Ranks of Elliptic Curves

Keith Conrad

April 15, 2018

Elliptic Curve Addition and the Rank

Generalized integers

In number theory, many basic ideas (primes factorization, modular arithmetic, *etc.*) can be applied in settings beyond $\mathbf{Z}$. The first example of this goes back to Gauss: the "complex integers" or Gaussian integers

$$\mathbf{Z}[i] = \{x + yi : x, y \in \mathbf{Z}\}.$$

This is closed under addition and multiplication. Other examples, using real numbers, are

$$\begin{aligned}
\mathbf{Z}[\sqrt{2}] &= \{x + y\sqrt{2} : x, y \in \mathbf{Z}\} \\
\mathbf{Z}[\sqrt[3]{2}] &= \{x + y\sqrt[3]{2} + z\sqrt[3]{4} : x, y, z \in \mathbf{Z}\} \\
\mathbf{Z}[\sqrt[4]{2}] &= \{x + y\sqrt[4]{2} + z\sqrt[4]{4} + w\sqrt[4]{8} : x, y, z, w \in \mathbf{Z}\} \\
&\vdots \\
\mathbf{Z}[\sqrt[d]{2}] &= \{x_0 + x_1\sqrt[d]{2} + x_2\sqrt[d]{2}^2 + \cdots + x_{d-1}\sqrt[d]{2}^{d-1} : x_i \in \mathbf{Z}\}.
\end{aligned}$$

Each of these is closed under addition and multiplication.

Units among generalized integers

Invertible elements under multiplication are called **units**. Products of units are units: $uu' = 1$ and $vv' = 1 \Rightarrow (uv)(u'v') = 1$.

In $\mathbf{Z}$, the units are ± 1: boring!

In $\mathbf{Z}[\sqrt{2}]$, $x + y\sqrt{2}$ is a unit when $x^2 - 2y^2 = \pm 1$ and all units are

$$\pm(1 + \sqrt{2})^n, \ n \in \mathbf{Z}.$$

In $\mathbf{Z}[\sqrt[3]{2}]$, the units are

$$\pm(1 - \sqrt[3]{2})^n, \ n \in \mathbf{Z}.$$

In $\mathbf{Z}[\sqrt[4]{2}]$, the units are

$$\pm(1 + \sqrt{2})^n(1 + \sqrt[4]{2})^{n'}, \ n, n' \in \mathbf{Z},$$

where $1 + \sqrt{2}$ and $1 + \sqrt[4]{2}$ are *multiplicatively independent*: if $(1 + \sqrt{2})^n(1 + \sqrt[4]{2})^{n'} = 1$ then $n = n' = 0$.

We say $\mathbf{Z}$ has unit rank 0, $\mathbf{Z}[\sqrt{2}]$ and $\mathbf{Z}[\sqrt[3]{2}]$ have unit rank 1, and $\mathbf{Z}[\sqrt[4]{2}]$ has unit rank 2.

Dirichlet's unit theorem (special case)

Theorem (Dirichlet, 1846): *For $d \geq 1$, the units in $\mathbf{Z}[\sqrt[d]{2}]$ are finitely generated under multiplication: there is a finite list of units $\varepsilon_1, \ldots, \varepsilon_r$ in $\mathbf{Z}[\sqrt[d]{2}]$ such that the set of all units in $\mathbf{Z}[\sqrt[d]{2}]$ is*

$$\pm\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}, \ n_i \in \mathbf{Z}.$$

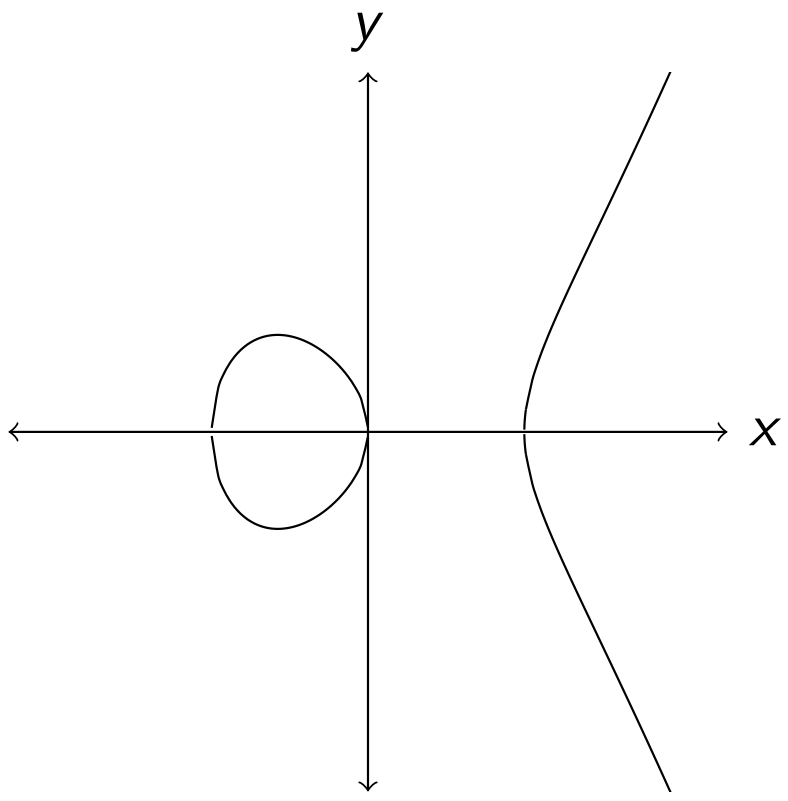
When d is even the least r is $d/2$, and when d is odd the least r is $(d-1)/2$.

