Diophantine characterization of rational torsion structures on elliptic curves

Irene García–Selfa
igselfa@us.es

Departamento de Matemática Aplicada
Universidad de Huelva

Diciembre de 2006

Introduction (I)

$$E: \; Y^2 = X^3 + AX + B, \quad A, B \in \mathbf{Z}.$$

(A, B) characterize $E(\mathbf{Q}) = \mathrm{Tor}(E(\mathbf{Q})) + \mathbf{Z}^r$ up to

$$(A, B) \longrightarrow \left(u^4 A, u^6 B\right).$$

Introduction (II)

Stupid Question:

Introduction (II)

Stupid Question:

How does $(A, B$

Introduction (II)

Stupid Question:

How does (A, B) characterize $\mathrm{Tor}(E(\mathbf{Q}))$?

Answer to rank $\Longrightarrow$ \$1000000 (?), Fields (?),...

Introduction (II)

Stupid Question:

How does (A, B) characterize $\mathrm{Tor}(E(\mathbf{Q}))$?

Answer to rank $\Longrightarrow$ \$1000000 (?), Fields (?),...

(That is work in progress)

Diophantine characterization

1996 (K. Ono): Non–cyclic case characterized with (nice) Diophantine equations.

Diophantine characterization

1996 (K. Ono): Non–cyclic case characterized with (nice) Diophantine equations.

1999 (Qiu–Zhang): Even cyclic case characterized with (horrible) Diophantine equations (three times!).

Warning: Don't look for (A, B) here!

Reduction

It is enough:

Reduction

It is enough:

$E[2]$ (solving $X^3 + AX + B = 0$).

Reduction

It is enough:

$E[2]$ (solving $X^3 + AX + B = 0$).

$E[n]$ for $n = 3, 4, 5, 7, 8, 9$ (Mazur).

Overview

$n = 3, 4, 5, 7, 8, 9$

Overview

$n = 3, 4, 5, 7, 8, 9$

There are polynomials $F_n(p, q),\ G_n(p, q) \in \mathbf{Z}[p, q]$ such that

Overview

$n = 3, 4, 5, 7, 8, 9$

There are polynomials $F_n(p, q),\ G_n(p, q) \in \mathbf{Z}[p, q]$ such that

$$E[n] \neq \emptyset \iff \left\{ \begin{array}{l} A = F_n \\ B = G_n \end{array} \right. \text{ has integral solution}$$

Remarks

–) Degenerate conditions.

Remarks

–) Degenerate conditions.

–) F_n, G_n (quasi–)homogeneous.

Remarks

–) Degenerate conditions.

–) F_n, G_n (quasi–)homogeneous.

–) Either F_n or G_n irreducible $\Longrightarrow$ Thue equations.

Remarks

–) Degenerate conditions.

–) F_n, G_n (quasi–)homogeneous.

–) Either F_n or G_n irreducible $\Longrightarrow$ Thue equations.

–) More than one possible system.

Remarks

–) Degenerate conditions.

–) F_n, G_n (quasi–)homogeneous.

–) Either F_n or G_n irreducible $\Longrightarrow$ Thue equations.

–) More than one possible system.

–) The solutions also give the torsion points.

Rational Torsion: Order 3

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists \; P \in E(\mathbf{Q})$ *of order* 3 *iff*

Rational Torsion: Order 3

Theorem

Given $E: \ Y^2 = X^3 + AX + B$, $\exists\ P \in E(\mathbf{Q})$ *of order* 3 *iff*

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6, \quad n \neq -9m^3.$$

Rational Torsion: Order 3

Theorem

Given $E: \; Y^2 = X^3 + AX + B$*,* $\exists\ P \in E(\mathbf{Q})$ *of order* 3 *iff*

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6, \quad n \neq -9m^3.$$

Even more, $P = (3m^2, \pm(9m^3 + n))$*.*

Rational Torsion: Order 3

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists \; P \in E(\mathbf{Q})$ *of order* 3 *iff*

