初等数论

吴 伊 涛

2022 年春

Diophantine Equations

What is a Diophantine Equation?

- $x^3 + 2022x + 404 = 0$
- $5x + 6y + 8z = 9$
- $x^2 + y^2 = z^2$
- $x^{2022} + y^{2022} = z^{2022}$
- $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$
- $y^x - x^y = 1$
- $e^{x+y} - \sin(xy) = 2022$

Diophantine Equations

In what follows, we call a Diophantine Equation an equation of the form

$$f(x_1, \cdots, x_n) = 0 \quad (*)$$

where f is an n-variable function.

If f is a polynomial with integral coefficients, then (*) is called an algebraic Diophantine equation.

Examples:

- $5x + 6y + 8z = 9$ is a(an) (algebraic) Diophantine equation.
- $x^2 + y^2 = z^2$ is a(an) (algebraic) Diophantine equation.

- $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$ is a Diophantine equation(and can be translated into an algebraic Diophantine equation).

- $y^x - x^y = 1$ is a Diophantine equation.

Def. An n-tuple $(t_1, \cdots, t_n) \in \mathbb{Z}^n$ satisfying (*) is called a solution of (*). An equation having one or more solutions is called solvable, otherwise, it is called unsolvable.

Examples:

- $5x + 6y + 8z = 9$ is solvable because $x = -1, y = 1, z = 1$ is a solution of it.
- $x^2 + y^2 = z^2$ is solvable because $x = 3, y = 4, z = 5$ is a solution of it.
- $2x = 1$ is unsolvable because there doesn't exist an integer t such that $2t = 1$(or, the solution of the original solution in $\mathbb{Q}$ is $\frac{1}{2}$, which is not an integer.)

3 basic questions

- **Q1**: Is the equation solvable?
- **Q2**: If it is solvable, how many solutions does it have?
- **Q3**: If it is solvable, find all its solutions.

A trivial case

Let $a, b \in \mathbb{Z}$, $a \neq 0$, consider a Diophantine equation

$$ax = b \quad (*)$$

Clearly, we have:

- (*) is solvable iff $a|b$.
- If (*) is solvable, then it has a unique solution.
- If (*) is solvable, divide (*) by a, we get the unique solution of (*):

$$x = \frac{b}{a}$$

Case $ax^2 + bx + c = 0$

Now, consider a Diophantine equation

$$ax^2 + bx + c = 0 \quad (*)$$

where $a, b, c \in \mathbb{Z}$ and $a, c \neq 0$(why we assume $c \neq 0$?).

Of course, we can solve (*) via the formula:

$$x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$$

where $\Delta = b^2 - 4ac$.

So, (*) is solvable iff one of $\frac{-b-\sqrt{\Delta}}{2a}, \frac{-b+\sqrt{\Delta}}{2a}$ is an integer...

Let’s consider (*) in a number theoretic way.

(*) can be rewritten as:

$$(ax + b)x = -c$$

So, if t is an integral solution of (*), then t is a divisor of c.

Thus, to get all integer solutions of (*), we just need to consider all factors of c: $c_1, c_2, \cdots, c_n$, and check if $ac_i^2 + bc_i + c = 0$.

Example: Solve $3x^2 - 7x + 2 = 0$

Solution:

If x_0 is a solution, then $x_0|2$, so $x_0 \in \{1, -1, 2, -2\}$.

When $x_0 = 1$, $3x_0^2 - 7x_0 + 2 = -2 \neq 0$, so $x_0 = 1$ is not a solution.

When $x_0 = -1$, $3x_0^2 - 7x_0 + 2 = 12 \neq 0$, so $x_0 = -1$ is not a solution.

When $x_0 = 2$, $3x_0^2 - 7x_0 + 2 = 0$, so $x_0 = 2$ is a solution.

When $x_0 = -2$, $3x_0^2 - 7x_0 + 2 = 28 \neq 0$, so $x_0 = -2$ is not a solution.

