Rational points on algebraic curves
Lecture I, January 22, 1999

Ed Schaefer, Santa Clara University

Abstract:

We are interested in finding the set of points on an algebraic curve in a given number field. One of the key ingredients is the Mordell-Weil group of the Jacobian associated to the given curve and number field. We will spend much of this lecture series discussing the computation of the structure of such groups.

In this first talk, we will define Mordell-Weil groups and Jacobians. We will motivate interest in them by solving the following problem (first solved by Mordell in the 1960's): when is the product of two consecutive integers equal to the product of three consecutive integers? We will be able to solve the problem, modulo computation of the Mordell-Weil group. Hopefully this will convince the audience of the desireability of being able to compute such groups. In a later lecture, we will compute the structure of the Mordell-Weil group for this case, and thus complete the solution of this problem.

Motivating problems

1. When is the product of two consecutive integers equal to the product of three consecutive integers?

2. 1, 25, 49 are squares in arithmetic progression. What is the longest sequence of such?

3. The equation $y^2 = x^5 + 1$ has only trivial integer solutions: $(-1, 0)$, $(0, \pm 1)$. Are there other rational solutions? There are solutions in other number fields like $(1+i, 1-2i)$. What can we say about solutions in other number fields?

For proofs I do not give in today's lecture, see Silverman's *Arithmetic of Elliptic Curves.*

An (algebraic) curve C, over a (perfect) field K, is a smooth, irreducible, projective curve defined by polynomial equations with coefficients in K. We will say that C is defined over K and denote this condition by C/K. The points of C are assumed to have coordinates in $\overline{K}$.

Problem: For a given curve C/K, where K is a number field, we want to find the set of points on C with coordinates in K; denote this set by $C(K)$.

This is a vast subject and I will not be able to cover it in 10 hours. Instead, I will treat parts of it, in particular algorithms for describing the Mordell-Weil group associated to a curve and number field and how it helps to find the set of points on the curve in that number field.

Algebraic curves are classified by their genus.
1. Conic sections are the genus 0 curves.
2. Genus 1 curves (with a specified point) are called elliptic curves.
3. Higher genus curves.

The problem has been solved for genus 0 curves. Much progress has been made this century on genus 1 curves. We will focus on genus 1 or more.

Today I want to start with a fun example that will motivate the interest in Mordell-Weil groups. It is probably better not to jump into Galois cohomology today or no one will come next time.

Problem to motivate interest in Mordell-Weil groups

When is the product of two consecutive integers equal to the product of three consecutive integers?

$$\begin{aligned} 6 &= 1\cdot 2\cdot 3 & &= 2\cdot 3 \\ & & &= -2\cdot -3 \\ 0 &= 0\cdot 1\cdot 2 & &= 0\cdot 1 \\ &= -1\cdot 0\cdot 1 & &= -1\cdot 0 \\ &= -2\cdot -1\cdot 0. & & \end{aligned}$$

We have two representations of 6, and 6 representations of 0. Are there others? Are there infinitely many others or only finitely many others? If there are finitely many others, how will we ever know that we have them all? We want integer solutions of $y(y+1) = (x-1)x(x+1)$ or $y^2 + y = x^3 - x$.

The solution set of such an equation is an elliptic curve. An elliptic curve E over the field K is any curve isomorphic over K, to a cubic curve (defined over K) in $\mathbf{P}^2$ along with a specified point of E, with coordinates in K. We will denote this condition by E/K.

The curves C_1/K and C_2/K are isomorphic over K, if there are maps $C_1 \to C_2$ and $C_2 \to C_1$ given locally on points by rational functions with coefficients in K, that are inverses.

We use the affine equation $y^2 + y = x^3 - x$ to define a projective curve, E, in

$$\mathbf{P}^2(\overline{\mathbf{Q}}) = \{[a:b:c] \mid a,b,c \in \overline{\mathbf{Q}},\ (a,b,c) \neq (0,0,0),\ [a:b:c] = [d:e:f]$$

$$\text{iff there is } \lambda \in \overline{\mathbf{Q}} \text{ such that } (a,b,c) = (\lambda d, \lambda e, \lambda f)\}$$

For K with $\mathbf{Q} \subseteq K$, a point is in $\mathbf{P}^2(K)$ if there is some representation $[a : b : c]$ with $a,b,c \in K$. Let $x = X/Z$, $y = Y/Z$. Then $[X : Y : Z]$ are coordinates for $\mathbf{P}^2$ and we get a homogeneous equation $Y^2Z + YZ^2 = X^3 - XZ^2$, which is well-defined on $\mathbf{P}^2$. If $Z = 1$, we get the earlier, affine equation. If $Z = 0$ we get $[0 : 1 : 0]$, the only point at infinity of the affine model. It is at the top and bottom of every vertical line in the affine plane.

