Problems IV

18. Solve the linear diophantine equation

\[ 6m + 10n + 15p = 1 \]

**Solution:** Let \( y = 10n + 15p \). Since \((10, 15) = 5\), we must have that \( y = 5x \) for some integer \( x \), and (as we shall see) we can find a solution in \( n \) and \( p \) for any \( x \). Thus, we start by solving

\[ 6m + 5x = 1 \]

by our usual technique. In this case we can use the readily apparent particular solution \( m_0 = 1, x = -1 \), and since 6 and 5 are already coprime we conclude that the general solution will be \( m = 1 - 5q_1, x = -1 + 6q_1 \) for \( q_1 \in \mathbb{Z} \). Next, we must solve the equation

\[ 10n + 15p = 5x \]

which is the same as solving

\[ 2n + 3p = x \]

Again, we can find a solution without much effort: \( n_0 = -x, p_0 = x \) will do. We already have divided by the gcd, so it is no surprise that 2 and 3 are coprime, and the general solution is \( n = -x + 3q_2, p = x - 2q_2 \) (with \( q_2 \in \mathbb{Z} \), of course). Substituting our solution for \( x \) from the previous paragraph, we get that the desired solutions to the original equation have the general form

\[ m = 1 - 5q_1, n = 1 - 6q_1 + 3q_2, p = -1 + 6q_1 - 2q_2 \]

19. **Prove that if there are no non-zero integer solutions to the equation \( x^n + y^n = z^n \) then there are no non-zero rational solutions.**

[Prove the contrapositive: show how a rational solution lead to an integer solutions]
Solution: Following the hint, it’s enough to prove the contrapositive. So suppose $x, y,$ and $z$ are a nonzero rational solution to $x^n + y^n = z^n$. Since they are rational numbers, we can let $x = \frac{x_1}{x_2}, y = \frac{y_1}{y_2}$, and $z = \frac{z_1}{z_2}$, where the $x_i, y_i,$ and $z_i$ are integers with $x_2, y_2, z_2 \neq 0$.

This means that

\[ \left( \frac{x_1}{x_2} \right)^2 + \left( \frac{y_1}{y_2} \right)^2 = \left( \frac{z_1}{z_2} \right)^2 \]

and clearing denominators, we get that

\[ x_1^2 y_2^2 z_2^2 + y_1^2 x_2^2 z_2^2 = z_1^2 x_2^2 y_2^2 \]

In other words,

\[ (x_1 y_2 z_2)^2 + (y_1 x_2 z_2)^2 = (z_1 x_2 y_2)^2 \]

so we have a nonzero (since we are multiplying the numerators—one of which is nonzero—by the nonzero denominators) integer solution.

Problems V

1. Prove, for positive integers $n$, that 7 divides $6^n + 1$ if and only if $n$ is odd.

Solution: 6 is congruent to -1 modulo 7, so

\[ 6^n + 1 \equiv (-1)^n + 1 \text{ (mod 7)} \]

which is 1 + 1 = 2 if $n$ is even and $-1 + 1 = 0$ if $n$ is odd. By the definition of congruence, this proves our result.

2. Prove that, for all integers $a$ and $b$, $a^2 + b^2 \equiv 0, 1, 2, 4 \text{ or } 5$ modulo 8. Deduce that there do not exist integers $a$ and $b$ such that $a^2 + b^2 = 12345790$.

Solution: We can check that the squares modulo 8 are 0, 1, and 4. Thus (since $4 + 4 \equiv 0$ as well) the possibilities are

\[ a^2 + b^2 \equiv 0 + 0 = 0 \]
\[ \equiv 0 + 1 = 1 \]
\[ \equiv 1 + 1 = 2 \]
\[ \equiv 0 + 4 = 4 \]
\[ \equiv 1 + 4 = 5 \]

12345790 is 6 mod 8, so it cannot have this form.

4. Suppose that a positive integer is written in decimal notation as $n = a_k a_{k-1} \cdots a_2 a_1 a_0$ where $0 \leq a_i \leq 9$. Prove that $n$ is divisible by 11 if and only if the alternating sum of its digits $a_0 - a_1 + \cdots + (-1)^k a_k$ is divisible by 11.
**Solution:** By assumption, we can write \( n = \sum_{i=0}^{k} a_i 10^i \). Being divisible by 11 is the same as being 0 mod 11, so we reduce this equation mod 10. But 10 \( \equiv -1 \) (mod 11), which yields

\[
n \equiv \sum_{i=0}^{k} a_i (-1)^i \pmod{11}
\]

This shows that the left hand side is 0 mod 11 if and only if the right hand side is, which is what we want.

