From Cubics to Elliptic Curves

Horn OS

1 Introduction

On the 23rd of September, Dr. Andras Hrasko, a renowned Hungarian mathematics researcher and educator, came to give a masterclass on Elliptic Curves to the Mathematical Society. Prior to this talk, he gave the Mathematical Society a set of problems to solve, each related in some way to the elements of his talk. The last of these problems was perhaps the most directly linked to elliptic curves, and was also the only problem to go unsolved. In this article I give a proof.

2 The Problem

Do there exist infinitely many primitive integer solutions to the equation $7x^3 + y^3 = z^3$?

A solution is *primitive* if $\gcd(x, y, z) = 1$. We are interested in non-trivial solutions, those with $x \neq 0$, since the only primitive solutions with $x = 0$ are $(0, 1, 1)$ and $(0, -1, -1)$.

The answer is yes.

The method we will be using is to convert the original equation into an elliptic curve, find one rational base point, and prove that it is possible to find infinitely many more rational points on the curve, which can be transformed back into infinitely many integer solutions to the original equation. We will use the base case $(x, y, z) = (1, 1, 2)$ which clearly satisfies the equation.

3 Turning the Equation into an Elliptic Curve

An elliptic curve is a curve of the form $Y^2 = X^3 + AX + B$. Its rational points (points whose coordinates are both rational) can be "added" together geometrically, which lets us build new points from old ones.

3.1 Forming an elliptic curve in Weierstrass form

Start with the original equation:

$$7x^3 + y^3 = z^3$$

Rearrange it:

$$y^3 + (-z)^3 = -7x^3$$

This is an equation of the form:

$$a^3 + b^3 = nc^3$$

We first treat the general equation $a^3 + b^3 = nc^3$. Let:

$$s = a + b, \qquad d = a - b$$

Then

$$a = \frac{s + d}{2}, \qquad b = \frac{s - d}{2}$$

$$a^3 + b^3 = \frac{(s + d)^3 + (s - d)^3}{8} = \frac{s^3 + 3sd^2}{4}$$

$$s^3 + 3sd^2 = 4nc^3$$

Assume $s \neq 0$. (For our equation $s = y - z$, so $s = 0$ would mean $y = z$ and hence $x = 0$, which is the trivial solution, so nothing is lost.) Divide by s^3:

$$3\left(\frac{d}{s}\right)^2 = 4n\left(\frac{c}{s}\right)^3 - 1$$

Crucially, this relates a square to a cube, so we can achieve a Weierstrass equation by rescaling the two ratios. Let:

$$X = \frac{12nc}{s}, \qquad Y = \frac{36nd}{s}$$

These factors are chosen so that the coefficients of Y^2 and X^3 come out equal. Hence:

$$\frac{c}{s} = \frac{X}{12n}, \qquad \frac{d}{s} = \frac{Y}{36n}$$

Substitute back into the equation:

$$3\left(\frac{Y}{36n}\right)^2 = 4n\left(\frac{X}{12n}\right)^3 - 1$$

Which simplifies to:

$$\frac{Y^2}{432n^2} = \frac{X^3}{432n^2} - 1$$
$$Y^2 = X^3 - 432n^2$$

For our original equation we have:

$$a = y, \qquad b = (-z), \qquad c = x, \qquad n = -7$$

So our elliptic curve in Weierstrass form is:

$$E : Y^2 = X^3 - 21168$$

Where:

$$X = \frac{84x}{z-y}, \qquad Y = \frac{252(y+z)}{z-y}$$

Our base case $(1, 1, 2)$ therefore maps to the point $(84, 756)$ on the elliptic curve. Checking that this point works: $84^3 - 756^2 = 592704 - 571536 = 21168$

3.2 Proving the converse

We need to make sure we can transform the rational points (X, Y) on our elliptic curve back into solutions (x, y, z) to the original equation.

