NUMBER THEORY

UNIT 3   DIOPHANTINE EQUATIONS

1.   Introduction

A Diophantine equation is an equation for which integral solutions are to be found. The most famous type of Diophantine equations in contemporary mathematics is perhaps those dealt with in Fermat's Last Theorem: $x^n + y^n = z^n$. When $n = 2$ this just reduces to the usual Pythagorean identity $x^2 + y^2 = z^2$ for right-angled triangles, and we are familiar with its positive integer solutions: (3, 4, 5); (5, 12, 13) etc. Fermat (1601–1665) asserted that when $n > 2$, the equation $x^n + y^n = z^n$ has no solution in positive integers. It was not until 1994 that this was proved by the English mathematician Andrew Wiles.

Solving a Diophantine equation means finding integer values of the variables (or positive integers or non-negative integers, depending on the question) which satisfy the equation. The techniques of solving Diophantine equations are best illustrated using examples. We shall discuss four specific techniques, namely, algebraic methods, modular arithmetic, inequality bounds and infinite descent. There is no general rule on which technique to use and the best way to gain experience is by practice.

2.   Algebraic Methods

In algebraic methods, we try to arrange the terms and simplify the equations properly and apply the basic theorems on divisibility. We usually try to write one side as the product of two or more factors or take out 'integer parts' in the expressions.

Example 2.1.

Find all integers n for which $n^2 - 2n + 4$ is a multiple of $n + 3$.

(This can be considered as the Diophantine equation $\dfrac{n^2 - 2n + 4}{n + 3} = k$ for integers n, k.)

Solution.

Note that

$$\frac{n^2 - 2n + 4}{n + 3} = n - 5 + \frac{19}{n + 3}.$$

So the condition is satisfied if and only if $n + 3$ divides 19. Since 19 is prime, $n + 3$ can only be 19, 1, –1 or –19. Hence we obtain four possible values of n, namely, 16, –2, –4 and –22. It is easy to check that these values of n satisfy the requirement.

Example 2.2.

Find all natural numbers x, y for which $\dfrac{5}{x} + \dfrac{6}{y} = 1$.

Solution.

Multiplying both sides by xy and transposing terms, we get $xy - 6x - 5y = 0$.

To make the left hand side the product of two factors, we add 30 on both sides and factorise:

$$(x - 5)(y - 6) = 30$$

Note that the two factors on the left are of the same sign. Moreover, since x, y are both positive, the two factors must be both positive. Hence the two factors may take values

$$(x - 5,\ y - 6) = (1, 30);\ (2, 15);\ (3, 10);\ (5, 6);\ (6, 5);\ (10, 3);\ (15, 2);\ (30, 1)$$

and these correspond to the solutions

$$(x, y) = (6, 36);\ (7, 21);\ (8, 16);\ (10, 12);\ (11, 11);\ (15, 9);\ (20, 8);\ (35, 7).$$

3. Modular Arithmetic

A very common technique of solving Diophantine equations is to consider the equation modulo certain integers. For example we can consider the parity of the variables (i.e. mod 2), or we can show that some variables must be multiples of certain integers.

The concept of 'quadratic residues' also plays an important role in solving Diophantine equations. An integer c is said to be a **quadratic residue** modulo m if there exists an integer x such

that $x^2 \equiv c \pmod{m}$. For instance, we know that all squares are either congruent to 0 or 1 modulo 4, so 0 and 1 are quadratic residues modulo 4, while 2 and 3 are non-residues.

Example 3.1.

Find all integers x, y such that $15x^2 - 7y^2 = 9$.

Solution.

Note that $7y^2 = 15x^2 - 9 \equiv 1 \pmod 5$, so $y^2 \equiv 3 \pmod 5$.

However, $0^2 \equiv 0$, $1^2 \equiv 4^2 \equiv 1$, $2^2 \equiv 3^2 \equiv 4 \pmod 5$, so 3 is a quadratic non-residue modulo 5.

So the equation has no solution.

Alternative Solution.

Since 3 divides 15 and 9, 3 also divides $7y^2$ and hence 3 divides y.

