Elliptic Curves over $\mathbb{Q}$

Peter Birkner

Technische Universiteit Eindhoven

DIAMANT Summer School on Elliptic and Hyperelliptic Curve Cryptography

16 September 2008

What is an elliptic curve? (1)

An elliptic curve E over a field k in Weierstraß form can be given by the equation:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

- The coefficients a_1, a_2, a_3, a_4, a_6 are in k.
- We need that the partial derivatives

  $$2y + a_1 x + a_3 \text{ and } 3x^2 + 2a_2 x + a_4 - a_1 y$$

  do not vanish simultaneously for each point (x, y) over $\overline{k}$. This is to avoid singularities on the curve.

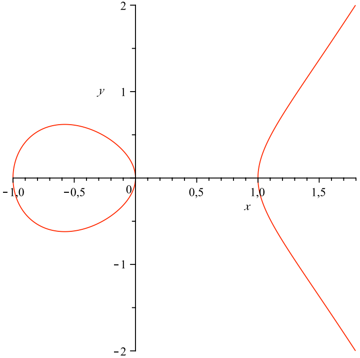
What is an elliptic curve? (2)

If $\mathrm{char}(k) \neq 2,3$ we can always transform to short Weierstraß form:

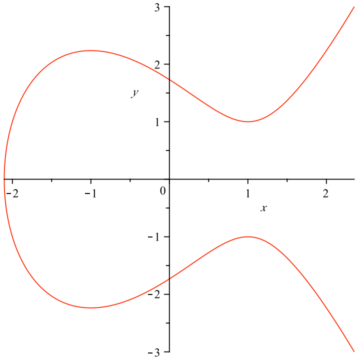
$$E : y^2 = x^3 + ax + b \quad (a, b \in k)$$

- If the discriminant $\Delta = -16(4a^3 + 27b^2)$ of E is $\neq 0$, then the equation describes an elliptic curve without singular points.
- From now on $k = \mathbb{Q}$ and short Weierstraß form!
- The set of all points on E together with the point at infinity P_∞ forms an additive group. P_∞ is the neutral element in this group.

Example: elliptic curves (over the reals)

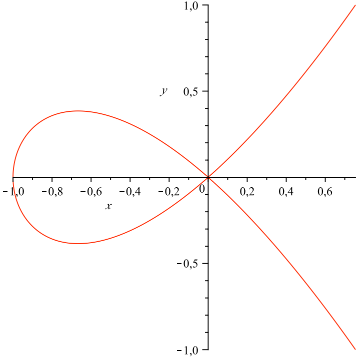


$E_1 : y^2 = x^3 - x$, $\Delta \neq 0$



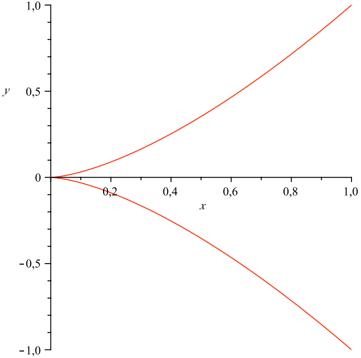
$E_2 : y^2 = x^3 - 3x + 3$, $\Delta \neq 0$

Example: non-elliptic curves (over the reals)



$E_3 : y^2 = x^3 + x^2$, $\Delta = 0$

"Node"



$E_4 : y^2 = x^3$, $\Delta = 0$

"Cusp"

Group law for $y^2 = x^3 + ax + b$, $\mathrm{char}(k) \neq 2, 3$

The set of points on an elliptic curve together with P_∞ forms an additive group $(E, \oplus)$.

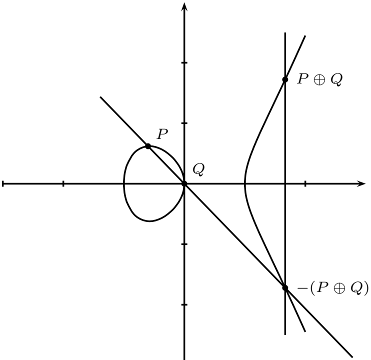
- The neutral element in this group is P_∞.
- The negative of a point $P = (x, y)$ is $-P = (x, -y)$.
- For two points $P = (x_1, y_1)$, $Q = (x_2, y_2)$ with $P \neq \pm Q$ we have $P \oplus Q = (x_3, y_3)$, where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

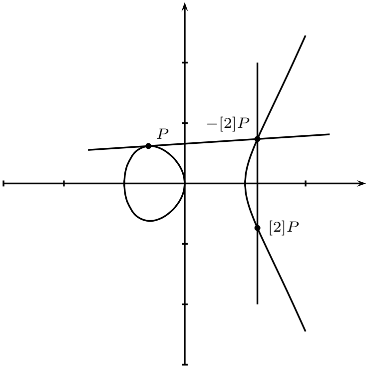
- For $P \neq \pm P$ we have $[2]P = (x_3, y_3)$, where

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

The graphical addition law



Addition: $P \oplus Q$



Doubling: $[2]P$

Order and torsion

- The order of a point P is the smallest positive integer n such that $[n]P = \underbrace{P \oplus \ldots \oplus P}_{n \text{ times}} = P_\infty$.
- If $[n]P$ never adds up to P_∞, then the order of P is ∞.
- The order of the neutral element P_∞ is 1.