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6, \quad n \neq -9m^3.$$

Even more, $P = (3m^2, \pm(9m^3 + n))$.

$$\Psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

Rational Torsion: Order 3

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists \; P \in E(\mathbf{Q})$ *of order* 3 *iff*

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6, \quad n \neq -9m^3.$$

Even more, $P = (3m^2, \pm(9m^3 + n))$.

$$\Psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

$$\frac{A}{x^2} = \frac{3(t+1)}{t-3}, \quad \frac{B}{x^3} = \frac{-t^2 + 6t + 3}{(t-3)^2}.$$

Rational Torsion: Order 5 (I)

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order 5 iff*

Rational Torsion: Order 5 (I)

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order 5 iff*

$$\begin{aligned}
A &= -x^2 - xv - v^2 + (x - v)s, \\
B &= -\frac{1}{4}(x + v)(-3x^2 + 2xv - 3v^2 + 2(x - v)s), \\
s^2 &= (2x + v)(x + 2v), \\
r^2 &= 3x + 2s + 3v.
\end{aligned}$$

Rational Torsion: Order 5 (I)

Theorem

Given $E: \ Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order 5 iff*

$$\begin{aligned} A &= -x^2 - xv - v^2 + (x-v)s, \\ B &= -\frac{1}{4}(x+v)(-3x^2 + 2xv - 3v^2 + 2(x-v)s), \\ s^2 &= (2x+v)(x+2v), \\ r^2 &= 3x + 2s + 3v. \end{aligned}$$

Even more, $P = (x, (x-v)r/2)$.

Rational Torsion: Order 5 (I)

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order 5 iff*

$$\begin{aligned} A &= -x^2 - xv - v^2 + (x - v)s, \\ B &= -\frac{1}{4}(x + v)(-3x^2 + 2xv - 3v^2 + 2(x - v)s), \\ s^2 &= (2x + v)(x + 2v), \\ r^2 &= 3x + 2s + 3v. \end{aligned}$$

Even more, $P = (x, (x - v)r/2)$.

$$\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = v, \quad \frac{v^4 - 2Av^2 - 8Bv + A^2}{4(v^3 + Av + B)} = x.$$

Rational Torsion: Order 5 (II)

Tate normal form $n = 5$: $Y^2 - \alpha XY - \alpha Y = X^3 - \alpha X^2$

Rational Torsion: Order 5 (II)

Tate normal form $n = 5$: $Y^2 - \alpha XY - \alpha Y = X^3 - \alpha X^2$

$$A(\alpha) = -27 - 324\alpha - 378\alpha^2 + 324\alpha^3 - 27\alpha^4,$$
$$B(\alpha) = 54 + 972\alpha + 4050\alpha^2 + 4050\alpha^4 - 972\alpha^5 + 54\alpha^6.$$

Rational Torsion: Order 5 (II)

Tate normal form $n = 5$: $Y^2 - \alpha XY - \alpha Y = X^3 - \alpha X^2$

$$A(\alpha) = -27 - 324\alpha - 378\alpha^2 + 324\alpha^3 - 27\alpha^4,$$
$$B(\alpha) = 54 + 972\alpha + 4050\alpha^2 + 4050\alpha^4 - 972\alpha^5 + 54\alpha^6.$$

$A(x, v, s) = u^4 A(\alpha)$, $B(x, v, s) = u^6 B(\alpha)$, $s^2 = (2x + v)(x + 2v)$.

$$\begin{array}{rcl} x & = & 3u^2(\alpha^2 - 6\alpha + 1), \\ v & = & 3u^2(\alpha^2 + 6\alpha + 1), \\ s & = & -9u^2(\alpha^2 - 1). \end{array}$$

