

# Diophantine Equations

Dylan Yu

NPU

## 1 Common Types and Techniques for Diophantine Equations

1. There are known formulas for some types of Diophantine equations. For example,
  - $ax + by = c$ : linear equations with two unknowns
  - $a^2 + b^2 = c^2$ : quadratic equations with three unknowns
  - $xy = zt$ : quadratic equations with four unknowns
2. Uniqueness of Prime Factorization
3. Completing the Square
4. Completing the Rectangle/SFFT
5. Limit the size of solutions or key quantities
6. The Squeeze Principle
7. Parity Analysis
8. Choosing Special Modulus
9. Change of Variables/Substitution
10. Modular contradiction (e.g. a number cannot be  $1 \pmod{4}$  and  $0 \pmod{2}$ .)
11. Factorizations
12. LTE
13. Pell equations
14. Recurrences
15. Infinite descent
16. Algebraic substitutions
17. Inequalities (similar to squeezing and bounding)
18. Legendre's formula for  $p$ -adic valuation of factorials
19. Geometric interpretation
20. Induction
21. Extensions of  $\mathbb{Z}$

## 2 Introduction

### 2.1 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. A *linear example* would be  $ax + by = c$ , where  $a, b, c, x, y$  are integers.

$\mathbb{Z}$ . 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.

### 2.2 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 us turn to one of the most important theorems for solving Diophantine equations:

**Law of Diophantines.** Let  $m > 1$  be a positive integer. If an equation has no solution modulo  $m$ , then it has no integer solutions.

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 (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.

**Remark:** Although taking mod 11 does seem like a weird thing to do, we are motivated to take mod 11 due to the fact that  $x^{10} \equiv 1 \pmod{11}$  for all  $x$ , which gives us a relatively low number of possible values of  $x^5$ .

## 2.3 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!**

**Simon's Favoring Factoring Trick**, abbreviated SFFT, is useful here.

**SFFT.** For all  $x, y, a, b$  (usually integers),

$$xy + ax + by + ab = (x + b)(y + a).$$

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

**Example.** 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  $(0, 0)$  or  $(-2, 2)$ .

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

. 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

$$\tau(n^2) = (2e_1 + 1)(2e_2 + 1) \dots (2e_k + 1),$$

solutions, where  $\tau(n)$  is the number of divisors of  $n$ .

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.

## 3 Examples

**Linear Equation with Two Unknowns.** The equation  $ax + by = c$  has integer solutions if and only if  $\gcd(a, b) \mid c$ . If  $\gcd(a, b) = 1$ , and  $x_0, y_0$  is one integer solution for  $ax + by = c$ , then the general solution is  $x = x_0 + bt, y = y_0 - at$ , where  $t$  is an integer.

There is a lot of mapping solutions to solutions in Diophantine equations. In other words, if  $(x_0, y_0)$  is a solution, then  $(f(x_0), g(y_0))$  is a solution, for some functions  $f, g$ .

**Example.** Find all positive integer solutions of

$$19x + 7y = 260.$$

**Solution.** A simple solution is  $x = y = 10$ . Thus, we can apply the method listed above and solve for all solutions. It turns out the only solutions are  $(10, 10)$  and  $(3, 29)$ .

Let's move on to higher degree equations:

**Quadratic Equation with Three Unknowns.** For the equation

$$x^2 + y^2 = z^2,$$

all positive integer solutions  $(x, y, z)$  that satisfy  $\gcd(x, y, z) = 1$  is

$$x = a^2 - b^2, y = 2ab, z = a^2 + b^2,$$

where integers  $a > b > 0$ , one even and one odd, and  $\gcd(a, b) = 1$ .

As you have probably realized, this is just the **parameterization** of the **Pythagorean triples**. This underlies something important in solving Diophantine equations – parameterization.

**Quadratic Equation with Four Unknowns.** For the equation

$$xy = zt,$$

all positive integer solutions can be found by letting

$$\frac{x}{z} = \frac{t}{y} = \frac{m}{n},$$

where  $\gcd(m, n) = 1$ , then  $x = pm, z = pn, t = qm, y = qn$ , where  $p = \gcd(x, z), q = \frac{y}{n}$ .

**Example.** Let  $a, b, c, d$  be positive integers, and  $ab = cd$ . Prove that  $a^4 + b^4 + c^4 + d^4$  is not prime.

**Solution.** From the theorem above, we have

$$\frac{a}{c} = \frac{d}{b} = \frac{m}{n},$$

so  $a = pm, c = pn, d = qm, b = qn$ . Now, plugging these numbers in, we get

$$a^4 + b^4 + c^4 + d^4 = p^4m^4 + q^4n^4 + p^4n^4 + q^4m^4 = (p^4 + q^4)(m^4 + n^4).$$

Because  $p, q, m, n$  are all positive integers, then

$$p^4 + q^4 > 1,$$

$$m^4 + n^4 > 1,$$

so the product cannot be prime.

**Example.** Let  $k$  be an even number. Is it possible to find  $k$  odd integers whose reciprocals add up to 1?

**Solution.** Let  $n_1, n_2, \dots, n_k$  be  $k$  odd integers. Then we must see if

$$\sum_{i=1}^k \frac{1}{n_i} = 1$$

exists. Note that if we take the common denominator, we have

$$\frac{\sum_{\text{sym}} n_2 n_3 \dots n_k}{n_1 n_2 n_3 \dots n_k} = 1,$$

and because there are  $k$  symmetric sums, the numerator is even, and the denominator is odd. Thus, it is impossible for any group of  $k$  odd integers to satisfy these conditions.

