4. Del

Weak Mordell and the rank of elliptic curves

Version 1.0— *Sunday, September 28, 2014 12:31:03 PM*
This is a preliminary version and subjected to change.

The Mordell theorem tells us that the abelian group $E(\mathbb{Q})$ of rational points of an elliptic curve E over $\mathbb{Q}$ is finitely generated. It can therefore be decompsoed as $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ where T is the torsion part of $E(\mathbb{Q})$. In one of the previous lectures we studied the torsion part T. The the theorem of Lutz and Nagell allows to compute T for any specific elliptic curve, and Mazur's teorem gives the astonoshingly short list of the finite groups that occur as torsion groups, and one may say that the torsion part of $E(\mathbb{Q})$ is very well under control. On the other hand the rank r is an evasive invariant and almost all natural questions about it remains unanswered.

For example: Is it is bounded? It is generally believed that it is not, and that one can find elliptic curves over $\mathbb{Q}$ with arbitrary large rank.

However, the world record to this day is just 28; to be precise Elkies found a curve that has rank at least 28 by exhibiting 28 rational points independent points in $E(\mathbb{Q})$, but he did not show there are no more (so the world record could in principle be higher). Needless to say that the equation of the curve involves some awesome numbers not made for human eyes:

$$y^2 + xy + y = x^3 - x^2 -$$
$$20067762415575526585033208209338542750930230312178956502x +$$
$$3448161179503055646703298569039072037485594435931918036 1$$
$$26600829629193944873224342 9$$

The following curve has rank 19, as shown by xxx; and that is the highest rank that is known:

$$y^2 + xy + y = x^3 + x^2 +$$
$$31368015812338065133318565292206590792820353345x +$$
$$30203880269856608733564318842954349862452204168387$$
$$4493555186062568159847$$

Our aim in this lecture is infinitely more modest. We just want to do just a few examples, to get the "feeling" of the rank problem. In some sense it is not very satisfactory to give a course on the arithmetic of elliptic curves without showing the computation the rank of any elliptic curve. We are following the expostion in [1] rather closely.

4.1 The weak Mordell theorem

The proof of Mordell's theorem (which we shall not give) is divided into two parts. The first is to establish what often is called the Weak Mordell theorem and consists of proving that the group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. This is certainly nessecary for the full Mordell's theorem to be true, but far from sufficient. Any divisible group A has $A = 2A$, but need not be finitely generated as the example $A = \mathbb{Q}$ shows. The second part of the proof copes with these problems, and relies heavily on what is called height functions.

Back to the weak Mordell's theorem and the rank of E. Assuming Mordell's thoerm and writing $E(\mathbb{Q}) = \mathbb{Z}^r \oplus T$, one sees that $E(\mathbb{Q})/2\mathbb{E}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}^r \oplus T/2/$. One may further decompose $T = \bigoplus_p T_p$ where T_p is the p-primary torsion part of T (*i.e.,* . those points killed by a power of the prime p).

If p is odd, $2T_p = T_p$ and T_p does not contribute to $T/2T$. In case $p = 2$, the group T_2 is a direct sum of cyclic groups S of the form $S = \mathbb{Z}/2^a\mathbb{Z}$. In each there is one non-trivial two-torsion element, and $S/2S \simeq \mathbb{Z}/2\mathbb{Z}$. Hence $T/2T \simeq (\mathbb{Z}/2\mathbb{Z})^s$ where s is such that $E_2(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^s$. We have shown the following lemma (assuming Mordell's theorem):

Lemma 4.1

$$E(\mathbb{Q})/2E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}^{r+s}.$$

There is an analogous statement for any integer m, but to stay with our principle of simplicity, we only treat the case $m = 2$.

The proof of the Weak Mordell's theorem has two parts as well. In the first one treats the particular class of elliptic curves over $\mathbb{Q}$ having three rational two-torison points. That is, those curves whose Weierstrass equation is on the form

$$y^2 = (x - a_1)(x - a_2)(x - a_3) \qquad (\text{✡})$$

where the a_i are integers. We let $g(x) = (x - a_1)(x - a_2)(x - a_3)$.

For these curves one constructs an inclusion $\psi\colon E(\mathbb{Q})/2E(\mathbb{Q}) \to 3\mathbb{Q}^*/\mathbb{Q}^{*2}$ and there is a fairly good description of the image. The group $\mathbb{Q}^*/\mathbb{Q}^{*2}$ of rational numbers modulo the squares is not finite, but one has a sufficiently firm grasp on the image of ψ to tell that is finite. In a few simple cases, one can even give a complete description of the image, and thus compute the rank of E.