Rational Torsion: Order 5 (III)

$$\alpha = p/q, \;\; u = u_1/u_2.$$

Rational Torsion: Order 5 (III)

$$\alpha = p/q, \;\; u = u_1/u_2.$$

$$x = x(P) \in \mathbf{Z} \quad \Rightarrow \quad q \mid u_1.$$

Rational Torsion: Order 5 (III)

$$\alpha = p/q, \;\; u = u_1/u_2.$$

$$x = x(P) \in \mathbf{Z} \quad \Rightarrow \quad q \mid u_1.$$

$$x, v, s \in \mathbf{Z} \quad \Rightarrow \quad u_2^2 \mid 6(p^2 + q^2), \;\; u_2^2 \mid 9(p^2 - q^2)$$

Rational Torsion: Order 5 (III)

$$\alpha = p/q, \ u = u_1/u_2.$$

$$\begin{aligned} x = x(P) \in \mathbf{Z} &\quad\Rightarrow\quad q \mid u_1. \\ x, v, s \in \mathbf{Z} &\quad\Rightarrow\quad u_2^2 \mid 6(p^2+q^2), \ u_2^2 \mid 9(p^2-q^2) \\ &\quad\Rightarrow\quad u_2 = 1. \end{aligned}$$

Thue Equations: Order 5

Theorem

Given $E: \ Y^2 = X^3 + AX + B$*,* $\exists P \in E(\mathbf{Q})$ *of order* 5 *iff*

Thue Equations: Order 5

Theorem

Given $E: \; Y^2 = X^3 + AX + B, \exists P \in E(\mathbf{Q})$ *of order* 5 *iff*

$$A = -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4),$$

$$B = 54(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4),$$

Thue Equations: Order 5

Theorem

Given $E: \;\; Y^2 = X^3 + AX + B, \exists P \in E(\mathbf{Q})$ *of order* 5 *iff*

$$A = -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4),$$

$$B = 54(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4),$$

with $p, q \in \mathbf{Z}$, $\gcd(p, q) = 1, \; pq \neq 0$.

Thue Equations: Order 5

Theorem

Given $E: \;\; Y^2 = X^3 + AX + B, \exists P \in E(\mathbf{Q})$ *of order* 5 *iff*

$$A = -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4),$$
$$B = 54(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4),$$

with $p, q \in \mathbf{Z}$, $\gcd(p, q) = 1, \; pq \neq 0$.

Even more,

$$\begin{aligned} P &= (3(p^2 - 6pq + q^2), 108p^2q), \\ 2P &= (3(p^2 + 6pq + q^2), 108pq^2), \\ 3P &= (3(p^2 + 6pq + q^2), -108pq^2), \\ 4P &= (3(p^2 - 6pq + q^2), -108p^2q). \end{aligned}$$

Thue Equations: Order 7

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order 7 iff*

Thue Equations: Order 7

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 7 *iff*

$$\begin{aligned}
A &= -27k^4(p^2 - pq + q^2)(q^6 + 5q^5p - 10q^4p^2 - 15q^3p^3 \\
&\quad +30q^2p^4 - 11qp^5 + p^6), \\
B &= 54k^6(p^{12} - 18p^{11}q + 117p^{10}q^2 - 354p^9q^3 + 570p^8q^4 \\
&\quad -486p^7q^5 + 273p^6q^6 - 222p^5q^7 + 174p^4q^8 - 46p^3q^9 \\
&\quad -15p^2q^{10} + 6pq^{11} + q^{12}),
\end{aligned}$$

Thue Equations: Order 7

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 7 *iff*

$$\begin{aligned} A &= -27k^4(p^2 - pq + q^2)(q^6 + 5q^5p - 10q^4p^2 - 15q^3p^3 \\ &\quad +30q^2p^4 - 11qp^5 + p^6), \\ B &= 54k^6(p^{12} - 18p^{11}q + 117p^{10}q^2 - 354p^9q^3 + 570p^8q^4 \\ &\quad -486p^7q^5 + 273p^6q^6 - 222p^5q^7 + 174p^4q^8 - 46p^3q^9 \\ &\quad -15p^2q^{10} + 6pq^{11} + q^{12}), \end{aligned}$$

with $p, q \in \mathbf{Z}$, $\gcd(p,q) = 1$, $pq \neq 0$, $p \neq q$ *y* $k = 1, 1/3$.

