Tour Nine - Modular Arithmetic

Problem 9.1: *Determine the last digit of* 3^{1999}.

Since we wish to find the last digit, let us analyze modulo 10.

Notice that $3^4 \equiv 1 \pmod{10}$. Then,

$$\begin{aligned} 3^4 &\equiv 1 \pmod{10} \\ (3^4)^{499} &\equiv (1)^{499} \pmod{10} \\ 3^{1996} &\equiv 1 \pmod{10} \\ 3^{1996} \cdot 3^3 &\equiv 1 \cdot 3^3 \pmod{10} \\ 3^{1999} &\equiv 27 \pmod{10} \\ 3^{1999} &\equiv 7 \pmod{10} \end{aligned}$$

Thus, 3^{1999} gives a remainder of 7 when divided by 10. This implies that the last digit of 3^{1999} is a 7.

Problem 9.2: *What is the rule for divisibility by* 9*? Prove it! Similarly, state and prove the rule for divisibility by* 11.

The rule for divisibility by 9 is that an integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.

Every integer n can be written in the form $a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$. For example, $1304 = 1 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 4 \cdot 10^0$.

Since $10^k \equiv 1^k = 1 \pmod{9}$, we have

$$\begin{aligned} n &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \\ &\equiv a_k \cdot 1^k + a_{k-1} \cdot 1^{k-1} + \ldots + a_2 \cdot 1^2 + a_1 \cdot 1^1 + a_0 \cdot 1^0 \pmod{9} \\ &\equiv a_k + a_{k-1} + \ldots + a_2 + a_1 + a_0 \pmod{9} \end{aligned}$$

Thus, n is congruent to the sum of its digits, modulo 9. Hence, n is divisible by 9 if and only if the sum of its digits is divisble by 9.

The rule for divisibility by 11 is that n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. For example, 12348809 is divisible by 11 because the alternating sum $1 - 2 + 3 - 4 + 8 - 8 + 0 - 9 = -11$ is divisible by 11. Proving this is the exact same idea as above, except now we use the fact that $10^k \equiv (-1)^k \pmod{11}$.

Problem 9.3: *Show that* $4^{3n+1} + 2^{3n+1} + 1$ *is divisible by* 7 *for all positive integers* n.

We could prove this by mathematical induction, but we can use modular arithmetic to find a more elegant solution. Since we want to prove that some expression is divisible by 7, let us analyze the problem in modulo 7, and show that $4^{3n+1} + 2^{3n+1} + 1$ is always congruent to 0 modulo 7. By definition, this will prove that $4^{3n+1} + 2^{3n+1} + 1$ is divisible by 7.

Since $4^3 = 64 \equiv 1 \pmod 7$, we have

$$\begin{aligned} 4^3 &\equiv 1 \pmod 7 \\ (4^3)^n &\equiv (1)^n \pmod 7 \\ 4^{3n} &\equiv 1 \pmod 7 \\ 4^{3n} \cdot 4 &\equiv 1 \cdot 4 \pmod 7 \\ 4^{3n+1} &\equiv 4 \pmod 7 \end{aligned}$$

Thus $4^{3n+1} \equiv 4 \pmod 7$, for all positive integers n. Similarly,

$$\begin{aligned} 2^3 &\equiv 1 \pmod 7 \\ (2^3)^n &\equiv (1)^n \pmod 7 \\ 2^{3n} &\equiv 1 \pmod 7 \\ 2^{3n} \cdot 2 &\equiv 1 \cdot 2 \pmod 7 \\ 2^{3n+1} &\equiv 2 \pmod 7 \end{aligned}$$

Thus, $2^{3n+1} \equiv 2 \pmod 7$. Hence, we have

$$4^{3n+1} + 2^{3n+1} + 1 \equiv 4 + 2 + 1 \equiv 0 \pmod 7.$$

Therefore, we have proven that $4^{3n+1} + 2^{3n+1} + 1$ is divisible by 7 for all positive integers n.

Problem 9.4: *Pick any* 55 *numbers from the set* $\{1, 2, 3, \ldots, 100\}$. *Prove that among those* 55 *numbers, you can find two of them that differ by* 9.

Here is a nice solution involving modular arithmetic and two applications of the Pigeonhole Principle. Split the first 100 integers into nine different pigeonholes, according to their remainder upon division by 9. So in the first pigeonhole put all the numbers that are congruent to 0 modulo 9, namely $9, 18, 27, 36, \ldots, 99$. In the second pigeonhole put all the numbers that are congruent to 1 modulo 9, in the third put all numbers congruent to 2 modulo 9, and so on. Formally, we say that we are partitioning the 100 integers into nine "congruence classes".