The second part of the weak Mordell's theorem is basically a replica (with some tribulations) of the above procedure, not done over $\mathbb{Q}$, but over the root field of $g(x)$.

There are two ways of presenting this material. One using group cohomology and the other relying on a few trivial computations. The cohomology way is scientifically the best without doubt, but unnavigable when presenting this material in a few hours for students lacking any cohomological background.

4.1.1 The group $\mathbb{Q}^*/\mathbb{Q}^{*2}$

Inside the multiplicative group $\mathbb{Q}^*$ one has the (multiplicative) subgroup of squares (if a and b are squares clearly ab is). The use of the quotient $\mathbb{Q}^*/\mathbb{Q}^{*2}$ of rational numbers mod squares goes at least back to Kummer and appears in a part of algebraic number theory that is called "Kummer theory".

Any rational number n may be written as a product

$$n = \operatorname{sign}(n) \prod_p p^{\epsilon_p(n)}$$

where $\operatorname{sign}(n) \in \mu_2$ denotes the sign of n, and where the product extends over all primes p. The exponents ϵ_p are all *integers*, and of course only finitely many of them are different from zero.

How do we detect that n is square? Well, it must be positive, *i.e.*, $\operatorname{sign}(n) = 1$ and *all* the exponents $\epsilon_p n$ must be *even*, and these conditions are as well sufficient. This means that the map

$$\mathbb{Q}^* \to \mu_2 \oplus \bigoplus_p \mathbb{Z}/2\mathbb{Z}$$

sending n to $\operatorname{sign}(n)$ in μ_2 and to the mod 2 class of $\epsilon_p(n)$ in the $\mathbb{Z}/2\mathbb{Z}$-summand corresponding to the prime p induces an isomorphism

$$\mathbb{Q}^*/\mathbb{Q}^{*2} \simeq \mu_2 \oplus \bigoplus_p \mathbb{Z}/2\mathbb{Z}$$

A convenient notation, conform with common usage, is to let $< p >$ stand for the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ generated by the prime p. This is just the direct factor isomorphic $\mathbb{Z}/2\mathbb{Z}$ corresponding to p.

4.1.2 A criterion for two divisibility

We proceed under the standing assumptun that E is an elliptic curve over $\mathbb{Q}$ with all two-torsion points being rational.

Pick a point (x_0, y_0) in $E(\mathbb{Q})$, the aim in this paragtaph is to give a criterion for when P is divisible by two. that is, when there exists a rational point (x_1, y_1) with $2(x_1, y_1) = (x_0, y_0)$. In geometric terms, this happens when tehre is a line through (x_0, y_0) with rational slope that touches E in another rational point. The equation of the line is $y = mx + y_0$, and finding the intersection bestween the line and the cubic amounts to solving the equation

$$(x - a_1)(x - a_2)(x - a_3) - (mx + y_0)^2 = 0$$

hence if x_0, x_{21} and x_2 are the x-coordinates of the three intersection points, one has

$$(x - a_1)(x - a_2)(x - a_3) - (mx + y_0)^2 = (x - x_0)(x - x_1)(x - x_2) \qquad (✣)$$

Assume the line is tangent touching in artional point. Then $x_1 = x_2$ is rational, and putting $x = a_i$ in ✣ gives

$$(x_0 - a_i) = (mx_0 + y_0)^2 (x_1 - a_i)^{-2}$$

Hence if (x_0, y_{o0}) is two-divisible, each $(x_0 - a_i)$ is a square in $\mathbb{Q}$. It turns aout that this also is a sufgicient condition:

Proposition 4.1 *Assume that E is an elliptic curve over $\mathbb{Q}$ having three rational two-torison points and with Weierstrass equation of the form (✡). Then a point $(x_0, y_0) \in E(\mathbb{Q})$ is two-divisible (in $E(\mathbb{Q})$) if and only if each $(x_0 - \alpha_i)$ is a square in $\mathbb{Q}$.*

PROOF: We just need to argue for one of the implications. So assume that the $(x_0 - a_i)$ all are squares in $\mathbb{Q}$. Changing the x coordinate we may assume that $x_0 = 0$. the assumption then becomes that each $-a_i$ is a square in $\mathbb{Q}$. So for $i = 1, 2, 3$, let α_i be a rational number with $\alpha_i^2 = -a_i$.

We want to determine a line through (x_0, y_0) tangent to E. The equation of a line through (x_0, y_0) is $y = mx + y_0$. It will be convienint to write

$$(x - a_1)(x - a_2)(x - a_3) = x^3 + s^1 x^2 + s^2 x + s_3$$

where $(-1)^i s_i$ is the i-th elementary symmetric function in the a_i's.