Start from:

$$X = \frac{12nc}{s}, \qquad Y = \frac{36nd}{s}$$
$$\frac{c}{s} = \frac{X}{12n}, \qquad \frac{d}{s} = \frac{Y}{36n}$$
$$\frac{a}{c} = \frac{s+d}{2c} = \frac{1+\frac{d}{s}}{2\frac{c}{s}} = \frac{1+\frac{Y}{36n}}{\frac{X}{6n}} = \frac{36n+Y}{6X}$$

Similarly, since $b = \frac{s-d}{2}$,

$$\frac{b}{c} = \frac{36n-Y}{6X}$$

For our particular equation,

$$a = y, \qquad b = (-z), \qquad c = x, \qquad n = (-7)$$

So:

$$\frac{y}{x} = \frac{Y-252}{6X}, \qquad \frac{z}{x} = \frac{Y+252}{6X}$$

To verify the converse works:

$$\left(\frac{z}{x}\right)^3 - \left(\frac{y}{x}\right)^3 = \frac{1512(Y^2+21168)}{216X^3}$$
$$= \frac{1512X^3}{216X^3}$$
$$= 7$$

Which can be rearranged to:

$$7x^3 + y^3 = z^3$$

Thus the transformation works in both directions. Any solution to $7x^3 + y^3 = z^3$ with $z \neq y$ produces a corresponding point (X, Y) on the elliptic curve $Y^2 = X^3 - 21168$. And, any rational point (X, Y) on the elliptic curve $Y^2 = X^3 - 21168$ provides a rational solution to the equation $7x^3 + y^3 = z^3$, which can be scaled up to an integer solution, with (x, y, z) in the ratio $6X : Y - 252 : Y + 252$.

4 Adding Points on an Elliptic Curve

To find more rational points on the elliptic curve, we must use the elliptic curve group law. It defines the **addition** of two points to find a third point on the curve, or the **doubling** of a single point to find another intersection point.

4.1 Addition

We have two points P and Q on the curve, and we find the third intersection point R of the curve with the line through P and Q. We define

$$P + Q = -R$$

Where $-R$ is the negative[1] of R, which is just its reflection in the X-axis.

The point at infinity, denoted by O, acts as the identity element. Consequently,

$$P + Q + R = O$$

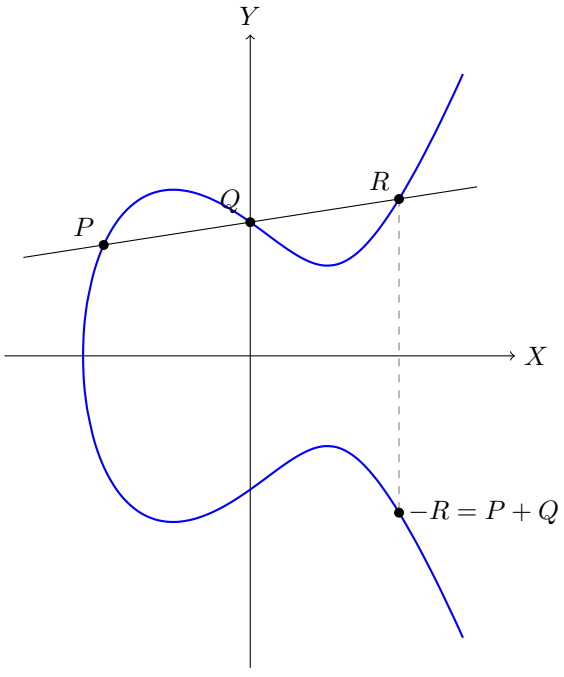


Figure 1: An elliptic curve, with a line through P and Q intersecting the curve again at point R. Reflecting R in the X-axis gives $-R = P + Q$.

4.2 Finding R

Let $P, Q = (X_1, Y_1), (X_2, Y_2)$. Let the gradient of the line passing through those points be m:

$$m = \frac{Y_2 - Y_1}{X_2 - X_1}$$

[1] Also called the inverse of R.