In each pigeonhole, pair off the numbers. For example, in the first pigeonhole, we have $(9, 18), (27, 36), (45, 54), (63, 72), (81, 90), (99)$. Every pigeonhole except for the second one (the pigeonhole containing the numbers $1, 10, 19, 28, \ldots, 100$) contain eleven numbers, while this second pigeonhole contains twelve numbers. Since every pigeonhole has eleven or twelve numbers, there will be exactly six "pairs" in each pigeonhole.

Now if we select 55 of these numbers from these 9 pigeonholes, by the Pigeonhole Principle, at least 7 of these numbers must belong to the same pigeonhole. Within this pigeonhole, there are 6 pairs. Now let's use the Pigeonhole Principle again. We have 7 numbers being placed into 6 pairs, and so two of these numbers must belong to the same pair. In each pair, the numbers differ by 9, and so we have proven that there must exist two numbers that differ by 9.

Note: If we choose 54 numbers instead of 55, it is not necessarily true that two of these numbers must differ by 9. That is because we can choose our 54 numbers such that there are six numbers in each pigeonhole, with the condition that each consecutive pair differed by 18. (For example, $9, 27, 45, 63, 81, 99$). Then no two numbers will have a difference of 9.

Problem 9.5: *Prove Fermat's Little Theorem: if p is prime and a is not divisible by p, show that $a^{p-1} \equiv 1 \pmod{p}$.*

Consider the integers $\{a, 2a, 3a, \ldots, (p-1)a\}$. We will show that these $p-1$ integers must be a permutation of $1, 2, 3, \ldots, p-1$, when reduced modulo p.

First we show that no two integers from this set are congruent modulo p. To do this, we will use a contradiction argument. Suppose that $ja \equiv ka \pmod{p}$ for some integers j and k, with $1 \leq j < k \leq p-1$. (By symmetry, we can assume that $j < k$). Then, $(k-j)a \equiv 0 \pmod{p}$. Since $(k-j)a$ is divisible by p, where p is prime, either $k-j$ or a (or both!) must be divisible by p. However, we are given in the question that a is not divisible by p, and furthermore, $1 \leq k-j \leq p-2$ because k is at most $p-1$ and j is at least 1. Since there are no multiples of p between 1 and $p-2$, it follows that $k-j$ cannot be divisible by p either. Since $k-j$ and a are not divisible by p, clearly their product cannot be either. This contradicts the fact that $(k-j)a \equiv 0 \pmod{p}$. Hence, no two integers from this set are congruent modulo p.

Secondly, no integer from this set is congruent to 0 modulo p. For if $ka \equiv 0$ modulo p for some k between 1 and $p-1$, then a would have to be divisible by p, since k clearly is not. But a is not divisible by p, as specified in the question. Hence, no integer from the set $\{a, 2a, 3a, \ldots, (p-1)a\}$ is congruent to 0 modulo p. Thus, each element in this set must give a remainder of $1, 2, 3, \ldots$, or $p-1$, when divided by p.

So we have $p-1$ elements in the set, and $p-1$ possible remainders. But we showed that no two elements in the set are congruent modulo p, and so no two elements in the set can have the same remainder when divided by p. In other words, each element must have a unique remainder, so it follows that when the set $\{a, 2a, 3a, \ldots, (p-1)a\}$ is reduced modulo p, we must get a permutation of $\{1, 2, 3, \ldots, p-1\}$.

Thus, if we multiply the elements in these two sets, they must be congruent modulo p, since one is just a permutation of the other. So,

$$\begin{aligned}
a \cdot 2a \cdot 3a \cdots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\
a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\
a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\
a^{p-1}(p-1)! - (p-1)! &\equiv 0 \pmod{p} \\
(p-1)!(a^{p-1}-1) &\equiv 0 \pmod{p}
\end{aligned}$$

Thus, we have shown that $(p-1)!(a^{p-1}-1)$ must be divisible by p. Since p is prime, either $(p-1)!$ or $a^{p-1}-1$ (or both) must be divisible by p. Now $(p-1)!$ is the product of the first $p-1$ integers, and because p is prime, none of these $p-1$ integers is divisible by p. Hence, their product cannot be divisible by p. So, $(p-1)!$ is not divisible by p, and thus it follows that $a^{p-1}-1$ must be divisible by p.

Therefore, $a^{p-1} - 1 \equiv 0 \pmod{p}$, so $a^{p-1} \equiv 1 \pmod{p}$, as required.