Indtroduction to Diophantine Equations

Qingyun Wang

November 13, 2011

(In the very beginning, divide the class into 4 groups, we will constantly do some competions, and the winners will earn a certain number of stars. The final winner will be the team with the most number of stars)
Diophantus, sometimes called "the father of algebra", was an Alexandrian Greek mathematician and the author of a series of books called Arithmetica. These texts deal with solving certain equations, which nowadays are called Diophantine equations, many of which are now lost.

Little is known about the life of Diophantus. He lived in Alexandria, Egypt, probably from between 200 and 214 to 284 or 298 AD. Much of our knowledge of the life of Diophantus is derived from a 5th century Greek anthology of number games and strategy puzzles. One of the problems (sometimes called his epitaph) states:

'Here lies Diophantus,' the wonder behold.
Through art algebraic, the stone tells how old:
'God gave him his boyhood one-sixth of his life,
One twelfth more as youth while whiskers grew rife;
And then yet one-seventh ere marriage begun;
In five years there came a bouncing new son.
Alas, the dear child of master and sage
After attaining half the measure of his father's life chill fate took him.
After consoling his fate by the science of numbers for four years, he ended his life.'

Competetion 1: Figure out how many years Diaphantus lived. The first two correct answers will get 1 stars

each. (84)

This is a determined equation. (number of unkowns equal to number of equations). Let's look at an example of an undetermined equation:

Example: Suppose dolls sell for 3 dollars each and toy train set sell for 4 dollars. A store sells only dolls and toy train sets. The total amount received is 40 dollars. How many of each were sold? List all possibilities:

(10, 0), (7, 4), (4, 8), (1,2)

Competetion 2: Find as many solutions as possible. Each solution worth half a star.
Look at the patern of all the solutions, write them in a column, what do you find?

Now let's do a game based on diaphantine equations, called Guessing the numbers:
Competetion 3: I have two natural numbers X(20) and Y(16) in my mind, Satisfy the Diophantine equations 3X+2Y=180. As we can see from the first example, there are many solutions. Now I am going to reveal more and more properties of these two numbers. After each property is revealed, you can present an answer satisfy all the properties listed. If you find such a pair but not the answer in my mind, you can earn half a star. If you figure out the correct answer, you will earn additional 1 stars.

Their sum is ≥ 75

They are both even

One of them is a perfect square

Their difference is divisible by 4.

One of them is a multiple of 21.

X=4.

Now let's turn to a different type of diaphantine equation.

$$10X - 14Y = 16$$

Competetion 3: Find as many solutions as you can. Each solution worth half a star, you can earn up to 2 stars in this competetion.

All these are called linear Diophantine equations. A general equation is given by aX+bY=c, where a, b, c are whole numbers. From what we observed, If x_0, y_0 is a solution, Then all solutions are of the form: $X = x_0 + kb$, $Y = y_0 - ka$, providing that gcd$< a, b >= 1$, i.e. a, b are coprime.
What if a,b are not coprime? divide the equation by their greatest common divisor.

How to prove this and how can we find one solution? The idea is similar to Euclid Algorithm.

Competetion 4: Find all solutions of $7X + 18Y = 208$. The first two correct answers get 2 stars each, the rest teams get 1 stars each.

Consider another type of Diophantine equations, called the Pythagorean triple: $X^2 + Y^2 = Z^2$ We are looking for integer solutions.

Let's do another game based on this: Guessing the Pythagorean triple: $X^2 + Y^2 = Z^2$, each number are between 1 and 100.

X is even

Y+Z is a twice as a perfect square

Y-Z is also twice as a perfect square

X is a product of 3 distinct primes.

Y is a perfect square

Z is less than 50.

Z-X=4.

X+Y=46

Now Since $X^2 = (Y + Z)(Z - Y)$, this suggest us to look for prime factorizations of Y+Z and Y-Z. Suppose Y+Z and Y-Z are coprime, do the following table:
Case 1(Y+Z and Y-Z are coprime):

X	Z+Y	Z-Y	Z	Y
3	9	1	5	4
5	25	1	13	12
15	225	1	113	112
	25	9	17	8
20	No	Solution		

What do you find? Y+Z and Z-Y are both pefect squares!
A proof: Look at the prime factorizations.

What if Y+Z and Z-Y are not coprime?
Case 2(Y+Z and Y-Z has greatest common divisor 2):

X	Z+Y	Z-Y	Z	Y
3	No	Solution		
6	18	2	10	8
10	50	2	26	24
20	200	2	101	99

Case 3(Y+Z and Y-Z has greatest common divisor 6):

X	$Z+Y$	$Z-Y$	Z	Y
3	No	Solution		
6	No	Solution		
18	54	6	30	24
30	150	6	78	72

Let's do a even/odd analysis. We can find that one of X and Y must be even. Without loss of generality, lets assume X is even. Let d be the greatest common divisor of Y+Z and Z-Y, then they are both even, so d=2k. We can then divide d on both sides, and return to the coprime case. So let $Y+Z=2km^2$ and $Z-y=2kn^2$. Then X=2kmn. We can check that this is a general solution to the Phythagorean triple.

Final Competetion: I'll give each team a Pythagoren triple. Battle between two teams: Guessing the other Pythagoren triple, by take turns to ask yes or no questions. (36,15,39) and (27,36,45). The first team figuring out the correct answer win two stars.

Now consider a even more complicated Diophantine equation:

$$X^3 + Y^3 = Z^3$$

There is no solution at all! In general, the Diophantine equation :

$$X^n + Y^n = Z^n$$

has no solution if $n \geq 3$. This is the so called Fermat's last theorem.

Around 1637, Fermat wrote his Last Theorem in the margin of his copy of the Arithmetica next to Diophantus' sum-of-squares problem:
Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

English translation:
it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

Fermat posed the cases of n = 4 and of n = 3 as challenges to his mathematical correspondents, such as Marin Mersenne, Blaise Pascal, and John Wallis. However, in the last thirty years of his life, Fermat never again wrote of his "truly marvellous proof" of the general case.

No successful proof was published until 1995 despite the efforts of countless mathematicians during the 358 intervening years. The final proof of the conjecture for all n came in the late 20th century. In 1984, Gerhard Frey suggested the approach of proving the conjecture through a proof of the modularity theorem for elliptic curves. Building on work of Ken Ribet, Andrew Wiles succeeded in proving enough of the modularity theorem to prove Fermat's Last Theorem, with the assistance of Richard Taylor. Wiles's achievement was reported widely in the popular press, and has been popularized in books and television programs.