- The set of all points with finite order is a subgroup of the group of points. It is called the torsion subgroup of E.
- Similarly, the group of points with order ∞, together with P_∞ is called the non-torsion subgroup of E.

Example (part 1)

$$E : y^2 = x^3 - \frac{1}{36}x^2 - \frac{5}{36}x + \frac{25}{1296} \text{ over } \mathbb{Q}$$

Points of order 4

$(0,\ -\frac{5}{36})$
$(0,\ \frac{5}{36})$
$(\frac{5}{9},\ -\frac{35}{108})$
$(\frac{5}{9},\ \frac{35}{108})$

Points of order 2

$(\frac{5}{18},\ 0)$
$(\frac{1}{6},\ 0)$
$(-\frac{5}{12},\ 0)$

There are no more points (over $\mathbb{Q}$) of finite order!

Together with P_∞ these points are all possible torsion points.
The torsion subgroup of E is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$.

The point $P = (\frac{77}{162}, \frac{170}{729})$ is a non-torsion point on E.

Example (part 2)

$$E : y^2 = x^3 - \frac{1}{36}x^2 - \frac{5}{36}x + \frac{25}{1296} \text{ over } \mathbb{Q}$$

The point $P = (\frac{77}{162}, \frac{170}{729})$ has order ∞ and is thus a non-torsion point on the curve E.

The subgroup $\langle P \rangle$ generated by P is isomorphic to $\mathbb{Z}$ via the mapping $\mathbb{Z} \to E(\mathbb{Q})$, $n \mapsto [n]P$.

Hence the group structure of E is $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}^r$, where $r > 0$.

The number r is called rank of the elliptic curve.

There could be another point of order ∞ which is not a multiple of P. In this case the rank would be 2 or higher.

Which torsion groups are possible?

Theorem of Mazur

Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of E is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/n \text{ for } n = 1,2,3,4,5,6,7,8,9,10 \text{ or } 12$$

$$\mathbb{Z}/2 \times \mathbb{Z}/2n \text{ for } n = 1,2,3,4.$$

For example, there is no elliptic curve over $\mathbb{Q}$ with a point of order 11, 13, 14 etc.

How to find torsion points? (part 1)

Theorem of Lutz-Nagell

Let E over $\mathbb{Q}$ be an elliptic curve with short Weierstraß equation

$$y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z}).$$

Then for all non-zero torsion points P we have:

1. The coordinates of P are in $\mathbb{Z}$, i.e. $\mathrm{x}(P)$, $\mathrm{y}(P) \in \mathbb{Z}$
2. If the order of P is greater than 2 (i.e. $\mathrm{y}(P) \neq 0$), then $\mathrm{y}(P)^2$ divides $4a^3 + 27b^2$.

How to find torsion points? (part 2)

Example

Let $p \in \mathbb{Z}$ be a prime and let $E : y^2 = x^3 + p^2$ be an elliptic curve over $\mathbb{Q}$. Since $x^3 + p^2 = 0$ has no solutions in $\mathbb{Q}$, there is no 2-torsion.

- Now, $4a^3 + 27b^2 = 27p^4$.
- Let (x, y) be a torsion point. Then we know that $x, y \in \mathbb{Z}$ and $y^2 \,|\, 27p^4$, thus $y \in \{\pm 1, \pm 3, \pm p, \pm p^2, \pm 3p, \pm 3p^2\}$.
- It is clear that $(0, \pm p) \in E$, and they can be checked to be points of order 3.

Reduction modulo p (part 1)

- Let E be an elliptic curve over $\mathbb{Q}$ given by the equation $E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$.
- Let p be a prime. Then we can consider the curve equation "modulo p", i.e. we take a and b modulo p.
- The new equation $E' : y^2 = x^3 + a'x + b'$ describes an elliptic curve if $\operatorname{disc}(E') \neq 0$, i.e. not a multiple of p.

Definition

We say that E has good reduction at p if the discriminant of E is not a multiple of p, otherwise E has bad reduction at p.

Reduction modulo p (part 2)

Example

Let E over $\mathbb{Q}$ be given by $y^2 = x^3 + 3$. The discriminant of this curve is $\Delta = -3888 = -2^4 3^5$.

Thus the only primes of bad reduction are 2 and 3, and E modulo p is non-singular for all $p \geq 5$.

