

Tour Eleven - Quadratic Residues

The hardest part of each of these questions is figuring out which mod to use. Once you figure that out, the solution is usually very concise and elegant.

Problem 11.1: *Determine all solutions in integers x and y to the equation $x^2 + y^2 = 2003$.*

Let's analyze in mod 4. The quadratic residues modulo 4 are 0 and 1. In other words, for any integer x , x^2 must be congruent to either 0 or 1 (mod 4). Similarly, y^2 must be congruent to either 0 or 1 (mod 4). Therefore, $x^2 + y^2$ must be congruent to 0, 1, or 2 (mod 4). However, $2003 \equiv 3 \pmod{4}$, and so $x^2 + y^2 = 2003$ cannot have any solutions in integers x and y .

Problem 11.2: *Prove that the sequence $\{11, 111, 1111, 11111, \dots\}$ contains no perfect squares.*

Let's analyze in mod 4. How does one figure out to use mod 4? Well, you don't. You just have to try different possibilities (mod 3, mod 10, etc.) until you finally get something that works. That's an often painful and frustrating part of the problem-solving process!

Since the last two digits of each term is 11, every term in the sequence can be written in the form $100x + 11$, for some integer x . Since $100x + 11 \equiv 3 \pmod{4}$, every term in the sequence is congruent to 3 modulo 4. However, the quadratic residues modulo 4 are 0 and 1, and thus, no number that is congruent to 3 (mod 4) can be a perfect square. Hence, the sequence $\{11, 111, 1111, 11111, \dots\}$ contains no perfect squares.

Problem 11.3: *If $a^2 + b^2$ is a multiple of 7, prove that a and b must both be multiples of 7.*

Given the context of the question, it seems natural to analyze this problem in mod 7. The quadratic residues modulo 7 are 0, 1, 2, and 4. Therefore, a^2 must be congruent to 0, 1, 2, or 4 (mod 7). Similarly, b^2 must be congruent to 0, 1, 2, or 4 (mod 7).

Since $a^2 + b^2$ is a multiple of 7, we have $a^2 + b^2 \equiv 0 \pmod{7}$.

If $a^2 \equiv 1 \pmod{7}$, then $b^2 \equiv 6 \pmod{7}$, and that is a contradiction.

If $a^2 \equiv 2 \pmod{7}$, then $b^2 \equiv 5 \pmod{7}$, and that is a contradiction.

If $a^2 \equiv 4 \pmod{7}$, then $b^2 \equiv 3 \pmod{7}$, and that is a contradiction.

Thus, we must have $a^2 \equiv 0 \pmod{7}$, and so $b^2 \equiv 0 \pmod{7}$. If a^2 is a multiple of 7, because 7 is a prime, it follows that a must be a multiple of 7 as well. Similarly, b must be a multiple of 7. Thus, if $a^2 + b^2$ is a multiple of 7, then a and b must both be multiples of 7.

Problem 11.4: *Find all solutions in positive integers to the equation $x^2 - 2y^2 = 3$.*

Let's analyze in mod 3. Then $x^2 - 2y^2 = 3$ becomes $x^2 + y^2 \equiv 0 \pmod{3}$. The quadratic residues modulo 3 are 0 and 1. Hence, $x^2 \equiv 0 \pmod{3}$ or $x^2 \equiv 1 \pmod{3}$, and similarly with y^2 . Since $x^2 + y^2 \equiv 0 \pmod{3}$, this implies that we must have $x^2 \equiv 0 \pmod{3}$ and

$y^2 \equiv 0 \pmod{3}$. But 3 is prime, and so if x^2 is a multiple of 3, then that must mean that x is a multiple of 3 as well. Similarly, y must be a multiple of 3.

Thus, $x = 3a$ and $y = 3b$, for some positive integers a and b . Then substituting into our original equation, we get $(3a)^2 - 2(3b)^2 = 3$, which simplifies to $3a^2 - 6b^2 = 1$. Dividing both sides by 3, we get $a^2 - 2b^2 = \frac{1}{3}$. Since a and b are both integers, $a^2 - 2b^2$ is an integer as well, and so it can never equal $\frac{1}{3}$. Thus, there are no solutions in integers to $a^2 - 2b^2 = \frac{1}{3}$, and therefore, we conclude that there are no solutions in integers to $x^2 - 2y^2 = 3$.

