Diophantine Equations

Dylan Yu

December 30, 2021

A large part of olympiad number theory is diophantine equations. In this handout, we learn the "basic toolbox" for solving diophantine equations: modular arithmetic, factoring, and inequalities.

Thanks to Rushil Shah for proofreading.

Contents

1 Definitions 1

2 Modular Arithmetic 2

3 Factoring 3

4 Inequalities 4

5 Problems 5
- 5.1 Modular Arithmetic 5
- 5.2 Factoring 5
- 5.3 Inequalities 5

6 Selected Solutions 7
- 6.1 Solution 1 (Folklore) 7
- 6.2 Solution 2 (Balkan MO) 7
- 6.3 Solution 5 7
- 6.4 Solution 6 (Titu) 7
- 6.5 Solution 9 8
- 6.6 Solution 10 (UK MO) 8

1 Definitions

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

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.

$\mathbb{Z}$
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, $27 \equiv 12 \pmod{5}$ because if we subtract 3 fives from 27, we get 12. 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 modulo 2 are always 1, and even numbers are always 0.
2. **Checking Squares**. In modulo 3, squares are either 0 or 1. In modulo 4, squares are also either 0 or 1.
3. **Checking Cubes**. In modulo 4, cubes are either 0, 1, or 3.

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

Example 1 (Folklore)
Prove that if $x \in \mathbb{Z}$, $x^2 \equiv 3 \pmod{4}$ has no solutions.

Walkthrough. Literally just check them. Make a chart if you want. Note that we only need to check 0 to 3, because the cases for $x = k$ and $x = k + 4$ are the same. (Why?)

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

Walkthrough.

1. What are the residues of x^5 in modulo 11?
2. What about y^2 in modulo 11?
3. Do any pairs (x, y) yield $x^5 - y^2 = 4 \pmod{11}$?

Remark 3. Modulo 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 modulo 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 4 (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 5
Find all integral solutions to $xy - x + y = 0$.

Walkthrough. Subtract 1 and factor.

Example 6 (Titu)
Find all integral solutions to the equation

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

Walkthrough. Don't let the huge equation scare you. (Okay fine maybe a little.)

1. Move everything except the 4 to the left side.
2. You'll find terms of the form $x^2y^2 - 2xy + 1$ and $x^2 - 2xy + y^2$. It should be clear what you want to do with these.
3. Prove the equation given in the problem is equal to

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

   and use $u = xy - 1, v = x - y$ to turn the LHS into a square.
4. Finish using SFFT.

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

Theorem 7
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 also 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 8 (Trivial Inequality)
Squares are always greater than or equal to 0, i.e. $x^2 \geq 0$ for all real x.

Example 9
Find all pairs (x, y) of integers such that

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

Walkthrough.

1. Prove that if $x + y = 0$ then the given equation is satisfied.
2. Assume $x + y \neq 0$ from now on. Divide both sides of the given equation by $x + y$.
3. Complete squares until you get something nice. In particular, until you get:
$$(x-y)^2 + (x-1)^2 + (y-1)^2 = 2.$$
4. Finish by casework.

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

Example 10 (UK MO)
Find all triples (x, y, z) of positive integers such that

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

Walkthrough. WLOG let $x \geq y \geq z$.

1. Prove $\frac{1}{x} \leq \frac{1}{y} \leq \frac{1}{z}$.
2. Use the above step to show
$$\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right) \leq f(z),$$
where $f(z)$ is a function in terms of z.
3. Now bound z. You should get three possible values of z.
4. Finish by casework.

Remark 11. 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.

Remark 12 (Casework). By now you've noticed a common theme: we want to **reduce the diophantines until we get a small number of cases**. This is basically why we do modular arithmetic and bounding in the first place.

5 Problems

5.1 Modular Arithmetic

Problem 1. Prove that the equation

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

is not solvable.

Problem 2 (Russia MO). Find all pairs (p,q) of prime numbers such that

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

Problem 3 (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 4 (IMO 1990/3). Determine all integers $n \geq 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

5.2 Factoring

Problem 5. Let p, q be primes. Solve, in positive integers, the equation

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

Problem 6 (India MO). Determine all nonnegative integral pairs (x,y) for which

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

Problem 7 (Poland MO). Solve the following equation in integers x, y:

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

Problem 8 (Romania MO). Find all pairs (x,y) of integers such that

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

5.3 Inequalities

Problem 9 (Romania MO). Solve the following equation in positive integers x, y, z:

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

Problem 10 (Romania MO). Determine all triples (x, y, z) of positive integers such that

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

Problem 11 (Australia MO). Determine all pairs (x, y) of integers that satisfy the equation

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

Problem 12 (Russia MO). Find all integer solutions to the equation

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

6 Selected Solutions

6.1 Solution 1 (Folklore)

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.

6.2 Solution 2 (Balkan MO)

Note that x^5 is either $-1, 0$, or 1 modulo 11 and y^2 is either $0, 1, 3, 4, 5$, or 9 modulo 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.

6.3 Solution 5

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 $\boxed{(-2,2)}$.

6.4 Solution 6 (Titu)

Let's expand (almost) everything:

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

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

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

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

implying $xy - x + y - 1 = 2$ or -2. Note that $xy - x + y - 1 = (x+1)(y-1)$, which gives us solutions of

$$(-3,0), (-3,2), (-2,-1), (-2,3), (0,-1), (0,3), (1,0), (1,2),$$

implying there are $\boxed{8}$ solutions.

6.5 Solution 9

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.

6.6 Solution 10 (UK MO)

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.