We must find the third intersection point. Take any elliptic curve $Y^2 = X^3 + AX + B$ and any straight line $Y = mX + k$ and equate them to each other.

$$\begin{aligned}(mX + k)^2 = Y^2 &= X^3 + AX + B \\ m^2X^2 + 2kmX + k^2 &= X^3 + AX + B \\ X^3 - m^2X^2 + (A - 2km)X + (B - k^2) &= 0\end{aligned}$$

Using Vieta's formula for the roots of a cubic, we know that the three roots of this equation (i.e. the X-coordinates of the three intersection points) sum to m^2. Thus $X_3 = m^2 - X_1 - X_2$. To find Y_3 we find the equation of the line:

$$\begin{aligned}\frac{Y - Y_1}{X - X_1} &= m \\ Y &= m(X - X_1) + Y_1 \\ Y_3 &= m(X_3 - X_1) + Y_1\end{aligned}$$

Thus we have the coordinates of the 3rd intersection point R. But we define $P + Q = -R$, so we require $-R$, which is just R reflected in the X-axis. Thus:

$$-R = P + Q = \left(m^2 - X_1 - X_2,\ m(X_1 - X_3) - Y_1\right)$$

4.3 Doubling

We have one point P on the curve, and we find the other intersection point R of the curve with the tangent line at P. Since this case is essentially a variant of addition where $P = Q$, we define the doubling operation $P + P = 2P = -R$.

The only difference to the graph is the gradient of the intersecting line, which is found by differentiating the elliptic curve at the point P. For our elliptic curve $Y^2 = X^3 - 21168$, let $Y = f(X)$:

$$\begin{aligned}\frac{d}{dX} f(X)^2 &= \frac{d}{dX}\left(X^3 - 21168\right) \\ 2f(X)f'(X) &= 3X^2\end{aligned}$$

The gradient m in this case is $f'(X)$, so:

$$m = \frac{3X^2}{2f(X)} = \frac{3X^2}{2Y}$$

All the other equations remain the same for finding (X_3, Y_3), except for the fact that $X_3 = m^2 - 2X_1$.

5 Generating Solutions

We only started with one point $P = (84, 756)$, so to find a new point we must first double it to get $2P$. Let's start with the gradient m.

$$\begin{aligned}m &= \frac{3X_P^2}{2Y_P} = \frac{3 \cdot 84^2}{1512} = 14 \\ X_{2P} &= m^2 - 2X_P = 196 - 168 = 28 \\ Y_{2P} &= m(X_P - X_{2P}) - Y_P = 14(84 - 28) - 756 = 28 \\ 2P &= (28, 28)\end{aligned}$$

From this new point we can return to our original equation

$$\begin{aligned}x : y : z &= 6X : Y - 252 : Y + 252 \\ &= 168 : -224 : 280 \\ &= 3 : -4 : 5\end{aligned}$$

Thus $x = 3$, $y = -4$, $z = 5$ is another primitive integer solution to the equation $7x^3 + y^3 = z^3$. We can check this:

$$\begin{aligned}7(3^3) + (-4)^3 &= 7 \cdot 27 - 64 = 125 \\ &= 5^3\end{aligned}$$

We can find further points $3P, 4P, \ldots$ by adding P to $2P$, doubling $2P$, and so on. A remarkable (and non-obvious) fact is that this addition is associative and commutative, so different routes to the same multiple produce the same point on the graph. For instance, one could reach $6P$ by adding P to $5P$, or by doubling $3P$, but the coordinates of $6P$ would remain the same regardless. Each new point produces a different solution to the original equation.

The next two points are:

$$3P = (57, -405)$$

$$4P = (1708, -70588)$$

Which produce primitive integer solutions to the original equation:

$$3P : (x, y, z) = (38, -73, -17)$$

$$4P : (x, y, z) = (183, -1265, -1256)$$

These calculations suggest that we can continue generating solutions indefinitely. However, computing more points is not a proof that the process never repeats. Thus, we must prove it some other way.