With a little elementary algebra, one brings equation ✣ on the form

$$x^2 + (s_1 - m^2)x + (s_2 - 2my_0) = 0,$$

and we want to determine a rational m such that this equation has a double root. The condition for this is that the discriminant vanishes, that is

$$(s_1 - m^2)^2 = 4(s_2 - 2my_0).$$

This is an equation of degree four, which is troublesom to solve, unless you happen to know the solution. And we do! (Just look it up in textbook). Any combination of the α_i's of the form $m = \sum_i \epsilon_i \alpha_i$ with the ϵ_i's being ± 1 with $\epsilon_1\epsilon_2\epsilon_3 = -1$ will do, for example $\alpha_1 + \alpha_2 - \alpha_3$.

Indeed:

$$\alpha_1^2 + \alpha 2^2 + \alpha_3^2 - (\alpha_1 + \alpha_2 - \alpha_3)^2 = -2(\alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3)$$

Hence the left side is

$$4(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 - -2(\alpha_1 + \alpha_2 - \alpha_3)\alpha_1\alpha_2\alpha_3)$$

but this is just the right side! ❑

4.1.3 The definition of ψ

We now proceed to the definition of the homomorphism ψ. For each of the a_i's there is a group homomorphism ψ_{a_i}. The salient point is that the map $\psi = \psi_{a_1} \times \psi_{a_2} \times \psi_{a_3}$ defines an *injection*

$$\psi \colon E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

Indeed, using only two of them will do. Here comes the definition of the ψ_{a_i}'s. It is convenient to let a denote one of a_i's and b and c the two others (this is often expressed in the slightly more fancy way $\{a, b, c\} = \{a_1, a_2, a_3\}$). We start by giving a map $\tilde{\psi}_a \colon E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ that vanishes on $2E(\mathbb{Q})$ and hence descends to a map ψ_a on $E(\mathbb{Q})/2E(\mathbb{Q})$.

$$\tilde{\psi}_a(P) = \begin{cases} x - a & \text{if } P = (x, y) \text{ and } \ x \neq a \\ (a - b)(a - c) & \text{if } x = a, \text{ that is } P = (a, 0) \\ 1 & \text{if } P = O \end{cases}$$

where the expressions on the right side are understood as classes in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. The basic property of the ψ_a's is the following:

Proposition 4.2 *The maps $\tilde{\psi}_a$ are group homomorphisms that vanish on $2E(\mathbb{Q})$.*

The second statement shows that $\tilde{\psi}_a$ descends to $E(\mathbb{Q})/2\mathbb{E}(Q)$ and gives us a group homomorphism ψ_a as announced above.

PROOF: Firstly, the criterion for two-divisibility 4.1 immediately gives the vanishing in the second statement. We do the first statement for $\tilde{\psi}_{a_1}$. One has $z = z^{-1}$ in the group $\mathbb{Q}^*/\mathbb{Q}^{*2}$ since all squares are equal to one. Since P and $-P$ have the same x-coordinate (if $P = O$ they are even equal), one has $\tilde{\psi}(-P) = \tilde{\psi}(P) = \tilde{\psi}(P)^{-1}$. From this follows that $\tilde{\psi}(P - P) = \tilde{\psi}(P)\tilde{\psi}(-P)$ both being equal to 1.

We shall therefore be through once we have establisted that $(x_1-a_1)(x_2-a_1)(x_3-a_1)$ is a square in $\mathbb{Q}$ whenever the x_i's are the x-coordinates of the intersection points of E with a non-vertical line. Let $y = mx + b$ be the equation of the line. The basic relation is

$$(x - a_1)(x - a_2)(x - a_3) - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3) \qquad (✣)$$

which determines the x-coordinates of the intersection points of the line and the cubic. There are three cases to establish:

□ None of the x_i's equals a_1: Put $x = a_1$ in the basic relation (✣) above to get

$$(x_1 - a_1)(x_2 - a_1)(x_3 - a_1) = (ma_1 + b)^2 \in \mathbb{Q}^{*2}$$

□ One of the x_i is equal to a_1, say x_1. The equation of the line then becomes $m(x-a_1)$, and the relation above reduces to

$$(x - a_2)(x - a_3) - m(x - a_1) = (x - x_2)(x - x_3).$$

Upon setting $x = a_1$ this leads to

$$(a_1 - a_2)(a_1 - a_3) = (x_2 - a_1)(x_3 - a_1),$$

and therefore

$$\big((a_1 - a_2)(a_1 - a_3)\big)(x_2 - a_1)(x_3 - a_1) \in \mathbb{Q}^{*2}$$

□ A possible third case would occur when two of the x_i's are equal to a_1, but then the line is vertical. ❑