So $3x^2 - 7x + 2 = 0$ has a unique solution $x = 2$.

Case $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$

Now, consider a Diophantine equation

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \quad (**)$$

where $a_0, a_1, \cdots, a_n$ are integers and $a_0, a_n \neq 0$.

Clearly, (**) can be rewritten as:

$$(a_nx^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)x = -a_0$$

So, if t is an integral solution of (**), then t is a divisor of a_0.

Thus, to get all integer solutions of (**), we just need to consider all factors of a_0: $t_1, t_2, \cdots, t_l$, and check if $a_nt_i^n + a_{n-1}t_i^{n-1} + \cdots + a_1t_i + a_0 = 0$.

Example: Solve $x^4 + 2x^3 - 5x^2 - 4x + 6 = 0$

Solution:

If x_0 is a solution, then $x_0|6$, so $x_0 \in \{\pm1, \pm2, \pm3, \pm6\}$.

When $x_0 = 1$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 0$, so $x_0 = 1$ is a solution.

When $x_0 = -1$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 4 \neq 0$, so $x_0 = -1$ is not a solution.

When $x_0 = 2$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 10 \neq 0$, so $x_0 = 2$ is not a solution.

When $x_0 = -2$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = -6 \neq 0$, so $x_0 = -2$ is not a solution.

When $x_0 = 3$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 84 \neq 0$, so $x_0 = 3$ is not a solution.

When $x_0 = -3$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 0$, so $x_0 = -3$ is a solution.

When $x_0 = 6$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 1530 \neq 0$, so $x_0 = 6$ is not a solution.

When $x_0 = -6$, $x_0^4 + 2x_0^3 - 5x_0^2 - 4x_0 + 6 = 714 \neq 0$, so $x_0 = -6$ is not a solution.

So $x^4 + 2x^3 - 5x^2 - 4x + 6 = 0$ has integer solutions $x = 1, x = -3$.

Remarks

- In fact, we can find all **rational** solutions of the equation $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, where where $a_0, a_1, \cdots, a_n$ are integers and $a_0, a_n \neq 0$:

  Prop Let $x_0 = \frac{p}{q}(p, q$ are coprime integers) be a rational root of an integral coefficients polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then

$$q|a_n \quad and \quad p|a_0$$

Try to find all rational solutions of previous equations.

- An important corollary of the above proposition is:

  Cor. Let x_0 be a rational root of a monic integral coefficients polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then x_0 is an integer.

  By this corollary, we get a new proof of ”$\sqrt{2}$ is an irrational number”:

  Assume not, $\sqrt{2}$ is rational, consider a monic integral coefficients polynomial

  $$x^2 - 2$$

  $\sqrt{2}$ is a rational root of this polynomial.

  Since all rational roots of this polynomial are integers, we get $\sqrt{2}$ is an integer. But $\sqrt{2} \approx 1.414$ is not an integer. A contradiction. □

Similarly, we get a new proof of ”if m is not a square, then $\sqrt{m}$ is irrational”:

Let m be an integer, assume $\sqrt{m}$ is rational, consider a monic integral coefficients polynomial

$$x^2 - m$$

$\sqrt{m}$ is a rational root of this polynomial.
Since all rational roots of this polynomial are integers, we get $\sqrt{m}$ is an integer, i.e. m is a square. □

algebraic number and algebraic integer

Def. An algebraic number α is a complex number α that is a root of an integral coefficients polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0(a_0, a_1, \cdots, a_n$ are integers).

An algebraic integer ω is is a complex number ω that is a root of a monic integral coefficients polynomial $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0(a_0, a_1, \cdots, a_{n-1}$ are integers).

Example:

- Every algebraic integer is an algebraic number.
- $\sqrt{2}$ is an algebraic integer since $\sqrt{2}$ is a root of $x^2 - 2$.
- Every rational number $\frac{p}{q}$ is an algebraic number since $\frac{p}{q}$ is a root of $qx - p$.