Consequently, since 9 divides $7y^2$ and 9, it also divides $15x^2$. Thus 3 divides x.

Setting $x = 3a$ and $y = 3b$ and simplifying, the equation becomes $15a^2 - 7b^2 = 1$.

This implies $b^2 \equiv 2 \pmod 3$, which is impossible, as 2 is a quadratic non-residue modulo 3.

So there is no solution.

Example 3.2.

Find all integer solutions to the equation $x^3 + 2y^3 + 4z^3 = 9w^3$.

Solution.

Clearly, (0, 0, 0, 0) is a solution.

Suppose there is another solution. Without loss of generality, we may assume that x, y, z, w have no common factor greater than 1, for otherwise we can simply divide the whole equation by the cube of the common factor.

Now $x^3 + 2y^3 + 4z^3 \equiv 0 \pmod 9$, but we check that n^3 can only be congruent to 1, 0, −1 $\pmod 9$. The only possibility is that x, y, z are all congruent to 0 $\pmod 9$, i.e. 3 divides x, y and z. But this implies that the left hand side of the equation is divisible by 27, and thus forces 3 to divide w as well. This contradicts our assumption that x, y, z, w are relatively prime.

Hence the only solution is $(x, y, z, w) = (0, 0, 0, 0)$.

Example 3.3.

Find all pairs of prime numbers (p, q) such that $p^3 - q^5 = (p+q)^2$.

Solution.

Clearly, $p = 3$ yields no solution while $q = 3$ yields the solution $(7, 3)$.

Now suppose p, q are not equal to 3. Then $p, q \equiv 1$ or -1 (mod 3).

If $p \not\equiv q$ (mod 3), then $3 \mid p + q$, but $3 \nmid p^3 - q^5$.

If $p \equiv q$ (mod 3), then $3 \mid p^3 - q^5$, but $3 \nmid p + q$.

Therefore there can be no other solutions. The only solution is $(7, 3)$.

4. Inequality bounds

In many cases, it is obvious that one side of an equation would 'grow faster' than the other side as the variables get large. In such cases solutions to the equations cannot be 'too large', and so we may apply inequalities to establish bounds for the variables.

Example 4.1.

Find all non-negative integers a, b such that $a - b = a^2 + ab + b^2$.

Solution.

Clearly the right hand side 'seems' to be larger than the left hand side.

Indeed, we have $a - b \leq a \leq a^2 \leq a^2 + ab + b^2$.

Equality holds only if $b = 0$ and $a = 0$ or 1.

It is easy to check that $(0, 0)$ and $(1, 0)$ are solutions, and these are the only solutions.

Example 4.2.

Find all integers x, y such that $x^3 + y^3 = (x+y)^2$.

Solution.

Since $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$, $x+y$ is a common factor of both sides. Hence $(k, -k)$ is a solution for all integers k.

Now suppose $x \neq -y$. We cancel out the common factors on both sides to obtain

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

Multiplying by 2 and transposing terms, we have

$$2x^2 - 2xy + 2y^2 - 2x - 2y = 0.$$

Completing squares, we get

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

It follows that $x - y$, $x - 1$ and $y - 1$ can only be equal to -1, 0 or 1.

By direct checking, we find that (0, 1), (1, 0), (1, 2) and (2, 1) are solutions.

Hence all the solutions are (0, 1), (1, 0), (1, 2) (2, 1) and $(k, -k)$ for any integer k.

Example 4.3.

Find all positive integers a, b such that $\dfrac{2^a + 1}{2^b - 1}$ is an integer.

Solution.

When $b = 1$, a can be any positive integer.

When $b = 2$, 3 divides $2^a + 1$, so a can be any odd positive integer.

If $b > 2$, write $a = qb + r$, $0 \leq r < b$. We have

$$\frac{2^a + 1}{2^b - 1} = 2^{a-b} + 2^{a-2b} + \cdots + 2^{a-qb} + \frac{2^r + 1}{2^b - 1},$$

which cannot be an integer since $0 < \dfrac{2^r + 1}{2^b - 1} < 1$.

Hence all the solutions are $(k, 1)$, $(2h-1, 2)$ where k, h are arbitrary positive integers.

