ORMC Olympiad Group Winter 2022
Week 3 Solutions

Sumith Nalabolu

January 21, 2022

Solution 1

We want to compute $1 \cdot 2 \cdots (p-1)$ modulo p. Note that for each $a \in \{1, 2, \ldots, p-1\}$, there exists its inverse a^{-1} modulo p, i.e. $aa^{-1} \equiv 1 \pmod{p}$. This motivates pairing each number with its inverse.

Furthermore, note that the only numbers which are their own inverse are 1 and -1; that is, if a is its own inverse modulo p, then we have $a^2 \equiv 1 \pmod{p}$. Manipulating and factoring this gives $(a-1)(a+1) \equiv 0 \pmod{p}$, i.e. $p \mid (a-1)(a+1)$. Since p is prime, this implies $p \mid a-1$ or $p \mid a+1$. Thus a must be either 1 or -1 modulo p. Hence these are the only numbers which are their own inverse (note why p had to be prime here).

Thus, in the product $1 \cdot 2 \cdots (p-1)$, we can pair every number other than 1 and $p-1$ with its inverse, and these pairs evaluate to 1 modulo p; thus we have

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p},$$

as desired. $\square$

Solution 3

The proof is similar to that of Fermat's Little Theorem. Let the $\phi(n)$ numbers which are relatively prime to n be $\{x_1, \ldots, x_{\phi(n)}\}$. Then, consider the set

$$\{a \cdot x_1, \ldots, a \cdot x_{\phi(n)}\}$$

taken modulo n. We claim this is in fact the same set as $\{x_1, \ldots, x_{\phi(n)}\}$. First we show that the elements of the set are all distinct; suppose that $a \cdot x_i \equiv a \cdot x_j \pmod{n}$ for some $i, j \in \{1, \ldots, \phi(n)\}$. Then, this implies $a(x_i - x_j) \equiv 0 \pmod{p}$, so $n \mid a(x_i - x_j)$. But $\gcd(n, a) = 1$, so this in fact means that $n \mid x_i - x_j$. However, x_i, x_j are just some numbers out of $\{1, 2, \ldots, n-1\}$. Hence $p \mid x_i - x_j$ implies that $x_i = x_j$. That is, if $ax_i \equiv ax_j \pmod{n}$, then $x_i \equiv x_j \pmod{n}$. Hence every element of the set

$$\{a \cdot x_1, \ldots, a \cdot x_{\phi(n)}\}$$

is distinct. To finish proving the above claim, we must show that each $a \cdot x_i$ is one of the x_j. That is, we must show $a \cdot x_i$ is relatively prime to n. But this follows from the fact that both a and x_i are relatively prime to n, so their product must be as well. Thus, we can conclude that the two sets

$$\{a \cdot x_1, \ldots, a \cdot x_{\phi(n)}\}, \qquad \{x_1, \ldots, x_{\phi(n)}\}$$

are the same sets when taken modulo n (just some permutations of each other). Hence their products must be equivalent, i.e.

$$\prod_{i=1}^{\phi(n)} (a \cdot x_i) \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n} \implies a^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}.$$

Finally, cancelling the $\prod_{i=1}^{\phi(n)} x_i$ term from both sides (note that this is allowed since it is relatively prime to n) gives $a^{\phi(n)} \equiv 1 \pmod{p}$. $\square$

Solution 4

Note that $111 = 3 \cdot 37$. In particular, this gives that $37 \mid 999$, so $1000 \equiv 1 \pmod{37}$. This motivates splitting the number into three digit numbers and summing those. If we let the number be $\overline{a231b312c}$, then it is equivalent to

$$\overline{a23} + \overline{1b3} + \overline{12c} \equiv (100a + 10b + c) + 246 \pmod{37}.$$

This must be 0 (mod 37), so simplifying gives $\overline{abc} \equiv 13 \pmod{37}$. So we must find the number of three digit numbers equivalent to 13 modulo 37, and each of these will correspond to one choice of the digits a, b, c. These numbers are $37(3) + 13, \ldots, 37(26) + 13$, for a total of $\boxed{24}$ numbers. $\square$

Solution 5

Note that $100 \equiv 1 \pmod{99}$; thus any $100^k \equiv 1 \pmod{99}$. So we can split the number into two digit numbers and then add those, and the result will be equivalent to the original number. Thus, we want the smallest two digit n such that $12 + 13 + \ldots + n \equiv 0 \pmod{99}$. Equivalently, this is the sum of 1 to n minus the sum of 1 to 11, so

$$\frac{n(n+1) - 11(12)}{2} \equiv 0 \pmod{99} \iff n(n+1) - 11(12) \equiv 0 \pmod{99}.$$

(This is true since $\gcd(2, 99) = 1$). The left side factors, so we have $(n - 11)(n + 12) \equiv 0 \pmod{99}$. Now note that $99 = 9 \cdot 11$, and since 11 is prime this implies n is either 0 or -1 modulo 11. Testing these values (they must also be either 2 or 6 modulo 9) starting with 21 gives that $n = \boxed{33}$ is the smallest that works. $\square$