Prop.A rational number $r \in \mathbb{Q}$ is an algebraic integer if and only if $r \in \mathbb{Z}$.

Thus $\frac{3}{5}$ is an algebraic number, but not an algebraic integer.

Case $ax + by = c$

Now, consider a Diophantine equation

$$ax + by = c \quad (*)$$

where $a, b, c \in \mathbb{Z}$ and $a, b \neq 0$.

Recall 3 basic questions of an equation are:

- **Q1**: Is the equation solvable?
- **Q2**: If it is solvable, how many solutions does it have?
- **Q3**: If it is solvable, find all its solutions.

The solvability of $ax + by = c$

$ax + by = c$ is solvable.

$\Leftrightarrow \exists u, v \in \mathbb{Z}$, s.t. $au + bv = c$.

$\Leftrightarrow c \in (a, b)$.

$\Leftrightarrow c \in (gcd(a, b))$.

$\Leftrightarrow gcd(a, b)|c$.

Prop. Let a, b, c be integers, the Diophantine equation $ax + by = c$ is solvable iff $gcd(a, b)|c$.

Examples

- $25x + 30y = 35$ is solvable since $gcd(25, 30) = 5|35$.
- $111x+48y = 77$ has no integer solutions since $gcd(111, 48) = 3 \nmid 77$.

Cor. Let a, b, c be integers and a, b coprime, then the Diophantine equation $ax + by = c$ is always solvable.

Examples

- $11x + 48y = c$ is solvable for all integers $c \in \mathbb{Z}$.

How to find $gcd(a, b)$ efficiently?

Euclidean Algorithm(辗转相除法)

Input: $a, b \in \mathbb{Z}^+$.

Step1: Use Division Algorithm, $a = q_1 b + r_1$, $0 \leq r_1 \leq b - 1$.

Step2: If $r_1 = 0$, then $gcd(a, b) = b$.

If $r_1 \neq 0$, then use Division Algorithm again,

$b = q_2 r_1 + r_2$, $0 \leq r_2 \leq r_1 - 1$.

Step3: If $r_2 = 0$, then $gcd(a, b) = r_1$.

If $r_2 \neq 0$, then use Division Algorithm again,

$r_1 = q_3 r_2 + r_3$, $0 \leq r_3 \leq r_2 - 1$.

......

Stepk+2: If $r_{k+1} = 0$, then $gcd(a, b) = r_k$.

Lemma. Let $a, b, k \in \mathbb{Z}$, then

$$gcd(a, b) = gcd(a - kb, b)$$

Idea of proof: It suffices to prove $(a, b) = (a - kb, b)$.

Assume $r_{k+1} = 0$ and $r_k \neq 0$.

In fact,

$$gcd(a, b) = gcd(a - q_1 b, b) = gcd(r_1, b)$$

$$= gcd(b, r_1) = gcd(b - q_2 r_1, r_1) = gcd(r_2, r_1)$$

$$= gcd(r_1, r_2) = gcd(r_1 - q_3 r_2) = gcd(r_3, r_2)$$

$$= gcd(r_2, r_3) = \cdots$$

$$= \cdots$$

$$= gcd(r_k, r_{k+1}) = gcd(r_k, 0) = r_k$$

E.g. $a = 5181103$, $b = 228408$, find g.c.d. (a, b).

Sol:

$a = 5181103$	
$b = 228408$	$22 = q_1$
$r_1 = 156127$	$1 = q_2$
$r_2 = 72281$	$2 = q_3$
$r_3 = 11565$	$6 = q_4$
$r_4 = 2891$	$4 = q_5$
$r_5 = 1$	$2891 = q_6$
$r_6 = 0$	

Thus g.c.d. $(5181103, 228408) = 1$.