The marvelous thing about an EC is that there is a natural way of putting a group structure on the points of the curve. We always let the specified point be the identity and denote it $\mathbf{O}$. For our curve, let $[0 : 1 : 0] = \mathbf{O}$.

Inverses and addition from rule: 3 points lying on a line, sum to $\mathbf{O}$. We will see where that comes from later on when we talk about divisor classes. Note, it follows from Bezout's theorem that every line meets a cubic curve in $\mathbf{P}^2(\overline{K})$ exactly three times (counting multiplicities). Let us see how this enables us to add points.

Let us say you want to add P and Q as in figure 1. Draw a line connecting them. If $P = Q$, then that is the tangent line. The line will meet the curve in a third point R (possibly P and/or Q). Those three points lie on a line so they sum to $\mathbf{O}$. Thus $P + Q = -R$. Now draw a line connecting R and 0. It meets the curve at R, $\mathbf{O}$ and one other point. Since the latter three must sum to $\mathbf{O}$, that one other point must be $-R = P + Q$.

The above method works for any elliptic curve (EC) given by a Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Note that any cubic curve C/K, with $C(K)$ not empty, is isomorphic over K to a curve described by a Weierstrass equation (over K). One can find an isomorphism that will match the **O**-points also. For an elliptic curve described by a Weierstrass equation, we traditionally take the point at infinity to be the **O**-point. Interestingly, any isomorphism of elliptic curves matching **O**-points induces an isomorphism of groups.

Let us apply this to our curve. See figure 2. We know the point $P = (0, 0)$ is on it. Its negative is $-P = (0, -1)$. Let us find $2P$. The tangent line at $2P$ is $y = -x$. That meets $y^2 + y = x^3 - x$ at $x^2 - x = x^3 - x$ or $x^3 - x^2 = 0 = (x - 0)^2(x - 1)^1$. This equation says that the line meets the curve twice where $x = 0$ and once where $x = 1$. That is the point $(1, -1)$ and it is $-2P$. Thus $2P = (1, 0)$. The line $y = 0$ connects P and $2P$. The third point of intersection is $-3P = (-1, 0)$. Thus $3P = (-1, -1)$. The line connecting P and $3P$ is $y = x$. This intersects $y^2 + y = x^3 - x$ where $x^2 + x = x^3 - x$ or $x^3 - x^2 - 2x = 0 = (x + 1)x(x - 2)$. The third point of intersection then is $(2, 2) = -4P$. Thus $4P = (2, -3)$.

If we put the coordinates of $\pm P, \pm 2P, \pm 3P$ into the equation we get a 0 on both sides and there were 6 representations of 0 as a product of two consecutive integers and a product of three consecutive integers. If we put the coordinates of $\pm 4P$ into the equation we get a 6 on both sides and there were 2 representations of 6 as a product of two and a product of three consecutive integers. We have exhausted the known solutions, but we can keep adding points.

By the same techniques we find $5P = (1/4, -5/8)$. This does not have integer coordinates so it does not give us a new solution to our problem. However $6P = (6, 14)$. This says $14 \cdot 15 = 5 \cdot 6 \cdot 7 = 210$. Let us keep going.

$$7P = (-5/9, 8/27),\ 8P = (21/25, -69/125),\ 9P = (-20/49, -435/343),$$

$$10P = (161/16, -2065/64), 11P = (116/23^2, -3612/23^3), 12P = (1357/29^2, 28888/29^3).$$

It seems that the denominators are getting worse. On the other hand, maybe there are other points with integer coordinates that are not multiples of P. We have hit a brick wall.