Let $p = 5$ and consider the reduction E' of E modulo 5. Then we have

$$E(\mathbb{Z}/5) = \{P_\infty, (1,2), (1,3), (2,1), (2,4), (3,0)\}.$$

Reduction modulo p (part 3)

Proposition
Let E over $\mathbb{Q}$ be an elliptic curve and let m be a positive integer and p a prime number such that $\gcd(p,m) = 1$. For E modulo p the reduction map modulo p

$$E(\mathbb{Q})[m] \to E'(\mathbb{Z}/p)$$

is injective.

Corollary
The number of m-torsion points of E over $\mathbb{Q}$ divides the number of points over $\mathbb{Z}/p$.

Reduction modulo p (part 4)

Example $E : y^2 = x^3 + 3$ over $\mathbb{Q}$

- Reduction modulo 5 gives $E(\mathbb{Z}/5) = \{P_\infty, (1,2), (1,3), (2,1), (2,4), (3,0)\}$, i.e. the reduced curve has 6 points.
- Reducing the curve modulo 7 gives 13 points.
- Now let's assume $q \neq 5, 7$ be prime.
- Proposition $\Rightarrow \#E(\mathbb{Q})[q]$ divides 6 and 13 $\Rightarrow \#E(\mathbb{Q})[q] = 1$.

Reduction modulo p (part 5)

Example $E : y^2 = x^3 + 3$ over $\mathbb{Q}$

- $q = 5$: Prop. $\Rightarrow \#E(\mathbb{Q})[5]$ divides 13, i.e. $5 \mid 13$ if $\#E(\mathbb{Q})[5]$ is non-trivial. Hence $\#E(\mathbb{Q})[5] = 1$.
- Same argument for $q = 7$: $\#E(\mathbb{Q})[7] = 1$.
- Outcome: $E(\mathbb{Q})$ has trivial torsion subgroup $\{P_\infty\}$.

  But $(1,2)$ is a point on the curve, so it must be a point with infinite order, and the rank is at least 1.

Rank records for elliptic curves over $\mathbb{Q}$

T	$B(T)>=$	Author(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	18	Elkies (2006)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (2007,2008)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	6	Dujella – Lecacheux (2001)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (2008), Dujella – Eroshkin (2008), Elkies (2008), Dujella (2008)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella – Kulesz (2001), Elkies (2006)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/9\mathbb{Z}$	3	Dujella (2001), MacLeod (2004), Eroshkin (2006), Eroshkin – Dujella (2007)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	3	Dujella (2001,2005,2006), Rathbun (2003,2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	14	Elkies (2005)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (2005), Eroshkin (2008), Dujella – Eroshkin (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006), Campbell – Goins (2003), Rathbun (2003,2006) Flores – Jones – Rollick – Weigandt (2007)

http://web.math.hr/~duje/tors/tors.html

How to construct elliptic curves with prescribed torsion subgroup?

TABLE 3. *Parametrization of torsion structures*

1. 0: $y^2 = x^3 + ax^2 + bx + c$; $\Delta_1(a,b,c) \neq 0$,
   $\Delta_1(a,b,c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.
2. $Z/2Z$: $y^2 = x(x^2 + ax + b)$; $\Delta_1(a,b) \neq 0$, $\Delta_1(a,b) = a^2b^2 - 4b^3$.
3. $Z/2Z \times Z/2Z$: $y^2 = x(x+r)(x+s)$, $r \neq 0 \neq s \neq r$.
4. $Z/3Z$: $y^2 + a_1xy + a_3y = x^3$; $\Delta(a_1, a_3) = a_1{}^3a_3{}^3 - 27a_3{}^4 \neq 0$.

(The form $E(b,c)$ is used in all parametrizations below where in $E(b,c)$ $y^2 + (1-c)xy - by = x^3 - bx^2$, $(0,0)$ is a torsion point of maximal order, $\Delta(b,c) = \alpha^4b^3 - 8\alpha^2b^4 - \alpha^3b^3 + 36\alpha b^4 + 16b^5 - 27b^4$, and $\alpha = 1-c$.)