The main tool in this paragraph is the map $\psi\colon E(Q) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$ having components ψ_1 and ψ_2. By proposition xxx is $P = (x, y)$ is two-divisible $x - a_i$ is a sqaure, and ψ takes the value one on $2E(\mathbb{Q})$. Therefore it factors thorugh the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ and induces a map $\tilde{\psi}\colon E(\mathbb{Q})/E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$

Corollary 4.1 *The map $\tilde{\psi}$ is an injective group homomorphism.*

PROOF: The only thing that is left to prove, is that $\tilde{\psi}$ is injective. If $x - a_1$ and $x - a_2$ both are squares, then $x - a_3$ is a squarere as well, the product of the three being y^2. So if $\tilde{\psi}(P) = 1$ and $P \neq (a_1, 0), (a_2, 0)$ it follows from proposition xxx that P is two-divisible. If say $\tilde{y}(a_1, 0) = 1$, then $a_1 - a_2$ is a square, and as $(a_1 - a_2)(a_1 - a_3)$ is a square as well,$(a_1 - a_3)$ will be a square, and by xxx $(a_1, 0)$ is two divisible. ❑

Description of the image

The next issue is the image of $\tilde{\psi}$. If P is a point of E, the components of $\tilde{\psi}(P)$ are $\text{sign}(x)$ and the residue classes of $v_p(x-a_i)$ modulo 2 for $1=1,2$ and p a prime. The point is as we shall see, that a the components of $\tilde{\psi}(P)$ only can be non-zero at primes dividing the discriminant Δ of E. This shows the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$ and for very small discriminants makes it possible to compute the rank of E. Recall that the discriminant is given as

$$\Delta = \prod_{i<j}(a_i - a_j)^2.$$

Recall further that

$$\tilde{\psi}\colon E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 = \mu_2 \oplus \mu_2 \oplus \bigoplus_p \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad (\text{✧})$$

Let $P=(x,y)$ be a rational point of the curve E, which we recall has the Weierstrass equation

$$y^2 = (x-a_1)(x-a_2)(x-a_3) \qquad (\text{✣})$$

where the a_i are integers, and as usual, we let $g(x) = (x-a_1)(x-a_2)(x-a_3)$.

Lemma 4.2 *If $v_p(x) < 0$, then $v_p(x-a_i) \equiv 0 \mod 2$*

PROOF: Since the a_i's by assumption are integers it holds that $v_p(a_i) \geq$. Hence $v_p(x) < v_p(a_i)$ and

$$v_p(x-a_i) = \min\{v_p(x), v_p(a_i)\} = v_p(x).$$

It follows from the Weierstrass equation (✡) that $2v_p(y) = \sum_i v_p(x_{a_i}) = 3v_p(x)$. Hence $n = v_p(y)/3$ is an integer and $v_p(x-a_i) = v_p(x) = 2n$. ❑

Lemma 4.3 *If $v_p(x) \geq 0$ and $v_p(x-a_1) \equiv 1 \mod 2$, then $p|\Delta$.*

PROOF: Since $v_p(a_i) \geq 0$ it holds that $v_p(x-a_i) \geq \min\{v_p(x), v_p(a_i)\} \geq 0$. In particular it follows that $v_p(x-a_1) > 0$. One has

$$\sum_i v_p(x-a_i) = 2v_p(y),$$

so if $v_p(x-a_j) = 0$ for $j=2,3$ it follows that $v_p(x-a_1)$ is even, which is not the case. Hence $v_p(x-a_j) > 0$ for at least one $j \neq 1$. But then $v_p(a_1-a_j) = v_p(x-a_j-(x-a_1)) > 0$, and $p|(a_1-a_j)$, hence p divides the discriminant. ❑

Proposition 4.3 *Let $\tilde{\psi}(P)$ be a point in the image of $\tilde{\psi}$. Then if p is a prime not dividing the discriminant of E, then the corresponding components of $\tilde{\psi}(P)$ in the decomposition xxx vanish.*