Problem 11.5: *If $2n + 1$ and $3n + 1$ are both perfect squares, show that n must be divisible by 40.*

Let $2n + 1 = a^2$ and $3n + 1 = b^2$, where a and b are positive integers. We will show that n must be divisible by 5 and 8.

The quadratic residues modulo 5 are 0, 1, and 4. Thus, $2n + 1$ is congruent to either 0, 1, or 4 (mod 5). Similarly with $3n + 1$. Suppose there exists an n satisfying the given conditions, where n is *not* divisible by 5. We consider four cases:

- If $n \equiv 1 \pmod{5}$, then $a^2 = 2n + 1 \equiv 3 \pmod{5}$, a contradiction.
- If $n \equiv 2 \pmod{5}$, then $b^2 = 3n + 1 \equiv 2 \pmod{5}$, a contradiction.
- If $n \equiv 3 \pmod{5}$, then $a^2 = 2n + 1 \equiv 2 \pmod{5}$, a contradiction.
- If $n \equiv 4 \pmod{5}$, then $b^2 = 3n + 1 \equiv 3 \pmod{5}$, a contradiction.

Thus, if $2n + 1$ and $3n + 1$ are both perfect squares, then n must be divisible by 5. (Note: the converse does not hold - if n is divisible by 5, then $2n + 1$ and $3n + 1$ do not necessarily have to be perfect squares).

Let's show n must be divisible by 8. The quadratic residues modulo 8 are 0, 1, and 4. Suppose that n is *not* divisible by 8. We consider seven cases:

- If $n \equiv 1 \pmod{8}$, then $a^2 = 2n + 1 \equiv 3 \pmod{8}$, a contradiction.
- If $n \equiv 2 \pmod{8}$, then $a^2 = 2n + 1 \equiv 5 \pmod{8}$, a contradiction.
- If $n \equiv 3 \pmod{8}$, then $a^2 = 2n + 1 \equiv 7 \pmod{8}$, a contradiction.
- If $n \equiv 4 \pmod{8}$, then $b^2 = 3n + 1 \equiv 5 \pmod{8}$, a contradiction.
- If $n \equiv 5 \pmod{8}$, then $a^2 = 2n + 1 \equiv 3 \pmod{8}$, a contradiction.
- If $n \equiv 6 \pmod{8}$, then $a^2 = 2n + 1 \equiv 5 \pmod{8}$, a contradiction.
- If $n \equiv 7 \pmod{8}$, then $a^2 = 2n + 1 \equiv 7 \pmod{8}$, a contradiction.

Thus, if $2n + 1$ and $3n + 1$ are both perfect squares, then n must be divisible by 8.

Since we have shown that n must be divisible by 5 and by 8, we have shown that n must be divisible by 40.

Problem 11.6: *If a , b , and c are odd integers, prove that the polynomial $ax^2 + bx + c$ has no rational roots.*

In Tour 1, we solved this question using parity. Let's use quadratic residues to solve this problem.

Suppose there is a rational root. We will establish a contradiction. By the quadratic formula (hah, thought you'd never use that ever again!), we have $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. If there

are rational roots, then the discriminant, $b^2 - 4ac$ must be a perfect square. Let's analyze this in mod 8.

So $b^2 - 4ac = n^2$, for some integer n . Since a , b , and c are odd, $b^2 - 4ac$ is the difference of an odd number and an even number, so n^2 will be odd. So it follows that n is odd as well. Thus, b and n are both odd integers. Rewrite this equation as $4ac = b^2 - n^2$. First, we'll prove that b^2 and n^2 must be congruent to 1 (mod 8).

If you take any odd integer (say $2k + 1$) and square it, you get $(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1 = 8 \cdot \frac{k(k+1)}{2} + 1$. Now, $\frac{k(k+1)}{2}$ is an integer for each value of k (do you see why this is true?), and so $(2k + 1)^2 = 8 \cdot \frac{k(k+1)}{2} + 1 \equiv 1 \pmod{8}$. So the square of every odd number is congruent to 1 (mod 8).