Thue Equations: Order 9

Theorem

Given $E: \ Y^2 = X^3 + AX + B, \exists P \in E(\mathbf{Q})$ *of order* 9 *iff*

Thue Equations: Order 9

Theorem

Given $E: \; Y^2 = X^3 + AX + B, \exists P \in E(\mathbf{Q})$ *of order* 9 *iff*

$$\begin{aligned}
A &= -27k^4(q^3 - 3p^2q + p^3)(q^9 - 9q^7p^2 + 27q^6p^3 - 45q^5p^4 \\
&\qquad +54q^4p^5 - 48q^3p^6 + 27p^7q^2 - 9p^8q + p^9), \\
B &= 54k^6(p^{18} - 18p^{17}q + 135p^{16}q^2 - 570p^{15}q^3 + 1557p^{14}q^4 \\
&\qquad -2970p^{13}q^5 + 4128p^{12}q^6 - 4230p^{11}q^7 + 3240p^{10}q^8 \\
&\qquad -2032p^9q^9 + 1359p^8q^{10} - 1080p^7q^{11} + 735p^6q^{12} \\
&\qquad -306p^5q^{13} + 27p^4q^{14} + 42p^3q^{15} - 18p^2q^{16} + q^{18}),
\end{aligned}$$

Thue Equations: Order 9

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 9 *iff*

$$\begin{aligned}
A &= -27k^4(q^3 - 3p^2q + p^3)(q^9 - 9q^7p^2 + 27q^6p^3 - 45q^5p^4 \\
&\qquad +54q^4p^5 - 48q^3p^6 + 27p^7q^2 - 9p^8q + p^9), \\
B &= 54k^6(p^{18} - 18p^{17}q + 135p^{16}q^2 - 570p^{15}q^3 + 1557p^{14}q^4 \\
&\qquad -2970p^{13}q^5 + 4128p^{12}q^6 - 4230p^{11}q^7 + 3240p^{10}q^8 \\
&\qquad -2032p^9q^9 + 1359p^8q^{10} - 1080p^7q^{11} + 735p^6q^{12} \\
&\qquad -306p^5q^{13} + 27p^4q^{14} + 42p^3q^{15} - 18p^2q^{16} + q^{18}),
\end{aligned}$$

with $p, q \in \mathbf{Z}$, $\gcd(p,q) = 1$, $pq \neq 0$, $p \neq q$ *y* $k = 1, 1/3$.

Thue Equations: Order 9

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 9 *iff*

$$\begin{aligned}
A &= -27k^4(q^3 - 3p^2q + p^3)(q^9 - 9q^7p^2 + 27q^6p^3 - 45q^5p^4 \\
&\qquad +54q^4p^5 - 48q^3p^6 + 27p^7q^2 - 9p^8q + p^9), \\
B &= 54k^6(p^{18} - 18p^{17}q + 135p^{16}q^2 - 570p^{15}q^3 + 1557p^{14}q^4 \\
&\qquad -2970p^{13}q^5 + 4128p^{12}q^6 - 4230p^{11}q^7 + 3240p^{10}q^8 \\
&\qquad -2032p^9q^9 + 1359p^8q^{10} - 1080p^7q^{11} + 735p^6q^{12} \\
&\qquad -306p^5q^{13} + 27p^4q^{14} + 42p^3q^{15} - 18p^2q^{16} + q^{18}),
\end{aligned}$$

with $p, q \in \mathbf{Z}$, $\gcd(p, q) = 1$, $pq \neq 0$, $p \neq q$ *y* $k = 1, 1/3$.

