Diophantine Equations

Dylan Yu

NRU

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.

Example (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 $1 \bmod 11$ and y^2 is either $0, 1, 3, 4, 5$, or $9 \bmod 11$. Thus, if we have the congruence

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

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.

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 $\boxed{(0, 0)}$ or $\boxed{(-2, 2)}$.

Example (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:

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

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

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

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

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

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

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

Some exponential equations:

Example (New York 1977). Solve the Diophantine equation $2^x + 1 = y^2$.

Solution. Let's subtract by 1 and take a difference of squares:

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

Note that $x > 0$ since $x = 0$ has no solutions, and anything under that would make y non-integral. Thus,

$$2^m = y + 1,$$

$$2^n = y - 1,$$

for positive integers $m > n$. If we subtract the equations, we get

$$2^m - 2^n = 2,$$

and factoring we get

$$2^n(2^{m-n} - 1) = 2.$$

This implies $2^n = 1, 2^{m-n} - 1 = 2$, or vice versa. The first one yields no solutions, but the second one yields $m = 2, n = 1$. Thus, $y = 3$, and therefore $x = 3$. Thus, we have proven $(3, 3)$ is the only solution.

Example. Show that $x(x + 1) + 1 = y^2$ has no positive integer solutions.

Solution. Note that

$$y^2 = x^2 + x + 1,$$

and

$$x^2 < x^2 + x + 1 < (x + 1)^2,$$

for all positive integer x. Thus,

$$x^2 < y^2 < (x+1)^2,$$

and since all are positive,

$$x < y < x+1,$$

so there are no solutions.

Example. Find all integer solutions for

$$x^4 + 4y^4 = 2(z^4 + 4u^4).$$

Solution. This is similar to Sophie Germain, but intuition tells us that will be messy. Instead, let us take mod 2:

$$x^4 \equiv 0 \pmod 2,$$

so x is even. Let us substitute $x = 2x_1$:

$$(2x_1)^4 + 4y^4 = 2(z^4 + 4u^4).$$

If we divide by 2, we get

$$2(y^4 + 4x_1^4) = z^4 + 4u^4.$$

It turns out we get the same equation, only the variables have shifted. If this go on forever, then all integers must be 0, otherwise, we will eventually divide by two many 0s and get no solutions. Thus, $x = y = z = u = 0$.

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

Solution. Let $n_1, n_2, \ldots, n_k$ 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

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

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

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

for positive integer $1 \le x_1 < x_2 < x_3 < \ldots < x_n$. Then

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

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.

Example. Show that there are no integer solutions for the equation $y^2 = x^3 + 7$.

Solution. If x is even, then

$$y^2 \equiv 0 + 3 \equiv 3 \pmod 4,$$

which yields no solutions. Thus, x must be odd for there to exist solutions. If we add 1 to both sides and factor the RHS, we get

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4) = (x+2)((x-1)^2 + 3),$$

so we know that

$$(x-1)^2 + 3 \equiv 3 \pmod 4,$$

so

$$(x-1)^2 + 3 = p_1 p_2 \dots p_n.$$

This implies at least one $p \equiv 3 \pmod 4$. This in turn implies

$$y^2 + 1 \equiv 0 \pmod p,$$

$$y^2 \equiv -1 \pmod p.$$

Thus,

$$y^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p,$$

and by Fermat's Little Theorem we have

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod p,$$

so $\frac{p-1}{2}$ is even, so $p = 4k + 1$, or in other words $p \equiv 1 \pmod 4$. This is a direct contradiction of the fact that at least one $p \equiv 3 \pmod 4$, so there are no solutions to the equation.

Example. Solve $(x+1)^y - x^z = 1$ where $x, y, z > 1$ are integers.

Solution. If we take mod $x+1$, we get

$$0-(-1)^z \equiv 1 \pmod{x+1},$$

so z is odd. We know that

$$(x+1)^y = x^z + 1,$$

and since z is odd, we can factor the RHS side as

$$(x+1)^y = (x+1)(x^{z-1} - x^{z-1} + \ldots - x + 1),$$

$$(x+1)^{y-1} = x^{z-1} - x^{z-1} + \ldots - x + 1.$$

If x is odd, then the LHS is even, but the RHS is odd. This implies $x = 2k$. If we instead write the equation as