5. Infinite Descent

In infinite descent we show that if a positive solution exists, we can always find a 'smaller' solution. Since this process cannot carry on indefinitely, we come to the conclusion that the equation has no positive solutions. Alternatively, we may show that if a positive solution exists, one or more of the variables must be divisible any power of a certain integer, thereby obtaining a contradiction.

Example 5.1.

Find all non-negative integers *x, y, z* such that $x^3 + 2y^3 = 4z^3$.

Solution.

Clearly, $(0, 0, 0)$ is a solution.

Suppose (x_1, y_1, z_1) is another solution. Then *x* is even since $2y^3$ and $4z^3$ are even. Write $x_1 = 2x_2$. Putting into the equation and dividing by 2, we have

$$4x_1^3 + y_1^3 = 2z_1^3,$$

so y_1 is even. Again writing $y_1 = 2y_2$, we see that z_1 is even, so $z_1 = 2z_2$.

This process can be repeated again and again, so that x_2, y_2 and z_2 are all even, and so on.

It follows that x_1, y_1 and z_1 are divisible by any power of 2, which is not possible unless they are equal to zero.

Thus the only solution is $(0, 0, 0)$.

Example 5.2.

(USAMO 1976) Find all non-negative integers *a*, *b*, *c* such that $a^2 + b^2 + c^2 = a^2b^2$.

Solution.

We claim that *a*, *b*, *c* must all be even. Recall that the square of an odd integer is always congruent to 1 (mod 4) and the square of an even integer is always congruent to 0 (mod 4). From the equation, we see that if *a*, *b* are even, then *c* must be even. If *a*, *b* are both odd, the right side is congruent to 1 (mod 4), but the left side cannot be. If exactly one of *a* and *b* is odd, then the right side is congruent to 0 (mod 4), but the left side is not. This establishes the claim.

Clearly, $(0, 0, 0)$ is a solution. Suppose there is another solution (a_0, b_0, c_0). Recall that all variables must be even, so we let $a_0 = 2a_1$, $b_0 = 2b_1$ and $c_0 = 2c_1$. Putting into the equation and dividing both sides by 4, we get $a_1^2 + b_1^2 + c_1^2 = 4a_1^2 b_1^2$. By exactly the same argument as before, we see that a_1, b_1 and c_1 must all be even again. Repeating this argument, a_0, b_0 and c_0 have to be divisible by any power of 2, which is not possible unless all of them are zeros.

So $(0, 0, 0)$ is the only solution.

6. Miscellaneous Examples

The techniques described above are by no means exhaustive. Nor does every problem fit into one of the above types. In this section we will look at some miscellaneous examples.

Example 6.1.

Prove that the equation $x^3 + y^3 + z^3 = x^2 + y^2 + z^2$ has infinitely many integer solutions.

Solution.

Setting $z = -y$, we get $x^3 = x^2 + 2y^2$.

Setting $y = mx$, we get $x^3 = x^2 + 2(mx)^2$, giving $x = 1 + 2m^2$ if $x \neq 0$.

Hence $(1 + 2m^2, m + 2m^3, -m - 2m^3)$ is a solution for any integer m, and it is clear that we get infinitely many solutions as m varies.

Example 6.2.

Prove that for all positive integers n, there exist positive integers x, y, z such that
$$x^2 + y^2 + z^2 = 421^n.$$

Solution.

If $x^2 + y^2 + z^2 = 421^n$, then $(421x)^2 + (421y)^2 + (421z)^2 = 421^{n+2}$.

Hence we need only check the cases $n = 1$ and $n = 2$.

Indeed, we have $4^2 + 9^2 + 18^2 = 421$ and $20^2 + 21^2 + 420^2 = 421^2$. The result follows.

Example 6.3.

(IMO 1997) Find all pairs (a, b) of integers $a \geq 1$, $b \geq 1$ that satisfy the equation $a^{b^2} = b^a$.

Solution.

Let $d = \gcd(a, b)$. Write $a = du$ and $b = dv$. Then $\gcd(u, v) = 1$ and the equation becomes

$$(du)^{dv^2} = (dv)^u.$$

Case 1: $dv^2 = u$

In this case $v \mid u$, so we must have $u = v = 1$, $d = 1$ and hence $a = b = 1$. We check that $(1, 1)$ is a solution.

