MAO Diophantine Equations

Dylan Yu

October 20, 2020

1 Definitions

Here we introduce some important notation and ideas that we will use throughout the handout.

Definition 1 (Diophantine Equation)
A ***diophantine equation*** is an equation that can be solved over the integers.

For example, $a + b = 32$, where a, b are integers, is a diophantine equation.

Definition 2 ($\mathbb{Z}$)
If $a \in \mathbb{Z}$, then a is an integer.

Furthermore, $\mathbb{Z}^-$ is the set of negative integers, $\mathbb{Z}^+$ is the set of positive integers, $\mathbb{Z}^{0+}$ is the set of nonnegative integers, and $\mathbb{Z}^{0-}$ is the set of nonpositive integers.

2 Modular Arithmetic

When we say "$a \equiv b \pmod{m}$" (this is read as "a is congruent to b mod m"), we mean that when we add or subtract a with some integer number of m's, we will get b. For example, $27 \equiv 2 \pmod{5}$ because if we subtract 5 5's from 27, we get 2. We can also say that $a \equiv b \pmod{m}$ if $a \div m$ and $b \div m$ have the same remainder. Now let's note a few important properties we will use in solving diophantines:

1. **Parity**. Taking odd numbers in mod 2 are always 1, and even numbers are always 0.

2. **Checking Squares**. In mod 3, squares are either 0 or 1. In mod 4, squares are also either 0 or 1.

3. **Checking Cubes**. In mod 4, cubes are either 0, 1, or 3.

There are more properties, but they are easily derived (just check all the possibilities).

Example 3 (Folklore)
Prove that if $x \in \mathbb{Z}$, $x^2 \equiv 3 \pmod{4}$ has no solutions.

Solution. Note that x is either $0, 1, 2$, or 3 in mod 4. Let's make a chart:

$x \pmod 4$	$x^2 \pmod 4$
0	0
1	1
2	0
3	1

Thus, in mod 4, squares are either 0 or 1 mod 4. This means x^2 can never be 3 mod 4. $\square$

Example 4 (Balkan MO)
Prove that the equation $x^5 - y^2 = 4$ has no solutions over the integers.

Solution. Note that x^5 is either $-1, 0$, or 1 mod 11 and y^2 is either $0, 1, 3, 4, 5$, or 9 mod 11. Thus, if we have the equation

$$x^5 - y^2 = 4 \pmod{11},$$

we realize that regardless of what we choose for the pair of mods from the list above, it will always never equal 4 (if you don't believe me, try it out!). Thus, there are no solutions. $\square$

Remark 5
Mod 11 is a strange thing to do, but with practice it becomes more natural. This is why practice is necessary – it allows you to more accurately pinpoint which mod to apply.

3 Factoring

Sometimes we can just factor the equation. However, it is usually extremely disguised, so **if you see a strangely arranged equation with many terms, try factoring!**

Theorem 6 (SFFT)
Simon's Favoring Factoring Trick, abbreviated SFFT, states that $xy + ax + by + ab = (x + b)(y + a)$.

This isn't very special, but sometimes it is disguised.

Example 7
Find all integral solutions to $xy - x + y = 0$.

Solution. Note that this is equivalent to $x(y-1) + y = 0$. If we subtract 1 from both sides, we get $x(y-1) + y - 1 = -1$, so

$$(x+1)(y-1) = -1,$$

implying we have $x + 1 = 1$ and $y - 1 = -1$ or $x + 1 = -1$ or $y - 1 = 1$. Thus, the solutions for (x, y) are $\boxed{(0, 0)}$ or $\boxed{(-2, 2)}$. $\square$

Example 8 (Titu)
Find all integral solutions to the equation

$$(x^2+1)(y^2+1)+2(x-y)(1-xy)=4(1+xy).$$

Solution. Let's expand (almost) everything:

$$x^2y^2+x^2+y^2+1+2(x-y)(1-xy)=4+4xy,$$

$$\begin{aligned} x^2y^2+x^2+y^2+1+2(x-y)(1-xy)&=4+4xy,\\ x^2y^2-2xy+1+x^2+y^2-2xy-2(x-y)(xy-1)&=4,\\ (xy-1)^2+(x-y)^2-2(x-y)(xy-1)&=4,\\ (xy-1-(x-y))^2&=4,\end{aligned}$$

implying $xy-x+y-1=2$ or -2. Note that $xy-x+y-1=(x+1)(y-1)$, which gives us solutions of $\boxed{(-3,2),(-2,3),(0,-1),(1,0)}$. $\square$

Here is an important theorem to keep in mind while solving:

Theorem 9
Let x, y be positive integers and let $n=p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$ (in other words, its prime factorization). Then the equation

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$$

has $(2e_1+1)(2e_2+1)\dots(2e_k+1)$ solutions.