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

then we factor the LHS side to get

$$(x+1-1)((x+1)^{y-1} + (x+1)^{y-2} + \ldots + (x+1) + 1),$$

so

$$x^{z-1} = (x+1)^{y-1} + (x+1)^{y-2} + \ldots + (x+1) + 1.$$

Since x is even, the RHS must also be even, but since all the terms are odd, y must be even, so $y = 2m$. Thus,

$$(x+1)^{2m} - 1 = x^z,$$

so

$$((x+1)^m - 1)((x+1)^m + 1) = x^z = 2^z \cdot k^z,$$

but $(x+1)^m - 1$ and $(x+1)^m + 1$ are consecutive even integers, so there greatest common factor is 2. This implies one of them gets one 2, and the other gets 2^{z-1} 2s, and one of them gets all of k^z. Note further that $(x+1)^m - 1$ is divisible by x, which implies it contains a $2k$. This implies either $(x+1)^m + 1$ has only a 2 and $(x+1)^m - 1$ has everything else, or $(x+1)^m + 1 = 2^{z-1}$ and $(x+1)^m - 1 = 2k^z$. The first case is impossible since that would imply

$$2 - 2^{z-1}k^z = 2,$$

so k would have to be 0, which would make $x = 0$, which contradicts the fact $x > 1$. Thus, the latter case yields

$$2^{z-1} > 2k^z,$$

so

$$2^{z_2} > k^z,$$

which implies $k = 1$, so $x = 2$. Thus, if we plug this back in we get

$$3^m - 1 = 2,$$

so $m = 1$. This implies $y = 2$, so

$$3^2 - 2^z = 1,$$

so $z = 3$. Thus, the only possible solution is $(2, 2, 3)$.

Example (Poland MO). Find the integer solution(s) for equation

$$x^{2000} + 2000^{1999} = x^{1999} + 2000^{2000}.$$

Solution. Let us take mod 1999:

$$x^{2000} + 1 \equiv x^{1999} + 1 \pmod{1999},$$

$$x^{1999}(x-1) \equiv 0 \pmod{1999}.$$

Thus, because 1999 is prime, either $x \equiv 0$ or $1 \pmod{1999}$. Note that

$$x^{2000} - x^{1999} = 1999 \cdot 2000^{1999},$$

so

$$(x-1) \cdot x^{1999} = 1999 \cdot 2000^{1999},$$

so unless $x = 0$, we cannot have $x \equiv 0 \pmod{1999}$. $x = 0$ does not work, so $x \equiv 1 \pmod{1999}$. Note that the LHS is monotonically increasing, so only one solution exists. This solution is $x = 2000$ by trial and error (and simple trial and error at that), so $x = 2000$ is the only solution.

4 Problems

Minimum is [40 ♟]. 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 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

[2 ♟] Problem 2 (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 $a - d$?

[2 ♟] Problem 3 (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?

[2 ♟] Problem 4 (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?

[3 ♟] Problem 5 (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?

[4 ♟] Problem 6 (AIME II 2000/2)
A point whose coordinates are both integers is called a lattice point. How many lattice points lie on the hyperbola $x^2 - y^2 = 2000^2$?

[4 ♟] Problem 7 (AIME I 2015/3)
There is a prime number p such that $16p + 1$ is the cube of a positive integer. Find p.

[4 ♟] Problem 8 (AIME I 2008/4)
There exist unique positive integers x and y that satisfy the equation $x^2 + 84x + 2008 = y^2$. Find $x + y$.

[6 ♟] Problem 9 (Moscow MO 1944)
Find all integer solutions of

$$x + y = x^2 - xy + y^2.$$

[6 ♟] Problem 10 (Italy MO 1995)

Find all pairs of positive integers x, y such that

$$x^2 + 615 = 2^y.$$

[9 ♟] Problem 11 (USAMO 1979)

Find all integer solutions of the equation

$$x_1^4 + x_2^4 + \ldots + x_{14}^4 = 1599.$$

[9 ♟] Problem 12 (East Germany 1973)

Find all integer solutions to the equation

$$x(x+1)(x+7)(x+8) = y^2.$$

[9 ♟] Problem 13 (Russia MO 1986)

Let x and y be integers satisfying

$$\frac{x+y}{x^2 - xy + y^2} = \frac{3}{7}.$$

Find the sum of all possible values of y.

[13 ♟] Problem 14 (USAJMO 2011/1)

Find, with proof, all positive integers n for which $2^n + 12^n + 2011^n$ is a perfect square.