Elliptic curves, volume 4
Points of finite order

Alexandr Kazda

Charles University, Prague

March 26, 2010

- Our goal: To prove that if P has finite order then P must have integer coordinates.
- The idea: We show that if $P = (x, y)$ has finite order then for all p prime p does not divide the denominator of x or y.
- This talk: A lemma about a certain important group homomorphism.

- Our goal: To prove that if P has finite order then P must have integer coordinates.
- The idea: We show that if $P = (x, y)$ has finite order then for all p prime p does not divide the denominator of x or y.
- This talk: A lemma about a certain important group homomorphism.

- Our goal: To prove that if P has finite order then P must have integer coordinates.
- The idea: We show that if $P = (x, y)$ has finite order then for all p prime p does not divide the denominator of x or y.
- This talk: A lemma about a certain important group homomorphism.

Exponent

- Let p be a fixed prime.
- If $q = p^\rho \cdot m/n$ then $\mathrm{ord}(q) = \rho$.

Exponent

- Let p be a fixed prime.
- If $q = p^\rho \cdot m/n$ then $\mathrm{ord}(q) = \rho$.

Exponent on $C(\mathbb{Q})$

- Assume
$$x = \frac{m}{np^\rho}, \quad y = \frac{u}{wp^\sigma}.$$
- Then the normal form gives us:
$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\rho + bmn^2p^{2\rho} + cn^3p^{3\rho}}{n^3p^{3\rho}}$$
- Therefore $2\sigma = 3\rho$ which is only possible when there is an integer τ such that $\sigma = 3\tau, \rho = 2\tau$.
- This is why we define
$$C(p^\rho) = \{(x, y) \in C(\mathbb{Q}) : \mathrm{ord}(x) \leq -2\rho, \mathrm{ord}(y) \leq -3\rho\}$$

Exponent on $C(\mathbb{Q})$

- Assume
$$x = \frac{m}{np^\rho}, \quad y = \frac{u}{wp^\sigma}.$$
- Then the normal form gives us:
$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\rho + bmn^2p^{2\rho} + cn^3p^{3\rho}}{n^3p^{3\rho}}$$
- Therefore $2\sigma = 3\rho$ which is only possible when there is an integer τ such that $\sigma = 3\tau, \rho = 2\tau$.
- This is why we define
$$C(p^\rho) = \{(x, y) \in C(\mathbb{Q}) : \mathrm{ord}(x) \leq -2\rho, \mathrm{ord}(y) \leq -3\rho\}$$

Exponent on $C(\mathbb{Q})$

- Assume
$$x = \frac{m}{np^\rho}, \quad y = \frac{u}{wp^\sigma}.$$
- Then the normal form gives us:
$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\rho + bmn^2p^{2\rho} + cn^3p^{3\rho}}{n^3p^{3\rho}}$$
- Therefore $2\sigma = 3\rho$ which is only possible when there is an integer τ such that $\sigma = 3\tau, \rho = 2\tau$.
- This is why we define
$$C(p^\rho) = \{(x, y) \in C(\mathbb{Q}) : \mathrm{ord}(x) \leq -2\rho, \mathrm{ord}(y) \leq -3\rho\}$$

Exponent on $C(\mathbb{Q})$

- Assume
$$x = \frac{m}{np^\rho}, \quad y = \frac{u}{wp^\sigma}.$$
- Then the normal form gives us:
$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\rho + bmn^2p^{2\rho} + cn^3p^{3\rho}}{n^3p^{3\rho}}$$
- Therefore $2\sigma = 3\rho$ which is only possible when there is an integer τ such that $\sigma = 3\tau, \rho = 2\tau$.
- This is why we define
$$C(p^\rho) = \{(x, y) \in C(\mathbb{Q}) : \mathrm{ord}(x) \leq -2\rho, \mathrm{ord}(y) \leq -3\rho\}$$

- For convenience, we add O to $C(p^\rho)$.
- Observe that $C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset \dots$
- We prove that they are actually subgroups.

- For convenience, we add O to $C(p^\rho)$.
- Observe that $C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset \dots$
- We prove that they are actually subgroups.

- For convenience, we add O to $C(p^\rho)$.
- Observe that $C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset \dots$
- We prove that they are actually subgroups.

One ring to rule them all

- We will need the ring $R = \{q \in \mathbb{Q} : \mathrm{ord}(q) \geq 0\}$.
- Observe (and do not forget) that $(x, y) \in C(p^\rho)$ iff

$$\frac{x}{y} \in p^\rho R \quad \& \quad \frac{1}{y} \in p^{3\rho} R.$$

One ring to rule them all

- We will need the ring $R = \{q \in \mathbb{Q} : \mathrm{ord}(q) \geq 0\}$.
- Observe (and do not forget) that $(x, y) \in C(p^\rho)$ iff

$$\frac{x}{y} \in p^\rho R \quad \& \quad \frac{1}{y} \in p^{3\rho} R.$$

Some random formulas

- $s_i = \alpha t_i + \beta$
- $s_i = t_i^3 + a t_i^2 s_i + b t_i s_i^2 + c s_i^3$
- $$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_1 + t_2)s_2 + b s_2}{1 - a t_1^2 - b t_1 (s_2 + s_1) - c(s_2 + s_1 s_2 + s_1^2)}$$