Solution 6

Note that $p = 2$ does not work, and that $p = 3$ does work. Now for $p > 3$, we consider the numbers modulo 3. Clearly $p \not\equiv 0 \pmod{3}$. If $p \equiv 1 \pmod{3}$, then $p^2 + p + 1 \equiv 0 \pmod{3}$ and thus cannot be prime. But if $p \equiv 2 \pmod{3}$, then $p + 10 \equiv 0 \pmod{3}$ and thus cannot be prime. So, no $p > 3$ can work. Thus the answer is $\boxed{3}$. $\square$

Solution 7

Let the n numbers be $a_1, \ldots, a_n$. Then, consider the n sums

$$s_1 = a_1, \qquad s_2 = a_1 + a_2, \qquad \ldots \qquad s_n = a_1 + a_2 + \ldots + a_n.$$

That is, s_i is the sum of a_1 through a_i. When taken modulo n, these are all numbers from 0 to $n - 1$. If any one of them is 0, then we are done. If none of them are 0, then this is a set of n numbers between 1 and $n - 1$. Thus (by pigeonhole principle) there must exist some two of them equal; that is, $s_i = s_j$ for some $i < j$. Then note that $s_j - s_i \equiv a_{i+1} + \ldots + a_j \equiv 0 \pmod{p}$, as desired. $\square$

Solution 8

Note that 109 is prime. Then, by FLT (Fermat's little thm), $k^{108} \equiv k \pmod{109}$ for each $k = 2, 3, 6$. Hence $k^{107} \equiv \frac{1}{k} \pmod{109}$. Then,

$$2^{107} + 3^{107} + 6^{107} \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} \equiv \boxed{1} \pmod{109}.$$

$\square$

Solution 9

The answer is $\boxed{\text{no}}$. Consider any number consisting of these numbers in some order. Then it will be equal to $\displaystyle\sum_{i=1}^{2008}(i^i)(10^{a_i})$ where the $a_i \geq 0$, i.e. the sum of the i^i times some power of 10. Now take this expression modulo 3. Since $10 \equiv 1 \pmod 3$, we can ignore the powers of 10, so it is equivalent to $\displaystyle\sum_{i=1}^{2008} i^i$.

Now note that any $a^3 \equiv a \pmod 3$; in particular, this means $a^k \equiv a \pmod 3$ for any odd k, and $a^k \equiv a^2 \pmod 3$ for even k. Hence the expression is

$$\sum_{i=1}^{1004}(2i-1) + \sum_{i=1}^{1004}(2i)^2.$$

The first term is the sum of the first 1004 odd integers and thus equals 1004^2. For the second term, take out the factor of 4 from each term and then use sum of squares; so, the expression is

$$1004^2 + (4)\frac{(1004)(1005)(2009)}{6} \equiv 2^2 + 2(1004)(335)(2009) \equiv 1 + 2(2)(2)(2) \equiv 2 \pmod 3.$$

But no square can be $2 \pmod 3$, so this expression can never be a perfect square. $\square$

Solution 10

Consider the equation modulo 81. For $n \geq 9$, we have that $81 \mid n!$. Also, note that by computation,

$$\sum_{i=1}^{8} i! \equiv 63 \pmod{81}.$$

In particular, this means that for $n = 8$, the left side of the equation is $81j + 63$, and as noted above, this will in fact still be some $81j + 63$ for any $n \geq 8$ because we will only add multiples of 81.

But this means that for $n \geq 8$, the equation is $81j + 63 = m^k \implies 9(9j + 7) = m^k$. Note that the highest power of 3 dividing the left side is 3^2, which implies $k \leq 2$ (since $3 \mid m^k \implies 3 \mid m$, so then $k \leq 2$). It is given that $k \geq 2$, so $k = 2$.

Then, the solutions (see problem 5 from week 2) are $(n, m) = (3, 3), (1, 1)$, so the answer is $\boxed{(3,3,2),(1,1,k),k\geq 2}$ (we can easily verify that there exist no solutions with other k for $n \leq 7$). $\square$

Solution 11

First we consider the equation modulo p. By Fermat's little theorem, $3^p \equiv 3 \pmod 3$, so the equation becomes

$$3 - 4 \equiv m^2 \pmod p \implies -1 \equiv m^2 \pmod p.$$

Then, note that $(-1)^{\frac{p-1}{2}} \equiv (m^2)^{\frac{p-1}{2}} \pmod p$. But the right side simplifies to $m^{p-1} \equiv 1 \pmod p$. Hence we have $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. This means $\frac{p-1}{2}$ must be even, i.e. $p \equiv 1 \pmod 4$.