Let us go back to the theory of elliptic curves. Let $E/\mathbf{Q}$ be arbitrary. Then $E(\mathbf{Q})$ is a subgroup of $E = E(\overline{\mathbf{Q}})$.

Theorem (Mordell-Weil): $E(\mathbf{Q})$ is a finitely generated abelian group.

In our case, $E(\mathbf{Q}) \cong \mathbf{Z}$, and is generated by $P = (0, 0)$. This is motivation for this series of talks. How do you prove such a thing? Now let us assume it and solve the problem at hand. In a later lecture, we will prove this statement.

Indeed we have all the integer points. It suffices to consider the positive multiples of P. Let $R = (x, y) \in E(\mathbf{Q})$. Given the equation $y^2 + y = x^3 - x$, it is clear that $x \in \mathbf{Z}$ iff $y \in \mathbf{Z}$. When $x, y \in \mathbf{Z}$, we will call R an integer point.

Claim: If $R \in E(\mathbf{Q})$ is not an integer point, then $2R$ is not either.

Let $R = (x, y)$ and $2R = (x', y')$. We can do some algebra and see that $x' = (x^4 + 2x^2 - 2x + 1)/(4x^3 - 4x + 1)$. If $x \notin \mathbf{Z}$ then there is a prime p with $v_p(x) = -n < 0$. Thus $v_p(x^4 + 2x^2 - 2x + 1) = -4n$, $v_p(4x^3 - 4x + 1) \geq -3n$, so $v_p(x') \leq -n < 0$ and $x' \notin \mathbf{Z}$.

Every positive integer is of the form $2^n \cdot 1$, $2^n \cdot 3$, or $2^n \cdot m$ where m is odd, $m > 3$. If m is odd, then mP is on the left-hand component. This could only fail if a line met the left-hand component an odd number of times, which is impossible. We found all integer points on left-hand component, so if $m > 3$ (odd) then mP is not an integer point, so $2^n \cdot mP$ is not either. $8P$ is not integer point so $2^n \cdot 1P$ is not either for $n > 2$. $12P$ is not integer point so $2^n \cdot 3P$ is not either for $n > 1$. We have found them all. The answer to the original question is 0,6,210. This was first proven by Mordell in the early 1960's.

In case you are curious. It was shown in the early 1970's that the only integers that are simultaneously the product of 3 and of 4 consecutive integers are 0, 4!, $2 \cdot 3 \cdot 4 \cdot 5 = 4 \cdot 5 \cdot 6$ and $19 \cdot 20 \cdot 21 \cdot 22 = 55 \cdot 56 \cdot 57$.

More on the Mordell-Weil theorem for elliptic curves

Let $E/\mathbf{Q}$. Then $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\text{tors}}$. $E(\mathbf{Q})_{\text{tors}}$ is finite and there are fast and easy algorithms to determine it. There is no known effective algorithm guaranteed to find r in a given case (when the coefficients are not extraordinarily large, it seems we always manage to find it). The number r is called the Mordell-Weil rank. We will spend much of our time trying to find r.

For $E : y^2 + y = x^3 - x$, let us compute $E(\mathbf{Q})_{\text{tors}}$.

Theorem (Nagell-Lutz): Let $E/\mathbf{Q}$ with equation $y^2 = x^3 + Ax + B$, with $A, B \in \mathbf{Z}$. If (x, y) is a torsion point, then $x, y \in \mathbf{Z}$, and either $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.

We have $y^2 + y = x^3 - x \cong v^2 = u^3 - 16u + 16$ by $v = 8y + 4, u = 4x$. Note $4A^3 + 27B^2 = -37 \cdot 2^8$. So we must check $v = \pm 2^j$ where $0 \leq j \leq 4$. v-coordinates either do not give u-coordinates on the curve or give points of infinite order (since their multiples are not integer points). So $E(\mathbf{Q})_{\text{tors}} = 0$. Therefore we just want to show that $r = 1$ and $(0, 0)$ generates $E(\mathbf{Q})$. We will do that in a later lecture.

Jacobians

To the curve $y^2 + y = x^3 - x$ we have associated a group. To every curve we can associate a group, which is also a projective variety, called its Jacobian. (A variety is a geometric object described by algebraic equations.) We are interested in the group (more than the variety structure). The dimension of the Jacobian equals the genus of the curve. So only for genus 1 curves is it possible to think of elements of the Jacobian as being the points on the curve itself. The group is isomorphic to the degree 0 divisor classes of the curve, to be described soon.