PROOF: If $x \neq a_1$ and $x \neq a_2$ this is just the statements in the two lemmas above. If *e.g.*, $x = a_1$, the image is the pair $(a_1 - a_2, (a_1 - a_2)(a_1 - a_3))$ mod squares. Since $v_p(a_1 - a_2) \geq 0$, the congruence $v_p(a_1 - a_2) \equiv 1 \mod 2$ implies that $v_p(a_1 - a_2) > 0$, and p divides the discriminant. In a similar fashion, if $v_p((a_1 - a_2)(a_1 - a_3)) \equiv 1 \mod 2$, at least one the factors is divisible by p. ❑

Examples

Before we start on the examples, we make one general observation. The sign-component of $\psi(P)$ is confined to the subgroup of μ_2^3 isomorphic to μ_2 consisting of the two elements $(+,-,-)$ and $(+,+,+)$. This is generally true when the three roots are ordered so that

$$a_1 < a_2 < a_3,$$

because then

$$x - a_1 > x - a_2 > x - a_3$$

for all x. Indeed, since the product of the three is a square, necessarily $x - a_1 > 0$, and the sign-distribution for two smaller is either $++$ or $--$.

EXAMPLE 4.1. — $y^2 = x(x-1)(x+1)$. We take closer look at the curve E whose equation is $y^2 = x(x-1)(x+1)$, and we shall see that $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, that is, the only rational points E has are the obvious ones: O, $(0,0)$ and $(\pm 1, 0)$.

The discriminant of E equals 2^4, so 2 is the only bad prime, and the image of ψ is confined to the subgroup $\mu_2^3 \oplus \langle 2 \rangle^3$ of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ where only the sign-components and the two-components are non-trivial.

Counting points in $E(\mathbb{F}_3)$ one finds 4, since $g(x)$ vanishes for all values of $x \in \mathbb{F}_3$. Since E has good reduction at 3, there is an inclusion $E_{tors}(\mathbb{Q}) \subseteq E(\mathbb{F}_3)$, and we conclude that $E_{tors}(\mathbb{Q}) = E_2(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$.

We proceed by computing the images of the three two-torsion points under the map $\psi = \psi_{a_1} \times \psi_{a_2} \times \psi_{a_3}$. The result is shown in the table below where the i-th line represents $\psi((a_i, 0))$; the first column shows the values as in the definition before we reduce mod $\mathbb{Q}^{*2}$, the next three the $\pm$-components and last three the 2-components. The computation is trivial using the definition of ψ_a, which we for convenience recall:

$$\psi_a(P) = \begin{cases} x - a & \text{if } P = (x,y) \text{ and } x \neq a \\ (a-b)(a-c) & \text{if } x = a, \text{ that is } P = (a,0) \\ 1 & \text{if } P = O \end{cases}$$

where $\{a,b,c\} = \{a_1, a_2, a_3\}$.

$a_1 = -1$	$(2,-1,-2)$	$+$	$-$	$-$	1	0	1
$a_2 = 0$	$(1,-1,-1)$	$+$	$-$	$-$	0	0	0
$a_3 = 1$	$(2,1,2)$	$+$	$+$	$+$	1	0	1

The next thing to see is that the image $\psi(P)$ of any rational point of E appears among those vectors listed in the table, thus showing that $\operatorname{Im}\psi \simeq (\mathbb{Z}/2\mathbb{Z})^3$, and consequently that the rank is zero.

To that end pick a rational point $P = (x, y)$ in $E(\mathbb{Q})$ that is not two-torsion. If $v_2(x) < 0$, it follows from lemma 4.2 that $v_2(x - a_i) \equiv 0 \mod 2$, and the point has only trivial 2-components. Assume that $v_2(x) > 0$. Then $v_2(x \pm 1) = 0$, and it follows that $2v_2(y) = \sum_i v_2(x - a_i) = v_2(x)$, so $v_2(x) \equiv 0 \mod 2$. The 2-components of $\psi(P)$ are therefore zero. In both these cases $\psi(P)$ is either 0 or equal to $\psi((0,0))$.

The last case is $v_2(x) = 0$. Then $2v_2(y) = v_2(x+1) + v_2(x-1)$, and $v_2(x+1)$ and $v_2(x-1)$ are of the same parity. After the remark about the sign-distributions, which must be $+++$ or $+--$, $\psi((x,0))$ is either trivial or among the listed vectors. ❄

EXAMPLE 4.2. — $y^2 = x(x+2)(x-2)$. This time we examination the curve E with equation $y^2 = x(x+2)(x-2)$, which is slightly more delicate than the previous one. The discriminant in this case is 2^6, so the only place where E has bad reduction is at the prime 2. As in the previous example we construct the table showing the images of the two-torsion points under ψ. Subsequently we shall use the map $\psi_{a_1} \times \psi_{a_2}$, and the projection onto the corresponding factor $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is coulored dark green in the table.

