Number Theory	Misha Lavrov
Diophantine equations	
Western PA ARML Practice	*October 4, 2015*

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.*

   Rotating the digits takes a number $10a + b$ to $10^4 b + a$. (For example, $50635 = 5063 \cdot 10 + 5$ becomes $55603 = 5 \cdot 10^4 + 5063$.) If

   $$\begin{cases} 10a + b \equiv 0 \pmod p \\ a + 10^4 b \equiv 0 \pmod p \end{cases}$$

   then $a \equiv -10^4 b \pmod p$, so $0 \equiv 10a + b \equiv (-10^5 b) + b = (1 - 10^5)b \pmod p$, which means $p \mid (1 - 10^5)b$.

   The only way to guarantee this is to have $p \mid 10^5 - 1 = 99999$. Since $99999 = 3^2 \cdot 41 \cdot 271$, the solution we're looking for is $p = 271$.

2.2 Exponential Diophantine equations

1. *Solve over the integers:*

   (a) $2^x - 1 = 3^y$.

   The only solutions are $2^1 - 1 = 3^0$ and $2^2 - 1 = 3^1$.

   Take the equation modulo 8. We have $3^2 \equiv 1 \pmod 8$, so 3^y is either 1 or 3 modulo 8. On the other hand, $2^x - 1 \equiv 7 \pmod 8$, assuming $x \geq 3$, and 7 is neither 1 nor 3. Therefore $x \leq 2$. Now we try $x = 0$, $x = 1$, and $x = 2$: $x = 0$ doesn't work (giving $2^0 - 1 = 0$, not a power of 3) but $x = 1$ and $x = 2$ both produce solutions.

   (b) $7^x + 4 = 3^y$.

   There are no solutions.

   Take the equation modulo 3. On the left-hand side, we have $7^x + 4 \equiv 1^x + 4 \equiv 2 \pmod 3$. On the right-hand side, we have $3^y \equiv 0 \pmod 3$, unless $y = 0$, in which case $3^y \equiv 1 \pmod 3$, which is still not 2.

   (c) $3^x + 2 = 5^y$.

   The only solution is $3^1 + 2 = 5^1$.

Take the equation modulo 9. The powers of 5 modulo 9 are $1, 5, 7, 8, 4, 2, 1, \dots$. Assuming $x \geq 2$, the right-hand side is 2 modulo 9, so we must have $y \equiv 5 \pmod 6$.

Now take the equation modulo 7, chosen because $5^6 \equiv 1 \pmod 7$. This means $5^y = 5^5 \cdot (5^6)^k \equiv 3 \pmod 7$, so $3^x \equiv 3 - 2 = 1 \pmod 7$. The powers of 3 modulo 7 are $1, 3, 2, 6, 4, 5, 1, \dots$, so we must have $x \equiv 0 \pmod 6$.

In particular, x is even, so $3^x = 729^{x/6}$. Since $728 = 2^3 \cdot 7 \cdot 13$, we take the equation modulo 13. On the left-hand side, we get $729^{x/6} + 2 \equiv 1^{x/6} + 2 = 3 \pmod{13}$. On the right-hand side, since $5^6 \equiv -1 \pmod{13}$, we have $5^y \equiv \pm 5^5 \equiv \pm 5 \pmod{13}$, which is either 5 or 8.

This is a contradiction, so we must have $x < 2$. Trying $x = 0$ and $x = 1$, we find the only solution.

(d) $2^x + 1 = 3^y$.

The only solutions are $2^1 + 1 = 3^1$ and $2^3 + 1 = 3^2$.

Assume $y \geq 2$ and take the equation modulo 9. Then we have $2^x \equiv -1 \pmod 9$. The powers of 2 modulo 9 are $1, 2, 4, -1, -2, -4, 1, \dots$, repeating every 6 steps, so $x \equiv 3 \pmod 6$. In particular, x is divisible by 3.