FIGURE 1. $P + Q$

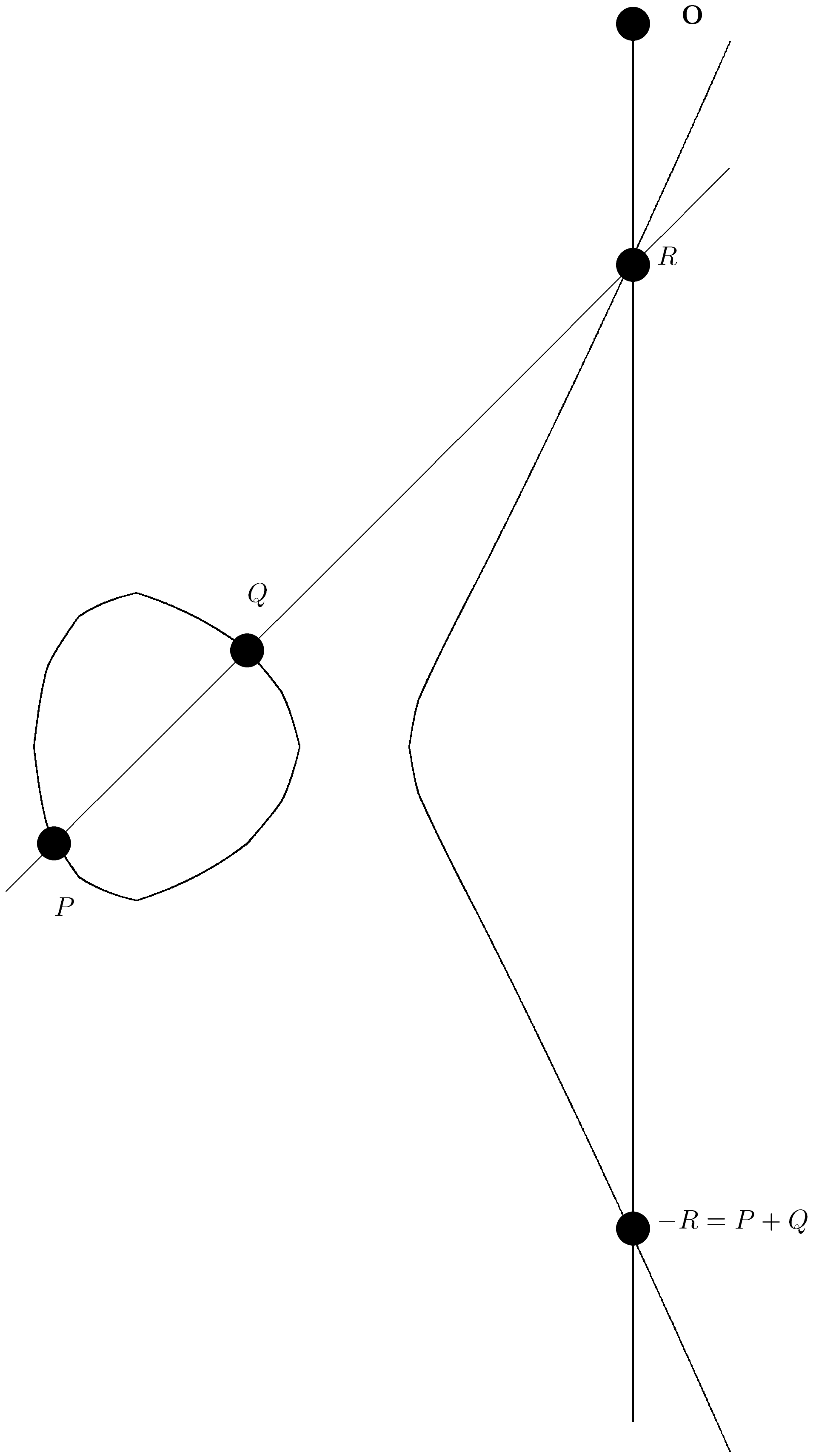

FIGURE 2. $y^2 + y = x^3 - x$