$a_1 = -2$	$(8,-2,-4)$	$+$	$-$	$-$	1	1	0
$a_2 = 0$	$(2,-4,-2)$	$+$	$-$	$-$	1	0	1
$a_3 = 2$	$(4,2,8)$	$+$	$+$	$+$	0	1	1

The trick is to add a combination of two-torsion points to the point P to obtain a new rational point P' whose two-components corresponding to ψ_{a_1} and ψ_{a_2} vanish (the "darker green" ones). To complete our task, we must see that this vanishing of two-components implies that $\psi(P')$ itself vanish, *i.e.,* that the sign distribution is $+++$. A counter example would be a point such that there are rationals a, b and c with

$$x + 2 = a^2 \quad x = -b^2 \quad x - 2 = -c^2.$$

□ Assume $v_2(x) > 1$. Then $2v_2(a) = v_2(x+2) = \min\{v_2(x), 1\} = 1$ which is impossibel, so $v_2(x) \leq 1$. But $v_2(x)$ being twice, $v_2(a)$ one has $v_2(x) \leq 0$.

□ Assume that $v_2(x) = 0$. Then $2v_2(c) = \min\{v_2(x), 1\} = 0$, and of course $v_2(b) = 0$ as well. Hence we have the relation $2 = c^2 - b^2$ with $v_2(c) = v_2(b) = 0$. Reducing mod 8 we arrive at contradiction, since the only invertible square in $\mathbb{Z}/8\mathbb{Z}$ is 1(the non-zero squares are $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$ and $(\pm 3)^2 = 1$)

□ Hence $v_2(x) < 0$, and it follows that $v_2(a) = v_2(b) = v_2(c) = \nu < 0$. Clearing powers of two from the denominators, we arrive at the relations

$$2^{2\nu}x + 2^{2\nu+1} = \alpha^2 \quad 2^{2\nu}x = -\beta^2 \quad 2^{2\nu}x - 2^{2\nu+1} = \gamma^2,$$

where now the numerators and denominators of α, β and γ are free from powers of two. Hence we get the equation $\alpha^2 \equiv -\beta^2 \mod 8$ with $v_2(\alpha) = v_2(\beta) = 0$. Impossible.

A final remark about this example. Eleminating x from the three equations above and introducing a new variable d to make them homogenous, we arrive at the two quadratic equations

$$a^2 + b^2 - 2d^2 = 0 \qquad c^2 - b^2 - 2d^2 = 0.$$

This is the intersection of two quadrics in $\mathbb{P}^3$ (with coordinates a, b, c and d). Such intersections are genus one curves, if they are smooth! And what we just have done, is to see that this curve does not have any rational point. (Hence it is not elliptic). One may show that it is isomorphich to our original curve over $\mathbb{C}$, but not over $\mathbb{Q}$ of course. Over $\mathbb{Q}$ it is another manifestation of E ; such "shadow curves" are often called *"torsors"*. This phenomenon is notorious when one tries to analyse the image of ψ. That leads to a bunch of new genus one curves for which one has to decide if they have rational points or not! ❄

As the final example we shall prove the proposition below about the curves from the family $y^2 = x(x^2 - p^2)$ where p is an odd prime. The discriminant is 2^2p^6, so the only places where the curve has bad reduction are the primes 2 and p. The rank is computed only in case it is zero, else the proposition merely gives an upper bound for the rank.

Proposition 4.4 *Let E be the elliptic curve $y^2 = x(x-p)(x+p)$. If r denotes the rank of E, one has*

- □ $r \leq 2$ *if* $p \equiv 1 \mod 8$
- □ $r = 0$ *if* $p \equiv 3 \mod 8$
- □ $r \leq 1$ *if* $p \equiv 5$ *or* $7 \mod 8$

Before we start the proof we remark that the discriminant of E equals 2^2p^6 so the only bad places are 2 and p. Except for $p = 3$ the curve E has good reduction at the prime 3, and the equation reduces to $y^2 = x(x-1)(x+1) \mod 3$. It follows that $\#E(\mathbb{F}_3) = 4$ and since $E_{tors}(\mathbb{Q})$ maps injectively into $E(\mathbb{F}_3)$ one has $E_{tors}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If $p = 3$ one has $\#E(\mathbb{F}_3) = 4$ as well, and $E_{tors}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ even in that case.
PROOF OF PROPOSITION 4.4: The beginning of the computation is a tabulation of the images of the two-torsion points. Here it comes:

$a_1 = -p$	$(2p^2, -p, -2p)$	$+$	$-$	$-$	1	0	1	0	1	1
$a_2 = 0$	$(p, -p^2, -p)$	$+$	$-$	$-$	0	0	0	1	0	1
$a_3 = p$	$(2p, p, 2p^2)$	$+$	$+$	$+$	1	0	1	1	1	0

where the p-components are coloured light green and the two-components not so light green. To ease reading (and writing!) let $H \simeq \mu_2^3 \times (\mathbb{Z}/2\mathbb{Z})^3$ denote the subgroup of $(\mathbb{Q}^*/\mathbb{Q}^{*2})^3$ consisting of the elements all whose components are trivial but the sign- and the 2-components.