Case 2: $dv^2 > u$

The equation becomes $d^{dv^2-u} u^{dv^2} = v^u$. It follows that $u \mid v$, so $u = 1$.

Consequently we have $d^{dv^2-1} = v$. The case $d = 1$ gives $v = 1$ and $a = b = 1$ as before. For $d \geq 2$ there is no solution as $d^{dv^2-1} \geq 2^{2v^2-1} > v$.

Case 3: $dv^2 < u$

The equation becomes $u^{dv^2} = d^{u-dv^2} v^u$. It follows that $v \mid u$, so $v = 1$. Consequently we have

$$u^d = d^{u-d}. \tag{*}$$

Note that $d = dv^2 < u$, from (*) we have $d < u - d$, i.e. $u > 2d$.

Write $u = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $d = p_1^{\beta_1} \cdots p_n^{\beta_n}$.

Putting into (*) and comparing powers, we have $d\alpha_i = (u-d)\beta_i$. So $\beta_i < \alpha_i$ for all i, i.e. $d \mid u$.

Write $u = kd$, where $k \geq 3$ is an integer. From (*), we have

$$k = d^{k-2}.$$

When $k = 3$, we have $d = 3$, $u = 9$, $v = 1$, $a = 27$, $b = 3$. We check that $(27, 3)$ is a solution.

When $k = 4$, we have $d = 2$, $u = 8$, $v = 1$, $a = 16$, $b = 2$. We check that $(16, 2)$ is a solution.

When $k \geq 5$, there is no solution since $d^{k-2} \geq 2^{k-2} > k$.

Therefore the only solutions are $(1, 1)$, $(27, 3)$ and $(16, 2)$.

7. Exercises

1. Find all integer solutions to the following Diophantine equations.

   (a) $\dfrac{5}{x} - \dfrac{7}{y} = 2$

   (b) $x_1{}^4 + x_2{}^4 + \cdots + x_{14}{}^4 = 1599$

   (c) $y^2 = x^3 + 7$

   (d) $3 \cdot 2^x + 1 = y^2$

   (e) $xy + yz + zx = xyz + 2$

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

   (g) $3(xy + yz + zx) = 4xyz$

2. Find all positive integers a, b, n and prime numbers p such that p is prime and $p^n = a^3 + b^3$.

3. (APMO 1993) Find all positive integers n such that the equation $x^n + (2+x)^n + (2-x)^n = 0$ has an integer solution.

4. Prove that for all positive integers n, there exist integers x and y such that $x^2 + xy + y^2 = 7^n$.

5. Let a, b, c be positive integers. The triple (a, b, c) is called a **Pythagorean triple** if it satisfies $a^2 + b^2 = c^2$ (i.e. the triangle with side lengths a, b, c is right-angled at the angle opposite the side with length c). If the G.C.D. of a, b, c is 1, then it is called a **primitive solution**.

   (a) Show that if (a, b, c) is a Pythagorean triple, then so is (ka, kb, kc) for any positive integer k.

   (b) Let u, v be relatively prime natural numbers of opposite parity and $u > v$. Show that
   $$\left(u^2 - v^2,\, 2uv,\, u^2 + v^2\right)$$
   is a primitive solution to the equation $a^2 + b^2 = c^2$.

   (c) Follow the steps below to show that every primitive solution is of the form in (b).

       (1) Let (a, b, c) be a primitive solution. Then a and b are of different parity.

       (2) Set $m = \dfrac{c+a}{2}$, $n = \dfrac{c-a}{2}$. Then $mn = \left(\dfrac{b}{2}\right)^2$.

(3) m and n must be perfect squares, say $m = u^2$ and $n = v^2$.

6. Using infinite descent, show that the equation $x^4 + y^4 = z^2$ has no solution in positive integers. (This proves Fermat's Last Theorem for the case $n = 4$.)

7. (IMO 1998) Determine all pairs (a, b) of positive integers such that $ab^2 + b + 7$ divides $a^2 b + a + b$.