Tour Ten - More Magnificent Modular Arithmetic

Problem 10.1: *Determine whether the number* $1234 \cdot 56 + 789 \cdot 100$ *is divisible by* 3.

Let this number equal S.

Given the context of this problem, it makes sense to analyze in mod 3. We have $1234 \equiv 1 \pmod 3$, $56 \equiv 2 \pmod 3$, $789 \equiv 0 \pmod 3$, and $100 \equiv 1 \pmod 3$. Therefore, we have

$$\begin{aligned} S &= 1234 \cdot 56 + 789 \cdot 100 \\ &\equiv 1 \cdot 2 + 0 \cdot 1 \pmod 3 \\ &\equiv 2 + 0 \pmod 3 \\ &\equiv 2 \pmod 3 \end{aligned}$$

Thus, S is not divisible by 3, since the remainder when S divided by 3 is two.

Problem 10.2: *i) If* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$, *prove that* $a + c \equiv b + d \pmod m$.
ii) If $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$, *prove that* $ac \equiv bd \pmod m$.
iii) If $a \equiv b \pmod m$, *then prove that* $a^n \equiv b^n \pmod m$, *for all integers* $n \geq 1$.

Let $a = km + b$ and $c = lm + d$ for some integers k and l.

Then $a + c = (km + b) + (lm + d) = m(k + l) + (b + d)$, and so by definition, we have $a + c \equiv b + d \pmod m$.

Also, $ac = (km + b)(lm + d) = klm^2 + m(bl + kd) + bd \equiv 0 + 0 + bd \equiv bd \pmod m$.

Finally, to prove iii), we use ii). Letting $c = a$ and $d = b$, we have $a \cdot a \equiv b \cdot b \pmod m$, so $a^2 \equiv b^2 \pmod m$. Using this, and the fact that $a \equiv b \pmod m$, we get $a^3 \equiv b^3 \pmod m$, from ii). And we can repeat this process indefinitely. (For a more rigorous treatment, we can use mathematical induction).

Problem 10.3: *Prove that* $2^{70} + 3^{70}$ *is divisible by* 13.

From the context of this problem, clearly we want to analyze in mod 13. Our goal is to show that $2^{70} + 3^{70} \equiv 0 \pmod{13}$, and then we are done.

Let's do 3^{70} first, since that is surprisingly easier. Notice that $3^3 \equiv 1 \pmod{13}$. Thus, we have $(3^3)^{23} \equiv 1^{23} = 1 \pmod{13}$. Since $3^{69} \equiv 1 \pmod{13}$, we get $3^{70} \equiv 3 \pmod{13}$, after we multiply both sides by 3.

Now let's do 2^{70}. If we notice that $2^{12} \equiv 1 \pmod{13}$ (Note: this is immediate by Fermat's Little Theorem), this comes out quite quickly. But let's say we didn't know that. That is okay.

Let's start with 2^5. We have $2^5 \equiv 6 \pmod{13}$.

Square both sides. We get $2^{10} \equiv 6^2 \equiv 10 \pmod{13}$.

Square both sides again. We get $2^{20} \equiv 10^2 \equiv 9 \pmod{13}$.

Do it once more. We get $2^{40} \equiv 9^2 \equiv 3 \pmod{13}$.

Thus, we have $2^{70} = 2^{40} \cdot 2^{20} \cdot 2^{10} \equiv 3 \cdot 9 \cdot 10 \equiv 270 \equiv 10 \pmod{13}$.

Therefore, we have proven that $2^{70} + 3^{70} \equiv 10 + 3 \equiv 0 \pmod{13}$, as required.

The solutions to the other problems from this tour can be found in Chapter 9.