Then we have $2^x + 1 = (2^{x/3})^3 + 1 = (2^{x/3} + 1)(2^{2x/3} - 2^{x/3} + 1)$. This is equal to 3^y, so both factors must be powers of 3. In particular, $2^{x/3} + 1$ is a power of 3, so if (x, y) is a solution to the Diophantine equation and $y \geq 2$, there is another solution with $x/3$ in place of x. We can keep dividing x by 3 until we descend to a solution with $y < 2$.

When $y = 0$ there is no solution, and when $y = 1$ we get the solution $(1, 1)$. Therefore all solutions must descend to the $(1, 1)$ solution. This gives us the $x = 3$ solution found above, but $2^9 + 1$ is not a power of 3, so we have exhausted all solutions.

(e) $3^x + 4^y = 5^z$.

The only solutions are $3^0 + 4^1 = 5^1$ and $3^2 + 4^2 = 5^2$.

Take the equation modulo 3. We'll deal with the $x = 0$ case later; if $x > 0$, we get $3^x + 4^y \equiv 0 + 1^y \pmod 3$ on the right, and $5^z \equiv (-1)^z$ on the left. This tells us that z is even.

Now we have $3^x = 25^{z/2} - 4^y = (5^{z/2} + 2^y)(5^{z/2} - 2^y)$, so both $5^{z/2} + 2^y$ and $5^{z/2} - 2^y$ are powers of 3. But their sum is $2 \cdot 5^{z/2}$, which is not divisible by 3, so one of the powers of 3 (the smaller one) must be $3^0 = 1$, and we are left with the equations

$$\begin{cases} 5^{z/2} + 2^y = 3^x, \\ 5^{z/2} - 2^y = 1. \end{cases}$$

Taking the difference, we get $3^x - 1 = 2^{y+1}$. This is the equation in part (d), so we must have $x = y = 2$ or $y = 0$ and $x = 1$. The first option gives us the $(2, 2, 2)$ solution, and the second option can't find a value of z.

It remains to consider the $x=0$ case, where we get $4^y+1=5^z$. The $y=1$ solution we've already found, so assume $y\geq 2$ and take the equation mod 8. Since $5^2\equiv 1 \pmod 8$, z must be even, so we have a difference of squares once again: $(5^{z/2}+2^y)(5^{z/2}-2^y)=1$. But this is impossible to satisfy, since the factors can't both be 1 or both -1, so there are no further solutions to be found.

2. *Find all positive integers x and y such that 2^x+3^y is a perfect square.*

   The only solutions are $2^0+3^1=4$, $2^3+3^0=9$, and $2^4+3^2=25$.

   Try $y=0$. Then $2^x+1=k^2$ for some k, so $2^x=k^2-1=(k+1)(k-1)$. This is only possible when $k-1=2$ and $k+1=4$, giving us one of the solutions.

   Otherwise, $y>0$, so we have $(-1)^x+0\equiv k^2 \pmod 3$. But k^2 can only be 0 or 1 modulo 3, so x must be even. Then we have a difference of squares:

   $$3^y=(k+2^{x/2})(k-2^{x/2}).$$

   So both $k+2^{x/2}$ and $k-2^{x/2}$ are powers of 3. But their difference is $2^{x/2+1}$, which is not divisible by 3. Therefore $k-2^{x/2}=3^0=1$. Solving for k, we get $k=2^{x/2}+1$, so

   $$2^x+3^y=(2^{x/2}+1)^2=2^x+2^{x/2+1}+1.$$

   This means that $3^y=2^{x/2+1}+1$, which has only two solutions, by problem 1(d). We can have $x/2+1=y=1$, giving $2^0+3^1=4$, or $x/2+1=3$ and $y=2$, giving us $2^4+3^2=25$.

3. *(BMO 1981) Find the smallest positive value of $|12^m-5^n|$, where m, n are positive integers.*

   Clearly, $|12^1-5^1|=7$ is achievable. Is any smaller value possible? We have $12^m-5^n\equiv 0^m-1^n\equiv 1 \pmod 2$, $12^m-5^n\equiv 0^m-(-1)^n\not\equiv 0 \pmod 3$, and $12^m-5^n\equiv 2^m-0^n\not\equiv 0 \pmod 5$, which rules out 2, 3, 4, 5, and 6. So it remains to check if there are any solutions to $12^m-5^n=\pm 1$.

