \leq m-1$. Now we can conclude that $(m-1)! = (m-1)(m-2)\cdots(2p)\cdots p\cdots 2\cdot 1$. Therefore, $p(2p) = 2m \mid (m-1)!$ and in particular, $m \mid (m-1)!$.

3. Let p be an odd prime. Show that $x^2 \equiv 1 \pmod{p}$ has exactly two incongruent solutions mod p .

Note that $x = 1$ and $x = -1$ are both solutions to $x^2 \equiv 1 \pmod{p}$. If $1 \equiv -1 \pmod{p}$, then $2 \equiv 0 \pmod{p}$, so $p = 2$. By assumption, p is odd and hence, $1 \not\equiv -1 \pmod{p}$. Therefore, $x = 1$ and $x = -1$ are incongruent solutions mod p .

To show that there are no more than two solutions mod p , suppose that $a \in \mathbb{Z}$ solves $x^2 \equiv 1 \pmod{p}$. Then $p \mid a^2 - 1 = (a - 1)(a + 1)$. Since p is prime, we can conclude that $p \mid a - 1$ or $p \mid a + 1$. But this exactly means that $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

4. Show that $x^2 \equiv 1 \pmod{2^s}$ has four distinct solutions $\pmod{2^s}$ when $s \geq 3$.

Note that $x = -1$ and $x = 1$ are both solutions and they are distinct $\pmod{2^s}$ since $s \geq 3$. Additionally, $x = 2^{s-1} - 1$ and $x = 2^{s-1} + 1$ are solutions because

$$\begin{aligned}(2^{s-1} - 1)^2 &\equiv 2^{2s-2} - 2 \cdot 2^{s-1} + 1 \equiv 1 \pmod{2^s} \\ (2^{s-1} + 1)^2 &\equiv 2^{2s-2} + 2 \cdot 2^{s-1} + 1 \equiv 1 \pmod{2^s}\end{aligned}$$

Moreover, since $s \geq 3$, $1 < 2^{s-1} - 1 < 2^{s-1} + 1 < 2^s - 1$ and hence, $x = 1, 2^{s-1} - 1, 2^{s-1} + 1$, and $x = 2^s - 1$ are distinct solutions $\pmod{2^s}$.

We claim that these solutions are the only solutions $\pmod{2^s}$. Suppose that $a \in \mathbb{Z}$ satisfies $a^2 \equiv 1 \pmod{2^s}$. Then $2^s \mid a^2 - 1 = (a - 1)(a + 1)$. For this to be the case, a must be odd. Then either $a - 1 \equiv 2 \pmod{4}$ or $a + 1 \equiv 2 \pmod{4}$. Hence, exactly one of $a - 1$ or $a + 1$ has at most one 2 in its prime factorization. But then the other must be divisible by 2^{s-1} if $(a - 1)(a + 1)$ is to be divisible by 2^s . So we can either write $a = 1 + k \cdot 2^{s-1}$ or $a = -1 + k \cdot 2^{s-1}$ for some $k \in \mathbb{Z}$. But only $1, -1 + 2^{s-1}, 1 + 2^{s-1}$, and $2^{s-1} - 1$ have this property among numbers between 0 and $2^s - 1$. Therefore, these are the only four solutions to $x^2 \equiv 1 \pmod{2^s}$.