Remarks

- Euclidean Algorithm is an efficient algorithm. The worst case is a, b are consecutive terms in the Fibonacci sequence $\{f_n\}$. Say $a = f_{n+2}$ and $b = f_{n+1}$, then it costs n division algorithms to find $gcd(a, b)$. In general, the number n of division algorithms to find $gcd(a, b)$ satisfying the condition:

$$f_{n+1} \leq min\{a, b\}$$

WLOG, assume $a \geq b$, recall that

$$f_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$$

So

$$n \leq [log_\phi \sqrt{5}b], \quad where \quad \phi = \frac{1+\sqrt{5}}{2}$$

- **Lame's Theorem**

  The number of divisions needed to find the greatest common divisor of two positive integers using the Euclidean algorithm does not exceed five times the number of decimal digits in the smaller of the two integers.

  (See Section3.4 of textbook.)

- **Theorem**(Dixon, 1970)

  Let $L(a, b)$ be the number of divisions needed to find $gcd(a, b)$ with $a \geq b$, then

  $$0.5 \log b \leq L(a, b) \leq 2.08(\log b + 1)$$

  for almost all pairs (a, b) with $a \geq b$.

- **Theorem**(Dixon, 1970)

  Notations as above, $\forall \epsilon > 0$,

  $$|L(a,b) - \frac{12 \log 2}{\pi^2} \log b| < (\log b)^{\frac{1}{2}+\epsilon}$$

  for almost all pairs (a, b) with $a \geq b$.

Now, let's consider the number of solutions of the Diophantine equation

$ax + by = c$.

If $ax + by = c$ is solvable and (x_0, y_0) is a solution, then we have a 1-1 correspondence:

$$\{ \text{ Solutions of } ax + by = c \} \quad \longleftrightarrow \quad \{ \text{ Solutions of } ax + by = 0 \}$$

$$(u, v) \to (u - x_0, v - y_0)$$

$$(s + x_0, t + y_0) \leftarrow (s, t)$$

Clearly, $ax + by = 0$ has infinitely many solutions:

$(b, -a), \quad (2b, -2a), \quad (3b, -3a), \cdots$

Prop. The Diophantine equation $ax+by=c$ has infinitely many integer solutions if $gcd(a,b)|c$.

Cor. If a,b are coprime integers, then the Diophantine equation $ax+by=c$ has infinitely many integer solutions.

We also find:

If we can find a solution of $ax + by = c$(called a special solution of $ax + by = c$), and find all solutions of $ax + by = 0$(called general solutions of $ax + by = 0$), then we find all solutions of $ax + by = c$.

Let's find the general solutions of $ax + by = 0$ first.

Note that $(kb, -ka)$, $\quad k \in \mathbb{Z}$ are solutions of $ax + by = 0$, but they may not cover all solutions of $ax + by = 0$. e.g. $(1, -1)$ is a solution of $2x + 2y = 0$ but $(1, -1) \neq (2k, -2k)$ for all integers k.

However...

Prop. If a, b are coprime integers, then the general solutions of the Diophantine equation $ax + by = 0$ are:

$$x = kb, \quad y = -ka \qquad k \in \mathbb{Z}$$

Proof:

If (u, v) is a solution of $ax + by = 0$, then $bv = -au$.

Since $gcd(a, b) = 1$, so $b|u$, say $u = tb$ for some integer t.

Then $v = -ta$.

It's straightforward to check that $x = kb, \quad y = -ka$ is a solution of $ax + by = 0$. □

Cor. Let a, b, c be integers(a, b nonzero), then the general solutions of the Diophantine equation $ax + by = 0$ are:

$$x = \frac{bk}{gcd(a,b)}, \quad y = \frac{-ak}{gcd(a,b)} \qquad k \in \mathbb{Z}$$

Idea of proof: It suffices to show that $\frac{b}{gcd(a,b)}$ and $\frac{a}{gcd(a,b)}$ are coprime.

Example

- The general solutions of $25x + 30y = 0$ are:

$$x = 6k, \quad y = -5k \qquad k \in \mathbb{Z}$$

谢谢！