6 Infinitely Many Solutions

The order of a point P on an elliptic curve is defined as the lowest possible positive integer N such that $NP = O$, where O is the point at infinity. We aim to prove that P has infinite order on our elliptic curve $Y^2 = X^3 - 21168$. Suppose, for contradiction, that P has finite order N.

We use the reduction theorem for elliptic curves, which states that, for a rational torsion point P of finite order N, if the elliptic curve has good reduction at a prime p,

$$N = \text{ord}(P_p) \cdot p^k$$

for some nonnegative integer k, where P_p is the reduction of P modulo p, and $\text{ord}(P_p)$ is its order in the finite group of points over $\mathbb{F}_p$.[2]

6.1 Good reduction

The curve has good reduction at a prime p if p does not divide its discriminant.

The discriminant of an elliptic curve $Y^2 = X^3 + AX + B$ is

$$\Delta = -16(4A^3 + 27B^2)$$

For our elliptic curve, this discriminant is

$$\Delta = -2^{12} \cdot 3^9 \cdot 7^4$$

Thus the lowest primes coprime to this are 5 and 11, and so they are the lowest primes of good reduction.

6.2 Reduction modulo 5 and 11

If we reduce the curve modulo 5 it becomes $Y^2 = X^3 + 2$ and point P becomes $(4, 1)$. Thereafter:

$$2P_5 = (3, 3)$$

$$3P_5 = (2, 0)$$

Adding a point to its negative gives O. Since the negative of a point (X, Y) is $(X, -Y)$, a point with $Y = 0$ is its own negative, so doubling a point with $Y = 0$ results in the point at infinity O. Thus:

$$2(3P_5) = 6P_5 = O$$

As well, $3P_5 \neq O$ and $2P_5 \neq O$. Since the order divides 6, this means $\text{ord}(P_5) = 6$, so:

$$N = 6 \cdot 5^a$$

[2] $\mathbb{F}_p$ is defined as the finite field of integers modulo p.

for some nonnegative integer a.

Reducing the curve modulo 11, it becomes $Y^2 = X^3 + 7$ and point P becomes $(7, 8)$. Thereafter:

$$\begin{aligned} 2P_{11} &= (6, 6) \\ 3P_{11} &= (2, 2) \\ 4P_{11} &= (3, 10) \\ 5P_{11} &= (4, 7) \\ 6P_{11} &= (5, 0) \end{aligned}$$

Thus:

$$2(6P_{11}) = 12P_{11} = O$$

As well, $6P_{11} \neq O$ and $4P_{11} \neq O$. Since the order divides 12, this means $\text{ord}(P_{11}) = 12$, so:

$$N = 12 \cdot 11^b$$

for some nonnegative integer b.

6.3 Contradiction

If P had finite order, we would have

$$6 \cdot 5^a = 12 \cdot 11^b$$

But these two expressions cannot be equal. If $a \geq 1$, the left-hand side is divisible by 5, whereas the right-hand side is not. If $a = 0$, the left-hand side is 6, whereas the right-hand side is at least 12. Both possibilities are impossible. Therefore, our assumption that P has finite order is false, and

$$\text{ord}(P) = \infty$$

7 Conclusion

Since P has infinite order, the points

$$P, 2P, 3P, 4P, \ldots$$

are all distinct. Moreover, no nP is the negative of another mP, since that would give $(n+m)P = O$. Since the transformation can be inverted, distinct points give distinct ratios $x : y : z$, so distinct multiples of P yield distinct rational solutions of

$$7x^3 + y^3 = z^3$$

(The points nP and $-nP$ would give the solutions (x, y, z) and $(x, -z, -y)$, which are essentially the same, which is why it matters that no two of our points are negatives of each other.) Scaling up or down as necessary produces primitive integer solutions. Hence there are infinitely many distinct primitive integer solutions to

$$7x^3 + y^3 = z^3$$