   Taking the equation modulo 4, we get $0^m-1^n\equiv \pm 1 \pmod 4$, so the 1 must be negative, and we have $5^n-12^m=1$.

   Taking the equation modulo 3, we ge $(-1)^n-0^m\equiv 1 \pmod 3$, so n must be even.

   Taking the equation modulo 5, we get $0^n-2^m\equiv 1 \pmod 5$, which is possible only for $m\equiv 2 \pmod 4$. So m must be even as well.

   But now we have the difference of squares $(5^{n/2})^2-(12^{m/2})^2=1$, which factors as $(5^{n/2}-12^{m/2})(5^{n/2}+12^{m/2})=1$. So both factors must be 1 or else both -1, which is impossible as $12^{m/2}>0$.

   So an absolute difference of 1 is rulled out, and the smallest achievable value is 7.

2.3 Other Diophantine equations

1. *Show that there are no integer solutions to $x^3 + y^3 + z^3 = 400$.*

   Take the equation modulo 9. It's easy to check that all perfect cubes are 0, 1, or -1 modulo 9, so the remainder modulo 9 of $x^3 + y^3 + z^3$ can be any of $\{-3, -2, -1, 0, 1, 2, 3\}$. However, $400 \equiv 4 \pmod 9$.

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).*

   Write the right-hand side as $(a^4 - 1) + (b^4 - 1) + (c^4 - 1)$. We have $x^4 - 1 \equiv 0 \pmod 2$ unless x is even, $x^4 - 1 \equiv 0 \pmod 3$ unless $x \equiv 0 \pmod 3$, and $x^4 - 1 \equiv 0 \pmod 5$ unless $x \equiv 0 \pmod 5$.

   Therefore $a^4 + b^4 + c^4 - 3 \equiv 0 \pmod 2$ unless a, b, or c is 2; it is divisible by 3 unless a, b, or c is 3; and it is divisible by 5 unless a, b, or c is 5. We can check that $p = 2$, $p = 3$, and $p = 5$ are too small to be a solution, so the only possibility is $p = 2^4 + 3^4 + 5^4 - 3 = 719$, which is indeed prime.

3. *(USAMO 1979) Determine all non-negative integer solutions, apart from permutations, of the equation*

   $$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

   Modulo 16, any perfect fourth power is either 0 or 1, so the sum on the right-hand side can be anything from 0 to 14 modulo 16. But $1599 = 1600 - 1$, so it is 15 modulo 16, and there are no solutions.

4. *Find all integer solutions to $x^2 + 2^x = y^2$.*

   The only solutions are $0^2 + 2^0 = 1^2$ and $6^2 + 2^6 = 10^2$.

   We have $2^x = y^2 - x^2 = (y + x)(y - x)$, so both $y + x$ and $y - x$ are powers of 2. Write $y + x = 2^i$ and $y - x = 2^j$; we have $x = 2^{i-1} - 2^{j-1}$. The equation $2^x = y^2 - x^2$ becomes

   $$2^{2^{i-1} - 2^{j-1}} = 2^{i+j}$$

   so $2^{i-1} - 2^{j-1} = i + j$.

   Since $i > j$, we have $2^{i-1} - 2^{j-1} \geq 2^{i-2}$, while $i + j < 2i$. Thus, $2^{i-2} < 2i$, which means $i > 2^{i-3}$. This is true only for $i \leq 5$: the right-hand side grows much faster than the left. Checking all values $0 \leq j \leq i \leq 5$, we only find the two solutions above.

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

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

   Almost any modulus will work. Modulo 100, the power tower of 2's will eventually stabilize at 36, and the power tower of 3's at 87, giving a lower bound of 49. It then suffices to check that no small values of x and y do better than $3^3 - 2^{2^2} = 11$.