Again, one whishes to apply the trick from the previous example applies and change the point P by a combination of two-torsion points so that $\psi(P)$ has no p-component, but for this to work, one must be sure that any p-component lies in the space generated by the p-components of the two-torsion points (the light green rows to the right in the table) and as theses are linearly dependent an argument is needed.

If $v_p(x) < 0$, all p-components vanish by lemma 4.2, and the argument given there applies to the case $v_p(x) = 0$ as well. If $v_p(x) \geq 2$, one has $v_p(x \pm p) = 1$. Hence $v_p(x)$ is even, and the vector is $(0, 1, 1)$. If $v_p(x) = 1$, one checks that $v_p(x + p) + v_p(x - p)$ is odd, so $v_p(x + p)$ and $v_p(x - p)$ are of opposite parities. The vectors are $(1, 0, 1)$ and $(1, 1, 0)$.

These modified values of ψ form a set of representatives for the quotient $\operatorname{Im}\psi/H \cap \operatorname{Im}\psi$, so the number of them being independent will equal the rank of E. Except for the zero vector there are exactly three possible such vectors:

x	$x+p$	$x-p$	x	$x+p$	$x-p$
$+$	$-$	$-$	0	0	0
$+$	$+$	$+$	0	1	1
$+$	$-$	$-$	0	1	1

This is easy to figure out using the three following properties:

☐ The sign configuration is either $+++$ or $---$.

☐ $v_2(x) = 0$. Indeed, if $v_2(x) < 0$, one has $v_2(x - a_i) \equiv 0 \mod 2$ and $\psi(P) \in H$. If $v_2(x) > 0$, one finds $v_2(x \pm p) = v_2(x)$ and using the Weierstrass equation one sees that $v_2(x)$ is even. Again all non-sign components vanish and $\psi(P) \in H$.

☐ $v_2(x+p) \equiv v_2(x-p) \mod 2$. Indeed, since $v_2(x) = 0$, the Weierstrass equation gives that $v_2(x + p) + v_2(x - p)$ is even, and hence the two have the same parity.

The relations in the table above are relations modulo $\mathbb{Q}^{*2}$. Lifting to equalities in Q^* one arrives at three sets of equations the quantities $x + p$, x and $x - p$ satisfy. They are listed in the next table, where $a, b, c \in \mathbb{Q}^*$.

	$x+p$	x	$x-p$
1	a^2	$-b^2$	$-c^2$
2	$2a^2$	b^2	$2c^2$
3	$2a^2$	$-b^2$	$-2c^2$

These conditions may be expressed in a common form as

$$x + p = \epsilon a^2 \qquad x^2 = \eta b^2 \qquad x - p = \kappa c^2$$

where ϵ, η and κ stands for appropriate number among ± 2 and ± 1 as in the table above. As a side remark, eliminating x, one finds the two quadratic equations

$$\epsilon a^2 - \eta b^2 = p \qquad \eta b^2 - \kappa c^2 = -p$$

that cut out the three shadow curves of this case.
The next step is to eliminate powers of p from the denominators of a, b and c. Now $v_p(x+p)$ is even, so $v_p(x) \leq 1$, hence $v_p(x) \leq 0$ being even. It follows that $v_p(x) = v_p(x \pm p) \leq 0$, and consequently that $v_p(a) = v_p(b) = v_p(c) = \nu \leq 0$. Clearing powers of p from the denominators, one finds the three equations:

$$p^{2\nu}x + p^{2v+1} = \epsilon\alpha^2 \qquad p^{2\nu}x = \eta\beta^2 \qquad p^{2\nu}x - p^{2\nu+1} = \kappa\gamma^2 \tag{✗}$$

Reducing these equations modulo p one finds

$$\epsilon\alpha^2 \equiv \eta\beta^2 \equiv \kappa\gamma^2 \tag{✗✗}$$

From here we proceed case by case:

□ Assume that the vector number one survives. In this case the values of ϵ and η are $\epsilon = 1$ and $\eta = -1$. Hence $\alpha^2 \equiv -\beta^2 \mod p$, so -1 has a square root mod p, and it follows that $p \equiv 1 \mod 4$, or $p \equiv 1$ or $5 \mod 8$.

