Computer assisted number theory*

Gunter Harder
University of Bonn

In this lecture I want to speak about a very special diophantine equation, which is actually a special case of a wide class of diophantine equations, namely those which are related to elliptic curves.

The equation is

$$y^2 = x^3 - p^2x,$$

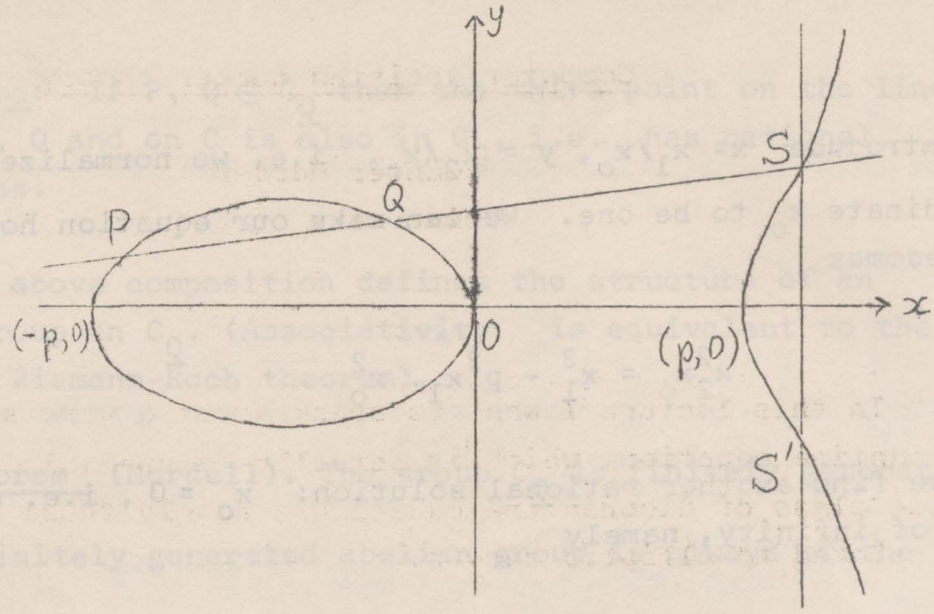
where p is a prime number. We can immediately see three (rational) solutions of the equation, namely

$$(x,y) = (0,0),\ (0,p),\ (0,-p)$$

Let me draw a picture of the graph of this equation.

---

* This is the text of a talk organised jointly by the Singapore Mathematical Society and the Department of Mathematics, University of Singapore, on 26 February 1976. The talk was aimed at a general audience, and the topic represents one of Professor Harder's interests although he did not do any research in this field. Those who wish to study the subject are referred to the articles in the bibliography. - Editor



This is the picture given by the real solutions of our equation, but we are mainly interested in rational solutions.

I want to start by explaining some general features of this equation which arise from the fact that this equation defines an elliptic curve.

We enlarge our affine plane with coordinates (x,y) to the projective plane by adding the line at infinity. As usual, we introduce homogeneous coordinates.

$$(x_o, x_1, y_2) \neq (0,0,0),$$

where two ordered triples (x_o, x_1, x_2), (x_o', x_1', x_2') define the same point in the projective plane if there exists a ξ such that

$$x_o = \xi x_o', x_1 = \xi x_1', x_2 = \xi x_2'$$

Our original affine plane corresponds to the part where $x_o \neq 0$:

we introduce $x = x_1/x_o$, $y = x_2/x_o$, i.e. we normalize the coordinate x_o to be one. We can make our equation homogeneous: it becomes

$$x_2^2 x_o = x_1^3 - p^2 x_1 . x_o^2$$

Now we find another rational solution: $x_o = 0$, i.e. on the line of infinity, namely

$$(0,0,1) = \theta .$$

This is the only point of our curve of infinity, therefore this point is an inflection point.

Now I look at the set of rational points of my curve i.e.

$$C_{\underline{Q}} = \left\{ (x,y) \in \underline{Q} \times \underline{Q} \mid y^2 = x^3 - p^2 x \right\} \cup \left\{ \theta \right\} .$$

I am going to construct a structure of an abelian group on $C_{\underline{Q}}$. The neutral element shall be θ, and I say: The sum of three points is θ if they lie on a line. With reference to the figure,

$$P + Q + S = \theta \text{ and } S' = P + Q .$$

If $P \in C_{\underline{Q}}$ then $2P$ is obtained by drawing a tangent at P.

Lemma: If $P, Q \in C_Q$ then the third point on the line joining P, Q and on C is also in C_Q, i.e. has rational coordinates.

The above composition defines the structure of an abelian group on C_Q. (Associativity is equivalent to the so-called Riemann-Roch theorem).

Theorem (Mordell). The group C_Q is finitely generated.