Even more, $P, \ldots, 8P$ *depending of* p *and* q.

Diophantine Equations: Order 4

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 4 *iff*

Diophantine Equations: Order 4

Theorem

Given $E: \; Y^2 = X^3 + AX + B, \exists P \in E(\mathbf{Q})$ *of order* 4 *iff*

$$\begin{array}{rcl} A & = & -3p^2 + 6pq^2 - 2q^4 \\ B & = & (2p - q^2)(p^2 + 2pq^2 - q^4) \end{array}$$

Diophantine Equations: Order 4

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 4 *iff*

$$\begin{array}{rcl} A & = & -3p^2 + 6pq^2 - 2q^4 \\ B & = & (2p - q^2)(p^2 + 2pq^2 - q^4) \end{array}$$

with $p, q \in \mathbf{Z}$, $\gcd(p, q) = 1$, $q \neq 0$, $q^2 \neq 3r$, $5q^2 \neq 12p$.

Diophantine Equations: Order 4

Theorem

Given $E: \;\; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 4 *iff*

$$\begin{aligned} A &= -3p^2 + 6pq^2 - 2q^4 \\ B &= (2p - q^2)(p^2 + 2pq^2 - q^4) \end{aligned}$$

with $p, q \in \mathbf{Z}$, $\gcd(p, q) = 1$, $q \neq 0$, $q^2 \neq 3r$, $5q^2 \neq 12p$.

Even more, the points of order four are $(p, \pm q(3p - q^2))$.

Thue Equations: Order 8

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 8 *iff*

Thue Equations: Order 8

Theorem

Given $E: \;\; Y^2 = X^3 + AX + B,\, \exists P \in E(\mathbf{Q})$ *of order* 8 *iff*

$$\begin{aligned}
A &= -27k^4(q^8 - 16pq^7 + 96p^2q^6 + 480p^4q^4 - 288p^3q^5 \\
&\qquad +16p^8 - 64p^7q + 224p^6q^2 - 448p^5q^3), \\
B &= 54k^6(8p^4 - 16p^3q + 16p^2q^2 - 8pq^3 + q^4)(8p^8 - 32p^7q \\
&\qquad -80p^6q^2 + 352p^5q^3 - 456p^4q^4 + 288p^3q^5 \\
&\qquad -96p^2q^6 + 16pq^7 - q^8)
\end{aligned}$$

Thue Equations: Order 8

Theorem

Given $E: \ Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 8 *iff*

$$\begin{aligned} A &= -27k^4(q^8 - 16pq^7 + 96p^2q^6 + 480p^4q^4 - 288p^3q^5 \\ &\qquad +16p^8 - 64p^7q + 224p^6q^2 - 448p^5q^3), \\ B &= 54k^6(8p^4 - 16p^3q + 16p^2q^2 - 8pq^3 + q^4)(8p^8 - 32p^7q \\ &\qquad -80p^6q^2 + 352p^5q^3 - 456p^4q^4 + 288p^3q^5 \\ &\qquad -96p^2q^6 + 16pq^7 - q^8) \end{aligned}$$

with $p, q \in \mathbf{Z} \setminus \{0\}$, $\gcd(p, q) = 1$, $2p \neq q$, $p \neq q$ *y* $k = 1, 1/2$.

Thue Equations: Order 8

Theorem

Given $E: \; Y^2 = X^3 + AX + B$, $\exists P \in E(\mathbf{Q})$ *of order* 8 *iff*

$$\begin{aligned} A &= -27k^4(q^8 - 16pq^7 + 96p^2q^6 + 480p^4q^4 - 288p^3q^5 \\ &\quad +16p^8 - 64p^7q + 224p^6q^2 - 448p^5q^3), \\ B &= 54k^6(8p^4 - 16p^3q + 16p^2q^2 - 8pq^3 + q^4)(8p^8 - 32p^7q \\ &\quad -80p^6q^2 + 352p^5q^3 - 456p^4q^4 + 288p^3q^5 \\ &\quad -96p^2q^6 + 16pq^7 - q^8) \end{aligned}$$

with $p, q \in \mathbf{Z} \setminus \{0\}$, $\gcd(p, q) = 1$, $2p \neq q$, $p \neq q$ *y* $k = 1, 1/2$.