**Example.** Find all distinct positive integers such that their product equals their sum.

**Solution.** Let

$$x_1 \cdot x_2 \cdot \dots \cdot x_n = x_1 + x_2 + \dots + x_n$$

for positive integer  $1 \leq x_1 < x_2 < x_3 < \dots < x_n$ . Then

$$(n-1)!x_n \leq x_1 \cdot x_2 \cdot \dots \cdot x_n = x_1 + x_2 + \dots + x_n \leq nx_n.$$

Thus,

$$(n-1)! < n,$$

so  $n = 2, 3$ . If  $n = 2$ , then

$$x_1 x_2 = x_1 + x_2,$$

so

$$(x_1 - 1)(x_2 - 1) = 1,$$

which implies  $x_1 = x_2 = 2$ . However, they must be distinct, so there are no solutions for  $n = 2$ . For  $n = 3$ , we have

$$x_1 x_2 x_3 = x_1 + x_2 + x_3 < 3x_3,$$

so

$$x_1 x_2 < 3.$$

Because  $x_1 \neq x_2$ , the only possible solution is

$$x_1 = 1, x_2 = 2.$$

Thus,  $x_3 = 3$ . Therefore, the only solution is  $(1, 2, 3)$  over all positive integers.

## 4 Problems

Minimum is [36 🧑]. Problems denoted with 🧑 are required. (They still count towards the point total.)

“Diophantine and valentine somehow don’t rhyme.”  
Dylan during quarantine.

[1 🧑] **Problem 1 (AMC 12A 2004/3)** For how many ordered pairs of positive integers  $(x, y)$  is  $x + 2y = 100$ ?

[1 🧑] **Problem 2 (AMC 12B 2008/5)** A class collects 50 dollars to buy flowers for a classmate who is in the hospital. Roses cost 3 dollars each, and carnations cost 2 dollars each. No other flowers are to be used. How many different bouquets could be purchased for exactly 50 dollars?

[2 🧑] **Problem 3 (AMC 12A 2005/8)** Let  $A$ ,  $M$ , and  $C$  be digits with

$$(100A + 10M + C)(A + M + C) = 2005$$

What is  $A$ ?

[2 🧑] **Problem 4 (AHSME 1989/16)** A lattice point is a point in the plane with integer coordinates. How many lattice points are on the line segment whose endpoints are  $(3, 17)$  and  $(48, 281)$ ? (Include both endpoints of the segment in your count.)

[2 🧑] **Problem 5 (AMC 12A 2006/9)** Oscar buys 13 pencils and 3 erasers for \$1.00. A pencil costs more than an eraser, and both items cost a whole number of cents. What is the total cost, in cents, of one pencil and one eraser?

[3 🧑] **Problem 6 (AMC 12A 2006/14)** Two farmers agree that pigs are worth 300 dollars and that goats are worth 210 dollars. When one farmer owes the other money, he pays the debt in pigs or goats, with “change” received in the form of goats or pigs as necessary. (For example, a 390 dollar debt could be paid with two pigs, with one goat received in change.) What is the amount of the smallest positive debt that can be resolved in this way?

[3 🧑] **Problem 7 (AMC 12B 2003/18)** Let  $x$  and  $y$  be positive integers such that  $7x^5 = 11y^{13}$ . The minimum possible value of  $x$  has a prime factorization  $a^c b^d$ . What is  $a + b + c + d$ ?

[3 🧑] **Problem 8 (AHSME 1968/19)** Let  $n$  be the number of ways 10 dollars can be changed into dimes and quarters, with at least one of each coin being used. Then what is  $n$ ?

[4 🧑] **Problem 9 (AMC 10B 2015/15)** The town of Hamlet has 3 people for each horse, 4 sheep for each cow, and 3 ducks for each person. Which of the following could not possibly be the total number of people, horses, sheep, cows, and ducks in Hamlet?

(A) 41      (B) 47      (C) 59      (D) 61      (E) 66

[6 🧑] **Problem 10 (AMC 12 2001/21)** Four positive integers  $a$ ,  $b$ ,  $c$ , and  $d$  have a product of 8! and satisfy:

$$ab + a + b = 524$$

$$bc + b + c = 146$$


$$cd + c + d = 104$$

What is  $a - d$ ?

[6 🧑] **Problem 11 (AMC 12A 2014/19)** There are exactly  $N$  distinct rational numbers  $k$  such that  $|k| < 200$  and


$$5x^2 + kx + 12 = 0$$


has at least one integer solution for  $x$ . What is  $N$ ?


[6 ] **Problem 12 (AMC 12A 2019/15)** Positive real numbers  $a$  and  $b$  have the property that


$$\sqrt{\log a} + \sqrt{\log b} + \log \sqrt{a} + \log \sqrt{b} = 100$$

and all four terms on the left are positive integers, where  $\log$  denotes the base 10 logarithm. What is  $ab$ ?

[6 ] **Problem 13 (AIME 1997/1)** How many of the integers between 1 and 1000, inclusive, can be expressed as the difference of the squares of two nonnegative integers?

[9 ] **Problem 14 (AIME II 2000/2)** A point whose coordinates are both integers is called a lattice point. How many lattice points lie on the hyperbola  $x^2 - y^2 = 2000^2$ ?

[9 ] **Problem 15 (AIME I 2015/3)** There is a prime number  $p$  such that  $16p + 1$  is the cube of a positive integer. Find  $p$ .

[9 ] **Problem 16 (AIME I 2008/4)** There exist unique positive integers  $x$  and  $y$  that satisfy the equation  $x^2 + 84x + 2008 = y^2$ . Find  $x + y$ .