A finitely generated abelian group is always of the form

$$C_Q = (C_Q)_{\text{tors}} \underbrace{\oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r}$$

where $(C_Q)_{\text{tors}}$ is the subgroup of torsion elements, and $\mathbb{Z}$ is the group of integers. It is always easy to compute $(C_Q)_{\text{tors}}$. In this case it consists of exactly the four points constructed above. Unfortunately, so far there is no effective way of computing the number r (called the rank of C_Q), or to compute effectively solutions $P_1, P_2, \ldots, P_r$ which generate the torsion-free part. There is a general method which gives an estimate for the number r and a student of mine (R. Wachendorff) carried out the computations and found that

$$r \leq 2 \text{ if } p \equiv 1 \pmod 8,$$

$$r = 0 \text{ if } P \equiv 3 \pmod 8,$$

$$r \leq 1 \text{ if } p \equiv 5,7 \pmod 8.$$

There exists a deep conjecture of Tate-Shafarewič which, combined with some results of Cassels, implies that

$$\text{estimated rank} - r \equiv 0 \pmod 2.$$

Therefore, in the case when $P \equiv 5,7 \pmod 8$, there should exist a point of infinite order on $C_{\underline{Q}}$ and we asked a computer to find this solution for small values of the prime p.

Our equation is

$$y^2 = x^3 - p^2 x .$$

We write $y = \frac{a}{n}$, $x = \frac{b}{m}$ where a,n and b,m are coprime respectively. Then our equation becomes

$$a^2 m^3 = n^2 . b(b - mp)(b + mp) .$$

It follows that there exists a natural number M such that $m = M^2$, $n = M^3$, and then we have to solve in integers

$$a^2 = b(b - M^2 p)(b + M^2 p).$$

For some reasons which I shall not explain here, we try to find a solution that satisfies, in addition, $b < 0$ and $p \nmid b$. Then it is clear that

$$b = -X^2,$$

$$b - M^2 p = -Y^2,$$

$$b + M^2 p = Z^2,$$

where X,Y,Z are positive integers. This follows since the left hand side is a square and the factors on the right hand side are coprime.

We obtain the equations

$$X^2 + pM^2 = Y^2,$$

$$-X^2 + pM^2 = Z^2,$$

or from this,

$$2X^2 = (Y^2 - Z^2) = (Y - Z)(Y + Z).$$

An argument similar to that giving Pythagorean numbers yields

$$Y - Z = 4U^2,$$
$$Y + Z = 2V^2,$$
$$x = 2UV,$$

or

$$Y - Z = 2U^2,$$
$$Y + Z = 4V^2,$$
$$X = 2UV,$$

where U, V are positive integers. But then we find

$$X^2 + Z^2 = (2UV)^2 + (V^2 - 2U^2)^2 = pM^2,$$

or

$$X^2 + Z^2 = (2UV)^2 + (2V^2 - U^2)^2 = pM^2.$$

Hence

$$4U^4 + V^4 = pM^2 \quad \text{or} \quad U^4 + 4V^4 = pM^2.$$

Since $Z = V^2 - 2U^2$. or $Z = 2V^2 - U^2$ is positive, we find $U \leqslant V.\sqrt{2}$. Therefore we can write a programme. We vary V from 1 to 100 and U from 1 to $V.\sqrt{2}$. Then we check whether one of the expressions

$$4U^4 + V^4 \quad \text{or} \quad U^4 + 4V^4$$

is divisible by p and whether the result of this division is a square. If this is so we find the solution by going backwards.

I have some solutions for $p \equiv 5 \pmod 8$ up to 101 but so far we did not find a solution for p = 157.

p	a	b	M
5	6	-4	1
13	1938	-36	5
29	6930	-4900	13
37	32672766	-1764	145
53	$5.01018762 \times 10^{13}$	-115833156	5945
61	2055675594	-10227204	445
101	No solution found on WANG 2200		

Bibliography

[1] B. J. Birch, "Elliptic curves", a progress report, Proc. of the 1969 Summer Institute on Number Theory, Stony Brook.

[2] B. Mazur, "Courbes elliptiques et symboles modulaires", Sem. Bourbaki, 414, 1972.

[Professor Günter Harder is Professor of Mathematics at the Mathematical Institute of the Gesamthochschule of Wuppertal and the University of Bonn (SFB 40). His field of interest includes algebraic geometry, arithmetically defined groups, automorphic functions. He studied at the University of Hamburg, West Germany, and has been a visiting member of the Institute for Advanced Study in Princeton, U.S.A. and of the Institut des Hautes Études Scientifiques in Paris.— Editor.]

* * * * * * * * * *

'We all believe that mathematics is an art. The author of a book, the lecturer in a classroom tries to convey the structural beauty of mathematics to his readers, to his listeners. In this attempt he must always fail. Mathematics is logical to be sure; each conclusion is drawn from previously derived statements. Yet the whole of it, the real piece of art, is not linear; worse than that its perception should be instantaneous. We all have experienced on some rare occasions the feeling of elation in realizing that we have enabled our listeners to see at a moment's glance the whole architecture and all its ramifications. How can this be achieved? Clinging stubbornly to the logical sequence inhibits the visualization of the whole, and yet this logical structure must predominate or chaos would result.'

Emil Artin (1898 - 1962)