□ Assume that the vector number two survives. Then $2\alpha^2 = \beta^2$, so 2 has a square root mot p. This occurs if and only if $p \equiv \pm 1 \mod 8$.

□ Assume that the vector number three survives. Then $\epsilon = 2$ and $\eta = \kappa = -1$, and the equations become $-2\alpha^2 = \beta^2$ and $-\beta^2 = -2\gamma^2$ so both -2 and 2 have square roots. It follows that $p \equiv 1$ or $3 \mod 8$ and $p \equiv \pm 1 \mod 8$, that is $p \equiv 1 \mod 8$.

Summing up, we see that if $p \equiv 3 \mod 8$, none of vectors survive and the the rank is zero. If $p \equiv 3$ or $5 \mod 8$, one of them possibly survives, and the rank is at most one. In the last case when $p \equiv 1 \mod 8$, all three vectors can survive, but as they dependent, the rank of E is bounded by two. ❑

Example 4.3. — The cases $p = 5$ and $p = 13$. If $p = 5$ one finds with a little thought and a short search the rational point $(-4, 6)$ on E. This is not a torsion point since there is only two-torsion. Hence one has $E(\mathbb{Q}) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with $(-4, 6)$ as a generator for an infinite subgroup (what are the others?).

The next prime p that is congruent 5 mod 8 is $p = 13$. One finds in that case the rational point $(\frac{6^2}{5^2}, \frac{6 \cdot 17 \cdot 19}{5^3})$ (may be with some deeper thought and some more work, but once the point is given, it is trivial to check). So in that case one also has $E(\mathbb{Q}) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. ❄

The congruent number problem

An old problem with deep roots in the antiquity concerns areas of right angled triangles. Which whole numbers n can be the area of a right angled triangle all of whose sides are rational? That is, which numbers n are of the form $n = ab/2$ for rational numbers a and b such that $a^2 + b^2 = c^2$ with c rational? Keith Conrad ([2]) has written a nice introductuon to this circle of ideas. The following exercise links the problem of the congruent numbers to the problem of determining the rank of certain elliptic curves like the ones we just studied:

Problem 4.1. Let the elliptic curve E be given by

$$y^2 = x^3 - n^2x$$

where n is a natural number.

a) Assume that n is congruent with a, b and c as above. Set $x = n(a + c)/b$ and $y = 2n^2(a + c)/b^2$. Show that (x, y) is a point on E.

b) If (x, y) is a rational point on E wich is two-torsion (*i.e.*, $y \neq 0$) show that n is congruent. Hint: $a = (x^2 - n^2)/y$, $b = 2nx/y$ and $c = (x^2 + n^2)/y$.

✸

The to first example in this paragraph that $n = 1$, which in fact goes back to Fermat, and $n = 2$ are not congruent. The congruent number problem is still partly open despite the effort of several of the cleverest mathematicians. The conjecture is that n should be congruent if it lies in one of the congruence classes 5, 6 or 7 modulo 8. If $n = p$ is a prime, we are in the third case of the proposition 4.4, and the prime case solved completely, the first one to claim a solution was the german mathematician Kurt Heegner, but it was unclear whether it was proved or not. Paul Monsky settled the prime cases in 1990, unnecessary to say, with very advanced techniques.

In our context we can thus formulate as a complement to proposition 4.4 the following proposition:

Proposition 4.5 *Let p be a prime such that $p \equiv 5$ or $7 \mod 8$, and let E be the ellitiptic curve*

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

Then $E(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The arithemtic of ellitiptic curves is filled with awfully big numbes, so also here. As an (modest) illustration is the case $p = 53$, which is a congruent number after the proposition. The right angled triangle with sides $a = 1873180325^2 - 1158313156^2$ and $b = 2 \cdot 1873180325 \cdot 1158313156$ has area $53 \cdot 297855654284978790^2$!

Problem 4.2. Show that the triangle with sides 20/3, 3/2 and 41/6 is right angled and has area 5. ✸

Problem 4.3. Use the rational point in example 4.3 above to find a right angled triangle with rational sides and area 13. ✸

Bibliografi

[1] Anthony W. Kapp: *Elliptic curves*, Mathematical notes, Priceton University, 1992. ISBN 0-691-08559-5(BP)

[2] Keith Conrad: *The congruent number problem* at http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/congnumber.pdf