Number Theory — Misha Lavrov

Diophantine equations

Western PA ARML Practice — *October 4, 2015*

1 Exponential Diophantine equations

Diophantine equations are just equations we solve with the constraint that all variables must be integers. These are generally really hard to solve (for example, the famous Fermat's Last Theorem is an example of a Diophantine equation).

Today, we will begin by focusing on a special kind of Diophantine equation: exponential Diophantine equations. Here's an example.

Example 1. *Solve* $5^x - 8^y = 1$ *for integers* x *and* y*.*

These can still get really hard, but there's a special technique that solves them most of the time. That technique is to take the equation modulo m.

In this example, if $5^x - 8^y = 1$, then in particular $5^x - 8^y \equiv 1 \pmod{21}$. But what do the powers of 5 and 8 look like modulo 21? We have:

- $5^x \equiv 1, 5, 4, 20, 16, 17, 1, 5, 4, \ldots$, repeating every 6 steps.
- $8^y \equiv 1, 8, 1, 8, \ldots$, repeating every 2 steps.

So there are only 12 possibilities for $5^x - 8^y$ when working modulo 21. We can check them all, and we notice that $1 - 1, 1 - 8, 5 - 1, 5 - 8, \ldots, 17 - 1, 17 - 8$ are not ever equal to 1. So the equation has no solutions.

Okay, but there's a magic step here: how did we pick 21?

Example 2. *Solve* $5^x - 8^y = 1$ *for integers* x *and* y*, but in a way that's not magic.*

There are several rules to follow for picking the modulus m. The first is one we've already broken:

Rule 1: Choose m to be a prime or a power of a prime.

The reason is that taking an equation modulo 21 gives you no extra information over knowing it modulo 3 and modulo 7. But calculations with 3 and 7 are easier, so we might as well stick to those. Okay, but which primes?

Rule 2: Choose m so that one or more powers repeat in only a few steps.

More precisely, if $m \mid a - 1$, then $a \equiv 1 \pmod{m}$, so powers of a will always be constant. If $m \mid a^2 - 1$, then $a^2 \equiv 1 \pmod{m}$, so powers of a repeat every two steps. If $m \mid a^3 - 1$, then powers of a repeat every three steps, and so on.

Choosing m so that $m \mid a$ is also useful, but a bit tricky: we'll consider this later on.

In this example, we should consider $m = 4$ first, since $4 \mid 8$ and $4 \mid 5 - 1$, but that doesn't help: since $5^x \equiv 1 \pmod 4$ and $8^y \equiv 0 \pmod 4$ for most y, we get the equation $1 - 0 \equiv 1 \pmod 4$, which is always true. (Of course, if it turned out to be false, we'd be done really quickly.)

Next, let's try $m = 7$, since $7 \mid 8 - 1$, so 8^y simplifies to $1^y = 1$ modulo 7. We get

$$5^x - 1 \equiv 1 \pmod 7$$

so $5^x \equiv 2 \pmod 7$. The powers of 5 modulo 7 are $1, 5, 4, 6, 2, 3, \ldots$, repeating every 6 steps, so x can be 4 or 10 or 16 or 22 or .... In particular, x is even, and we can write the original equation as

$$25^{x/2} - 8^y = 1.$$

Now taking $m = 3$ is very appealing, because $3 \mid 25 - 1$ and $3 \mid 8^2 - 1$. We get

$$1^{x/2} - (-1)^y \equiv 1 \pmod 3$$

which is impossible to satisfy, since $1 - (-1)^y$ is always either 0 or 2. So, once again, we've shown that there are no solutions.

Example 3. *Solve $4^x + 5^y = 6^z$ for integers x, y, and z.*

As a counterpoint, here is an example with a solution: $4^0 + 5^1 = 6^1$. (If we didn't spot this solution, proceeding as before would help us, telling us things such as "x is odd" or "y is a multiple of 3".) At this point, we want to proceed differently. We can't hope to show there are no solutions, because there is one. We want to show it's the only one.

Rule 3: After finding a solution, choose m to reduce a power to 0.

In this case, suppose we take the equation modulo 4. If $x \neq 0$, then $4^x \equiv 0 \pmod 4$, and we get

$$0 + 1^y \equiv 6^z \pmod 4.$$

This is impossible, because 6 is even, so a power of it can't be 1 modulo 4.

Next, we have to consider the $x = 0$ case, when $1 + 5^y = 6^z$. As before, we know that one solution ($y = z = 1$) exists. To rule out further solutions, we can take $m = 4$, $m = 9$, or $m = 25$. (The first two will make $6^z \equiv 0$ for $z \geq 2$; the last will make $5^y \equiv 0$ for $y \geq 2$.) Let's try $m = 4$ again first, as the simplest. We get

$$1 + 1^y \equiv 0 \pmod 4$$

which is a contradiction, since $2 \not\equiv 0 \pmod 4$. We conclude that no solution with $z \geq 2$ exists, so either $z = 0$ or $z = 1$. Checking both, we find no new solution, so $(0, 1, 1)$ is the only solution to the original equation.

2 Problems

2.1 Warm-up

1. (ARML 1993) There are several values for a prime p with the property that any five-digit multiple of p remains a multiple of p if you "rotate the digits". One such value is 41 (for example, since 50635 is a multiple of 41, so are 55603, 35506, 63550, and 6355); another such value is 3. Compute the value of p that is greater than 41.

2.2 Exponential Diophantine equations

1. Solve over the integers:
   (a) $2^x - 1 = 3^y$.
   (b) $7^x + 4 = 3^y$.
   (c) $3^x + 2 = 5^y$.
   (d) $2^x + 1 = 3^y$.
   (e) $3^x + 4^y = 5^z$.
2. Find all positive integers x and y such that $2^x + 3^y$ is a perfect square.
3. (BMO 1981) Find the smallest positive value of $|12^m - 5^n|$, where m, n are positive integers.

2.3 Other Diophantine equations

Note: in the case of polynomials (where the equation has, e.g., x^5 rather than 5^x) the key is still to choose a prime such that the power is simple, but this is now done differently. The power x^k reduces nicely modulo a prime p when $p-1$ divides k or at least a small multiple of k. For example, for all x, x^5 is one of $\{-1, 0, 1\}$ modulo 11, because $(x^5)^2 = x^{10} \equiv 1 \pmod{11}$ unless $11 \mid x$.

Experiment!

1. Show that there are no integer solutions to $x^3 + y^3 + z^3 = 400$.
2. (PUMaC 2009) Find all prime numbers p which can be written as $p = a^4 + b^4 + c^4 - 3$ for some primes a, b, and c (not necessarily distinct).
3. (USAMO 1979) Determine all non-negative integer solutions, apart from permutations, of the equation
$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$
4. Find all integer solutions to $x^2 + 2^x = y^2$.

5. Show that for any integers $x, y \geq 2$,

$$\left| \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{x} - \underbrace{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}_{y} \right| \geq 11.$$