Some random formulas

- $s_i = \alpha t_i + \beta$
- $s_i = t_i^3 + a t_i^2 s_i + b t_i s_i^2 + c s_i^3$
- $$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_1 + t_2)s_2 + b s_2}{1 - a t_1^2 - b t_1 (s_2 + s_1) - c(s_2 + s_1 s_2 + s_1^2)}$$

Some random formulas

- $s_i = \alpha t_i + \beta$
- $s_i = t_i^3 + a t_i^2 s_i + b t_i s_i^2 + c s_i^3$
- $$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_1 + t_2)s_2 + b s_2}{1 - a t_1^2 - b t_1 (s_2 + s_1) - c(s_2 + s_1 s_2 + s_1^2)}$$

Why??

- Observe that

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_1 + t_2)s_2 + bs_2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2 + s_1 s_2 + s_1^2)}$$

  has denominator not divisible by p.
- Therefore, $\alpha \in p^{2\rho} R$.
- From $\beta = \alpha t_1 - s_1$, we get $\beta \in p^{3\rho} R$.

Why??

- Observe that

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_1 + t_2)s_2 + bs_2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2 + s_1 s_2 + s_1^2)}$$

  has denominator not divisible by p.
- Therefore, $\alpha \in p^{2\rho} R$.
- From $\beta = \alpha t_1 - s_1$, we get $\beta \in p^{3\rho} R$.

Searching for t_3

- The equation for t_1, t_2 and t_3:

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3$$

- Therefore (Viète and some calculation):

$$t_1 + t_2 + t_3 = \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}$$

- Using $\alpha \in p^{2\rho}R$ and $\beta \in p^{3\rho}R$ gives us $t_1 + t_2 + t_3 \in p^{3\rho}R$.

Searching for t_3

- The equation for t_1, t_2 and t_3:

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3$$

- Therefore (Viète and some calculation):

$$t_1 + t_2 + t_3 = \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}$$

- Using $\alpha \in p^{2\rho}R$ and $\beta \in p^{3\rho}R$ gives us $t_1 + t_2 + t_3 \in p^{3\rho}R$.

Searching for t_3

- The equation for t_1, t_2 and t_3:

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3$$

- Therefore (Viète and some calculation):

$$t_1 + t_2 + t_3 = \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}$$

- Using $\alpha \in p^{2\rho}R$ and $\beta \in p^{3\rho}R$ gives us $t_1 + t_2 + t_3 \in p^{3\rho}R$.

Conclusions

- The map $t : (x, y) \mapsto x/y$ is a group homomorphism $C(p^\rho) \to \frac{p^\rho R}{p^{3\rho} R}$
- Kernel of t is $C(p^{3\rho})$, therefore

$$t : \frac{C(p^\rho)}{C(p^{3\rho})} \to \frac{p^\rho R}{p^{3\rho} R}$$

  is a one-to-one (injective) group homomorphism.
- Note that $\frac{p^\rho R}{p^{3\rho} R}$ is a cyclic group of order $p^{2\rho}$ and so $\frac{C(p^\rho)}{C(p^{3\rho})}$ is cyclic of order p^σ for some $\sigma \in \{0, 1, \ldots, 2\rho\}$.

Conclusions

- The map $t : (x, y) \mapsto x/y$ is a group homomorphism $C(p^\rho) \to \frac{p^\rho R}{p^{3\rho} R}$
- Kernel of t is $C(p^{3\rho})$, therefore

$$t : \frac{C(p^\rho)}{C(p^{3\rho})} \to \frac{p^\rho R}{p^{3\rho} R}$$

  is a one-to-one (injective) group homomorphism.
- Note that $\frac{p^\rho R}{p^{3\rho} R}$ is a cyclic group of order $p^{2\rho}$ and so $\frac{C(p^\rho)}{C(p^{3\rho})}$ is cyclic of order p^σ for some $\sigma \in \{0, 1, \ldots, 2\rho\}$.

Conclusions

- The map $t : (x, y) \mapsto x/y$ is a group homomorphism $C(p^\rho) \to \frac{p^\rho R}{p^{3\rho} R}$
- Kernel of t is $C(p^{3\rho})$, therefore

$$t : \frac{C(p^\rho)}{C(p^{3\rho})} \to \frac{p^\rho R}{p^{3\rho} R}$$

  is a one-to-one (injective) group homomorphism.
- Note that $\frac{p^\rho R}{p^{3\rho} R}$ is a cyclic group of order $p^{2\rho}$ and so $\frac{C(p^\rho)}{C(p^{3\rho})}$ is cyclic of order p^σ for some $\sigma \in \{0, 1, \ldots, 2\rho\}$.

Thanks for your attention.