Now, considering the equation modulo 4 gives

$$7(1) + (-1)^p - 4 \equiv m^2 \pmod p \implies 7 - 1 - 4 \equiv 2 \equiv m^2 \pmod 4.$$

Note that $(-1)^p \equiv -1 \pmod 4$ because p is odd. So $m^2 \equiv 2 \pmod 4$. But this does not hold for any integer m, so there are in fact no solutions to the equation. $\square$

Solution 12

First note that if $5 \mid x$, then $x^2 \equiv 0 \pmod{25}$. Now we consider all other values of x modulo 25. To count the number of distinct values of x^2, we will see in what cases $x^2 \equiv y^2 \pmod{25}$ holds when $x \neq y$. From factoring this with difference of squares, this implies $25 \mid (x-y)(x+y)$. Note that since $5 \nmid y$, and since the two terms $x-y$ and $x+y$ differ by $2y$, they cannot both be multiples of 5. Hence one of them must be divisible by 25. But $x \neq y$, so we must have $25 \mid x+y$. That is, $x+y=25$, as we are picking x, y from $\{1, \dots, 24\}$.

The number of $x \in \{0, \dots, 24\}$ which are not multiples of 5 is 20, so this contributes 10 distinct perfect squares mod 25. Then, 0 is also a perfect square as noted in the beginning, so there are $\boxed{11}$ perfect squares mod 25 in total. $\square$

Solution 13

The answer is odd n. To show this, first consider any odd n; we must construct a complete residue class satisfying the desired condition. Let the set of a_i with $a_i = i$ for $0 \leq i \leq n-1$ be the complete residue class. Then, the set of $a_i + i$ contains all distinct numbers: if $a_i + i \equiv a_j + j \pmod{n}$, then since each $a_i = i$, this means $2i \equiv 2j \pmod{n}$. But then since n is odd, this simplifies to $i \equiv j \pmod{n}$ (note that this step does not hold when n is even). Since $i, j \in \{0, \dots, n-1\}$ this implies $i = j$, so we see that the set $\{a_0, a_1 + 1, \dots, a_{n-1} + n - 1\}$ in fact consists of n distinct numbers, implying that it is a complete residue class.

Also, we must show that even n do not satisfy the condition. Assume for the sake of contradiction that there does some exist some $\{a_i\}$ such that $\{a_i + i\}$ is also a complete residue classes. Then they contain the same elements in some (possibly different) permutation; in particular, this means that the sums of the elements for each set must be equal. That is,

$$\begin{aligned} \sum_{i=0}^{n-1} a_i &\equiv \sum_{i=0}^{n-1} (a_i + i) \pmod{n} \\ \implies 0 &\equiv \sum_{i=0}^{n-1} i \pmod{n} \\ \implies 0 &\equiv \frac{(n-1)n}{2} \pmod{n}. \end{aligned}$$

But note that for even n, $n-1$ is odd so then it is clear that $n \nmid (n-1)\frac{n}{2}$ by considering the power of 2 in each expression. Hence even n cannot satisfy the desired condition. $\square$

Solution 14

The answer is odd n. The solution is analogous to the above. For any odd n, to construct a residue class satisfying the condition, simply take the set of a_i with $a_i = i$ for each $0 \leq i \leq n-1$. Then, the set of a_i contains all distinct numbers due to the following: the i-th number in this set is $i + 3i = 4i$, so if $4i \equiv 4j \pmod{n}$, then since n is odd we can cancel the factor of 4 to obtain $i \equiv j \pmod{n}$. This cannot happen for distinct indices $0 \leq i, j \leq n-1$. So this implies all of the $a_i + i$ are distinct, meaning that $a_0, a_1 + 3, \dots, a_{n-1} + 3(n-1)$ is a complete residue class.

So, all odd n satisfy the condition. Now we show that even n do not work. Suppose that n satisfies the given condition. Then, there exists a complete residue class $\{a_i : 0 \leq i \leq n-1\}$ such that $\{a_i + 3i : 0 \leq i \leq n-1\}$

is also a complete residue class, so these two sets contain the same elements, in some (possibly different) orders. So, they have the same sum:

$$\begin{aligned}\sum_{i=0}^{n-1} a_i &\equiv \sum_{i=0}^{n-1}(a_i + 3i) \pmod{n} \\ \implies 0 &\equiv \sum_{i=0}^{n-1} 3i \pmod{n} \\ \implies 0 &\equiv \frac{3(n-1)n}{2} \pmod{n}.\end{aligned}$$

But for even n, $n-1$ is odd, so it is clear that $n \nmid 3(n-1)\frac{n}{2}$ by considering the power of 2 in each expression. Hence even n cannot satisfy the desired condition. □

Solution 15

No. Suppose $\{a_1, 2a_2, \ldots, (p-1)a_{p-1}\}$ is a complete residue class where $\{a_1, \ldots, a_{p-1}\}$ also is one. Then, since each of these sets are just some permutation of $\{1, \ldots, p-1\}$, we have that

$$\prod_{i=1}^{p-1} ia_i \equiv (p-1)! \equiv -1 \pmod{p},$$

where the last step is by Wilson's theorem; but also, note that

$$\prod_{i=1}^{p-1} ia_i \equiv \left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} a_i\right) \equiv (p-1)!(p-1)! \equiv 1 \pmod{p},$$

again by Wilson's theorem. So this implies that $-1 \equiv 1 \pmod{p}$, but this is not possible since $p > 2$. □