Knowing key factorizations is important. For example,

$$x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-zx)$$

can help you solve problems of this nature quickly.

4 Inequalities

Sometimes, to show there are finite (or no) possibilities, we can use an inequality to bound the equation.

Theorem 10 (Trivial Inequality)
Squares are always greater than or equal to 0, i.e. $x^2\geq 0$ for all real x.

Example 11
Find all pairs (x, y) of integers such that

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

Solution. Factoring the LHS (left hand side), we get

$$(x+y)(x^2-xy+y^2) = (x+y)^2,$$

so if $x+y \neq 0$, then

$$\begin{aligned} x^2-xy+y^2 &= x+y, \\ x^2-xy+y^2-(x+y) &= 0, \\ 2x^2-2xy+2y^2-2x-2y &= 0, \\ x^2-2xy+y^2+x^2-2x+y^2-2y &= 0, \\ (x-y)^2+(x-1)^2+(y-1)^2 &= 2, \end{aligned}$$

and by the Trivial Inequality, two of these squares are equal to 1 and one of them is equal to 0. We can easily solve for the solutions then: $\boxed{(0,1),(1,0),(1,2),(2,1),(2,2)}$. However, we said this is what happens if $x+y \neq 0$. That means when $x+y=0$, we can have the solutions $\boxed{(k,-k)}$, and they all suffice. □

Another strategy is assuming $x \geq y \geq z$ without loss of generality (abbreviated WLOG). This sometimes holds if the equation is symmetric.

Example 12 (UK MO)
Find all triples (x,y,z) of positive integers such that

$$\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right) = 2.$$

Solution. WLOG let $x \geq y \geq z$. This means that $\frac{1}{x} \leq \frac{1}{y} \leq \frac{1}{z}$, so

$$1+\frac{1}{x} \leq 1+\frac{1}{y} \leq 1+\frac{1}{z}.$$

Thus,

$$2 = \left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right) \leq \left(1+\frac{1}{z}\right)^3,$$

implying

$$1+\frac{1}{z} \geq \sqrt[3]{2},$$

and solving this inequality gives us $z \leq 3$. Thus, we just test the possibilities where $z = 1,2,$ or 3, giving us $\boxed{(7,6,2),(9,5,2),(15,4,2),(8,3,3),(5,4,3)}$ in any order. □

Remark 13
Notice how we assumed $x \geq y \geq z$, but then we have to convert back to the original problem. This meant that if we considered something different, like $y \geq z \geq x$, it would be the exact same problem, except the variables would be moved around. That's why we put "in any order" in the last sentence.

5 Problems

5.1 Modular Arithmetic

Problem 14
Prove that the equation

$$(x+1)^2 + (x+2)^2 + \ldots + (x+2001)^2 = y^2$$

is not solvable.

Problem 15 (Russian MO)
Find all pairs (p, q) of prime numbers such that

$$p^3 - q^5 = (p+q)^2.$$

Problem 16 (IMO 1982/4)
Prove that if n is a positive integer such that the equation

$$x^3 - 3xy^2 + y^3 = n$$

has a solution in integers x, y, then it has at least three such solutions. Prove that the equation has no integer solution when $n = 2891$.

Problem 17 (IMO 1990/3)
Determine all integers $n \geq 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

5.2 Factoring

Problem 18
Let p, q be primes. Solve, in positive integers, the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{pq}.$$

Problem 19 (Indian MO)
Determine all nonnegative integral pairs (x, y) for which

$$(xy - 7)^2 = x^2 + y^2.$$

Problem 20 (Polish MO)
Solve the following equation in integers x, y:

$$x^2(y-1) + y^2(x-1) = 1.$$

Problem 21 (Romanian MO)
Find all pairs (x, y) of integers such that

$$x^6 + 3x^3 + 1 = y^4.$$

5.3 Inequalities

Problem 22 (Romanian MO)
Solve the following equation in positive integers x, y, z:

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}.$$

Problem 23 (Romanian MO)
Determine all triples (x, y, z) of positive integers such that

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

Problem 24 (Australian MO)
Determine all pairs (x, y) of integers that satisfy the equation

$$(x+1)^4 - (x-1)^4 = y^3.$$

Problem 25 (Russian MO)
Find all integer solutions to the equation

$$(x^2 - y^2)^2 = 1 + 16y.$$