6. **Prove that the diophantine equation** \( 3x^2 + 4y^2 = 5z^2 \) **has no non-trivial (ie, \((x, y, z) \neq (0, 0, 0)) \) solutions.**

**[Give a proof by contradiction. Obtain a contradiction by proving that if there is a non-trivial solution then there is a solution \((x_1, y_1, z_1) \) with \( x_1 \neq 0 \) mod 5 or \( y_1 \neq 0 \) mod 5.]**

**Deduce that the equation** \( 3x^2 + 4y^2 = 5z^2 \) **has no rational solutions.**

**Solution:** If \((x, y, z)\) is a nontrivial solution, we claim that one of \( x \) or \( y \) must be nonzero, as if they both are, then \( z = 0 \) as well. Now if 5 divides both \( x \) and \( y \), we substitute \( x = 5k, y = 5\ell \) \((k, \ell \in \mathbb{Z})\) to get

\[
3 \cdot 25k^2 + 4 \cdot 25\ell^2 = 5z^2
\]

Dividing by 5, we have

\[
3 \cdot 5k^2 + 4 \cdot 5\ell^2 = z^2
\]

The terms on the left hand side are both divisible by 5, so \( z^2 \), and hence \( z \) by an earlier homework problem, must be as well. This means that we can replace \((x, y, z)\) with \((\frac{x}{5}, \frac{y}{5}, \frac{z}{5})\) and still have a solution to the original equation. Repeating the process enough times to get rid of all the powers of 5 (which is possible, since one of them is nonzero) we can assume that one of \( x \) or \( y \) is not divisible by 5. So assume without loss of generality that \( x \neq 0 \) (mod 5). If we reduce the original equation mod 5, we see that

\[
3x^2 - y^2 \equiv 0 \pmod{5}
\]

or

\[
3x^2 \equiv y^2 \pmod{5}
\]

If \( x \neq 0 \) (mod 5), then \( x \) and 5 must be coprime (since 5 is a prime number), which means that there exists \( a, b \in \mathbb{Z} \) such that \( ax + 5b = 1 \). This means that \( ax \equiv 1 \) (mod 5); ie, \( x \) has an inverse mod 5. Multiplying both sides of the congruence by \( a^2 \) then yields

\[
3 \equiv (ay)^2 \pmod{5}
\]

so 3 is a square mod 5. If instead \( y \neq 0 \) (mod 5), then we can use the same trick (multiplying the equation by 3’s inverse mod 5, 2) to get that 2 is a square mod 5. Both cases provide a contradiction, so there can be no nontrivial solution to \( 3x^2 + 4y^2 = 5z^2 \).
Now if $3x^2 + 4y^2 = 5$ has a rational solution, then clearing denominators as in problem 19 shows that $3x^2 + 4y^2 = 5z^2$ has a nontrivial integer solution, which we have just shown to be impossible. Therefore there are no solutions to this equation.

7. What is the last digit of $2^{1000}$?

Solution: The last digit of $2^{1000}$ is the same as the remainder of $2^{1000}$ mod 10. First of all,

\[
2^{1000} \equiv (2^4)^{250} \\
\equiv 16^{250} \\
\equiv 6^{250} \pmod{10}
\]

But $6 \cdot 6 \equiv 6 \pmod{10}$ as well, and therefore (by induction, if you like) so is any positive power of 6. Thus the last digit is 6.

9. Solve the following linear congruences:

(ii) $3x \equiv 16 \pmod{18}$

Solution: $(3, 18) = 3$ does not divide 16, so there are no solutions.

10. Solve the following linear congruences:

(i) $23x \equiv 16 \pmod{107}$

Solution: Luckily, we can see easily that $23 \cdot 5 \equiv 8 \pmod{107}$, so $x \equiv 10$ is certainly a solution. But 23 and 107 are coprime, so this must be the unique solution mod 5 (for example, because if $x$ is any other solution, we can multiply $23x \equiv 23 \cdot 10$ by an inverse of 23 mod 107 to get that $x \equiv 10 \pmod{107}$).

(ii) $234x \equiv 20 \pmod{366}$

Solution: All of these numbers at least share a common factor of two, so it is equivalent to solve $117x \equiv 10 \pmod{183}$. But 117 and 183 are both divisible by 3, so there are no solutions as 10 is not divisible by 3.

(iii) $234x \equiv 6 \pmod{366}$

Solution: Using the calculations in the previous problem, we can see that it’s equivalent to solve $39x \equiv 1 \pmod{61}$. As usual, we can do this with the Euclidean algorithm, which tells us

\[
\begin{align*}
61 &= 39 + 22 \\
39 &= 22 + 17 \\
22 &= 17 + 5 \\
17 &= 3 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1
\end{align*}
\]
Working backwards from this, we find that $16 \cdot 61 - 25 \cdot 39 = 1$, so $x \equiv -25 \pmod{61}$, or $x \equiv 36 \pmod{61}$.

To find the solutions mod 366, we just add every possible multiple of 61 to 36 up to $5 \cdot 61$ (since adding 366 = $6 \cdot 61$ does not change the value mod 366). These are then $x \equiv 36, 97, 158, 219, 280, \text{ or } 341 \pmod{366}$.

(iv) $234x \equiv 36 \pmod{366}$

**Solution:** One solution mod 61 can be found from the previous problem, which says we can take $x \equiv 36 \cdot 6 \equiv 33 \pmod{61}$. Since 61 and 39 are coprime, this is the only solution mod 61. As before, this means that $x \equiv 33, 94, 155, 216, 277, \text{ or } 338 \pmod{366}$. 