5. $Z/4Z$: $E(b,c)$, $c = 0$, $\Delta(b,c) = b^4(1+16b) \neq 0$.
6. $Z/4Z \times Z/2Z$: $E(b,c)$, $b = v^2 - \frac{1}{16}$, $v \neq 0, \pm\frac{1}{4}$, $c = 0$.
7. $Z/8Z \times Z/2Z$: $E(b,c)$, $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$,
   $d = \alpha(8\alpha+2)/(8\alpha^2-1)$, $d(d-1)(2d-1)(8d^2-8d+1) \neq 0$.
8. $Z/8Z$: $E(b,c)$, $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$, $\Delta(b,c) \neq 0$.
9. $Z/6Z$: $E(b,c)$, $b = c + c^2$, $\Delta(b,c) = c^6(c+1)^3(9c+1) \neq 0$.
10. $Z/6Z \times Z/2Z$: $E(b,c)$, $b = c + c^2$, $c = (10-2\alpha)/(\alpha^2-9)$,
    $\Delta(b,c) = c^6(c+1)^3(9c+1) \neq 0$.
11. $Z/12Z$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = m + \tau$, $f = m/(1-\tau)$,
    $m = (3\tau - 3\tau^2 - 1)/(\tau - 1)$, $\Delta(b,c) \neq 0$.
12. $Z/9Z$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = f(f-1) + 1$, $\Delta(b,c) \neq 0$.
13. $Z/5Z$: $E(b,c)$, $b = c$, $\Delta(b,c) = b^5(b^2 - 11b - 1) \neq 0$.
14. $Z/10Z$: $E(b,c)$, $b = cd$, $c = fd - f$, $d = f^2/(f - (f-1)^2)$, $f \neq (f-1)^2$, $\Delta(b,c) \neq 0$.
15. $Z/7Z$: $E(b,c)$, $b = d^3 - d^2$, $c = d^2 - d$, $\Delta(b,c) = d^7(d-1)^7(d^3 - 8d^2 + 5d + 1) \neq 0$.

(Kubert: Universal Bounds on the Torsion of Elliptic Curves, 1976)

Construction of an elliptic curve with torsion $\mathbb{Z}/2 \times \mathbb{Z}/4$ and rank > 0

- Kubert's curve $E(b,c) : Y^2 + (1-c)XY - bY = X^3 - bX^2$
- Apply transformation $y = Y + \frac{(1-c)X-b}{2}$ and $x = X$ to get the form

$$E'(b,c) : y^2 = x^3 + \frac{(c-1)^2 - 4b}{4}x^2 + \frac{b(c-1)}{2}x + \frac{b^2}{4}$$

- For $\mathbb{Z}/2 \times \mathbb{Z}/4$ use $c = 0$ and $b = v^2 - \frac{1}{16}$, $v \neq 0, \pm\frac{1}{4}$ (see entry #6 of the previous slide)
- The curve $E'(v^2 - \frac{1}{16}, 0)$ has torsion subgroup $\mathbb{Z}/2 \times \mathbb{Z}/4$

How to get rank > 0?

Points of order 4

$(0,\ -\frac{1}{2}v^2 + \frac{1}{32})$

$(0,\ \frac{1}{2}v^2 - \frac{1}{32})$

$(2v^2 - \frac{1}{8},\ -\frac{1}{8}v(16v^2 - 1))$

$(2v^2 - \frac{1}{8},\ \frac{1}{8}v(16v^2 - 1))$

Points of order 2

$(v^2 - \frac{1}{16},\ 0)$

$(-\frac{1}{8} + \frac{1}{2}v,\ 0)$

$(-\frac{1}{8} - \frac{1}{2}v,\ 0)$

Try to find a point on the curve with x-coordinate different from the x-coordinate of all torsion points, for instance $x_0 = v^2 + \frac{175}{1296}$.

How to get rank > 0?

Plug in x_0 into curve equation $E'(v^2 - \frac{1}{16}, 0)$ and make monic:

$$y^2 = v^4 + \frac{175}{1458}v^2 + \frac{113569}{8503056}$$

To find solutions to this, we replace $u = v^2$ on the right-hand side and get

$$u^2 + \frac{175}{1458}u + \frac{113569}{8503056}.$$

Now, we require that u and $u^2 + \frac{175}{1458}u + \frac{113569}{8503056}$ are squares in $\mathbb{Q}$.

This leads to the elliptic curve

$$E_{gen} : z^2 = u\left(u^2 + \frac{175}{1458}u + \frac{113569}{8503056}\right).$$

How to get rank > 0?

$$E_{gen} : z^2 = u^3 + \frac{175}{1458}u^2 + \frac{113569}{8503056}u$$

Finding a point (u, z) on this curve, where u is a square, ensures that $u^2 + \frac{175}{1458}u + \frac{113569}{8503056}$ is a square and that we can write $u = v^2$.

With this we have a solution to $y^2 = v^4 + \frac{175}{1458}v^2 + \frac{113569}{8503056}$.

Using this v as parameter for $E'(v^2 - \frac{1}{16},\ 0)$ we know that the curve has a point with x-coordinate $v^2 + \frac{175}{1296}$ and this point is a non-torsion point. Hence, rank of $E' > 0$.

The curve E_{gen} has infinitely many points and thus there are infinitely many parameters v to generate a curve with torsion $\mathbb{Z}/2 \times \mathbb{Z}/4$ and rank at least 1.

Thank you for your attention!