Even more, $P, \dots, 7P$ *depending of* p *and* q*.*

Example

Given $E: \ Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

Example

Given $E: \; Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

$$\begin{aligned} -43 &= -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 &= 54(p^{12} - 18p^{11}q + \cdots + q^{12}). \end{aligned}$$

Example

Given $E: \; Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

$$\begin{aligned} -43 &= -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 &= 54(p^{12} - 18p^{11}q + \cdots + q^{12}). \end{aligned}$$

No integral solution.

Example

Given $E: \ Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

$$\begin{aligned} -43 &= -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 &= 54(p^{12} - 18p^{11}q + \cdots + q^{12}). \end{aligned}$$

No integral solution.

$$\begin{aligned} -43 \cdot 3^4 &= -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 \cdot 3^6 &= 54(p^{12} - 18p^{11}q + \cdots + q^{12}), \end{aligned}$$

Example

Given $E: \; Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

$$\begin{array}{rcl} -43 & = & -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 & = & 54(p^{12} - 18p^{11}q + \cdots + q^{12}). \end{array}$$

No integral solution.

$$\begin{array}{rcl} -43 \cdot 3^4 & = & -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 \cdot 3^6 & = & 54(p^{12} - 18p^{11}q + \cdots + q^{12}), \end{array}$$

has a solution $\{p = 2, q = 1\}$.

Example

Given $E: \; Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

$$\begin{array}{rcl} -43 & = & -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 & = & 54(p^{12} - 18p^{11}q + \cdots + q^{12}). \end{array}$$

No integral solution.

$$\begin{array}{rcl} -43 \cdot 3^4 & = & -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 \cdot 3^6 & = & 54(p^{12} - 18p^{11}q + \cdots + q^{12}), \end{array}$$

has a solution $\{p = 2, q = 1\}$.

$E': \; Y^2 = X^3 - 43 \cdot 3^4 X + 166 \cdot 3^6 \; \rightarrow \; \mathrm{Tor}(E'(\mathbf{Q})) = \langle (27, 216) \rangle.$

Example

Given $E: \; Y^2 = X^3 - 43X + 166$, we look for $P \in E(\mathbf{Q})$ of order 7.

$$\begin{array}{rcl} -43 & = & -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 & = & 54(p^{12} - 18p^{11}q + \cdots + q^{12}). \end{array}$$

No integral solution.

$$\begin{array}{rcl} -43 \cdot 3^4 & = & -27(p^2 - pq + q^2)(q^6 + \cdots + p^6), \\ 166 \cdot 3^6 & = & 54(p^{12} - 18p^{11}q + \cdots + q^{12}), \end{array}$$

has a solution $\{p = 2, q = 1\}$.

$E': \; Y^2 = X^3 - 43 \cdot 3^4 X + 166 \cdot 3^6 \;\rightarrow\; \mathrm{Tor}(E'(\mathbf{Q})) = \langle (27, 216) \rangle$.

$$\mathrm{Tor}(E(\mathbf{Q})) = \langle (3, 8) \rangle \text{ of order } 7.$$

Next in line...

- Galois field of $X^3 + AX + B$.

Next in line...

- Galois field of $X^3 + AX + B$.
- Density of trivial torsion.

Next in line...

- Galois field of $X^3 + AX + B$.
- Density of trivial torsion.
- Accuracy of the reduction.

Next in line...

- Galois field of $X^3 + AX + B$.
- Density of trivial torsion.
- Accuracy of the reduction.
- Number fields.