To illustrate this another way, recall that the quadratic residues modulo 8 are 0, 1, and 4. If we take the square of an odd number, we get an odd number. When we divide this odd number by 8, we must have an *odd* remainder. This odd remainder must be 0, 1, or 4, and so it follows that this remainder must be 1 (since 0 and 4 are both even). So this is another way to show that the square of an odd number must be congruent to 1 (mod 8).

Since b and n are both odd, $b^2 \equiv 1 \pmod{8}$ and $n^2 \equiv 1 \pmod{8}$. Therefore, $b^2 - n^2 \equiv 1 - 1 \equiv 0 \pmod{8}$. Since $4ac = b^2 - n^2$, it follows that $4ac \equiv 0 \pmod{8}$. So $4ac$ is divisible by 8, i.e., ac is divisible by 2. If ac is divisible by 2, then one of a or c (or both) must be even. However, this contradicts the given information that a and c are both odd.

Therefore, we have a contradiction and so the roots of this quadratic equation cannot be rational.

Problem 11.7: Find all solutions in integers to the equation $x^2 + y^2 = 3z^2$.

If we analyze in mod 3, one of the variables will disappear, so this seems like a natural thing to try. We find that $x^2 + y^2 \equiv 0 \pmod{3}$, and from the analysis in Problem 11.1, we must have x and y both being multiples of 3, and so $x = 3a$ and $y = 3b$ for some integers a and b . Substituting into our original equation, we have:

$$\begin{aligned} x^2 + y^2 &= 3z^2 \\ (3a)^2 + (3b)^2 &= 3z^2 \\ 9a^2 + 9b^2 &= 3z^2 \\ 3a^2 + 3b^2 &= z^2 \\ 3(a^2 + b^2) &= z^2 \end{aligned}$$

Thus, z^2 is a multiple of 3, so once again, z must be a multiple of 3 as well (since 3 is prime). Let $z = 3c$ for some integer c . Then, $3(a^2 + b^2) = (3c)^2 = 9c^2$, so $a^2 + b^2 = 3c^2$, which is the same form as our original equation.

Now, we know that a , b , and c are integers, with $a = \frac{x}{3}$, $b = \frac{y}{3}$, and $c = \frac{z}{3}$. Thus, we have shown that if (x, y, z) is an *integer* solution to the equation, then $(\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ is an *integer* solution as well. We will prove that there are no solutions in non-zero integers to the equation.

Suppose there is a solution (x, y, z) where z is a non-zero integer. Then we can divide all three of these variables by 3 to produce another integer solution. Since this is an integer

solution, we can once again divide all three variables by 3, and continue repeating this process. Since z is a finite integer, eventually we will reach a point where this term becomes a fraction if we continue to divide by 3. For a more formal approach, let 3^k be the highest power of 3 that divides z . Then $z = 3^k \times r$, where r is some integer that is not divisible by 3. Then if we repeat this process $k + 1$ times, z becomes $\frac{r}{3}$, which is not an integer. And that contradicts the fact that $(\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ is an *integer* solution to the equation. Thus, there cannot be a solution (x, y, z) , where z is a non-zero integer. Our only hope for a solution is when $z = 0$. In this case, we have $x^2 + y^2 = 3z^2 = 0$, and this clearly implies that $x = y = 0$. Thus, we conclude that there is only one solution, namely $(x, y, z) = (0, 0, 0)$.

For another approach to show that there is no solution (x, y, z) where z is a non-zero integer, consider the following argument. Suppose there are solutions (x, y, z) to the equation, where z is a non-zero integer. Just consider those solutions with $z > 0$, because if (x, y, z) is a solution to the equation, clearly so is $(x, y, -z)$. Consider the solution for which z is *least* (i.e., consider the smallest solution). Let this solution be (r, s, t) . In other words, these three integers satisfy $r^2 + s^2 = 3t^2$, and there is no other triple (x, y, z) satisfying the equation where $z < t$. Then by our analysis above, r , s , and t must all be multiples of 3, and so $(\frac{r}{3}, \frac{s}{3}, \frac{t}{3})$ is also a solution to the equation.

But because $t \neq 0$, we have $\frac{t}{3} < t$, and this contradicts the minimality of t . Hence, there cannot be a *smallest* solution, and so there is no solution, period. As before, we only have to consider the case $z = 0$, and we conclude that $x = y = z = 0$ is the only solution.