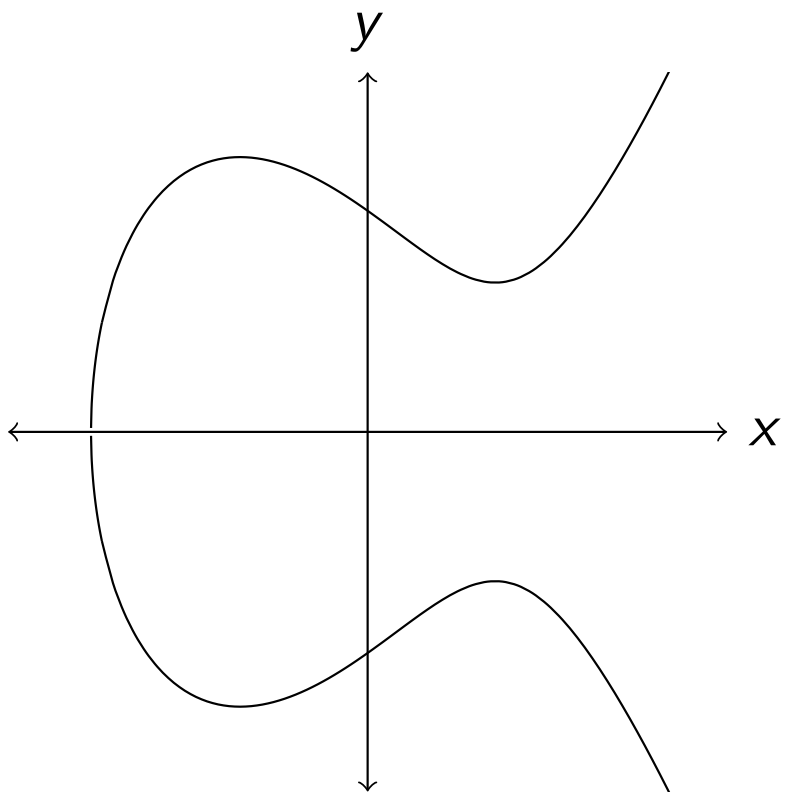
This says units in $\mathbf{Z}[\sqrt[d]{2}]$ for $d = 2$ and 3 are $\pm\varepsilon^n$, for $d = 4$ the units are $\pm\varepsilon_1^{n_1}\varepsilon_2^{n_2}$.

The least r is called the unit rank of $\mathbf{Z}[\sqrt[d]{2}]$, and the theorem gives a simple formula for it. Every positive integer is a unit rank, *e.g.*, r is unit rank of $\mathbf{Z}[\sqrt[2r]{2}]$.

Contrast: units of $\mathbf{Q}$ are nonzero rationals: $\pm p_1^{n_1} \cdots p_k^{n_k}$ where $k \in \{0, 1, 2, \ldots\}$ and $p_i \in \{2, 3, 5, \ldots\}$ are primes. This is *not* finitely generated: $2, 3, 5, 7, \ldots$ are multiplicatively independent.

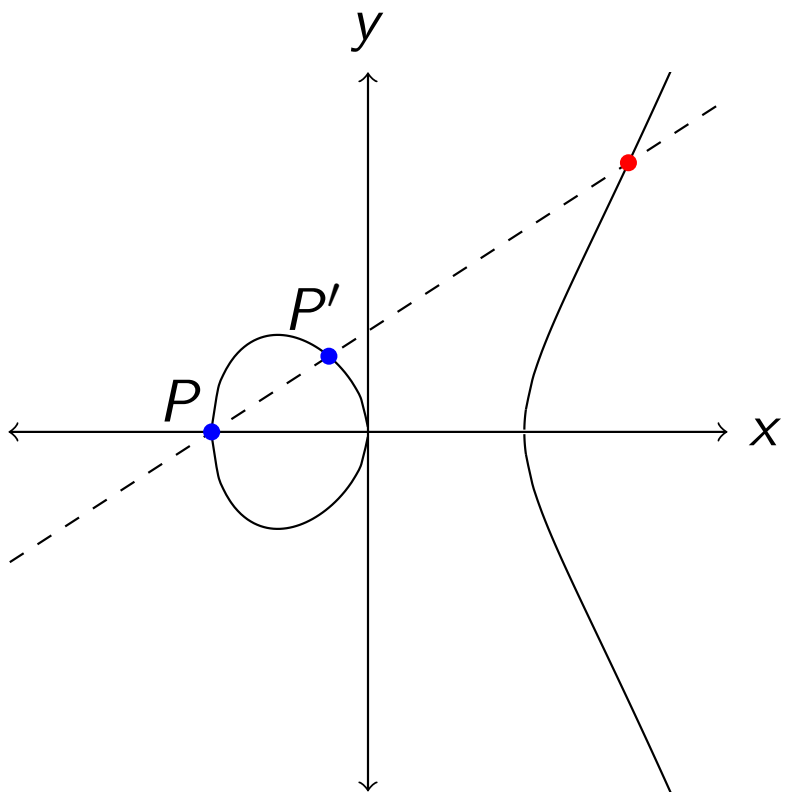
Elliptic curves

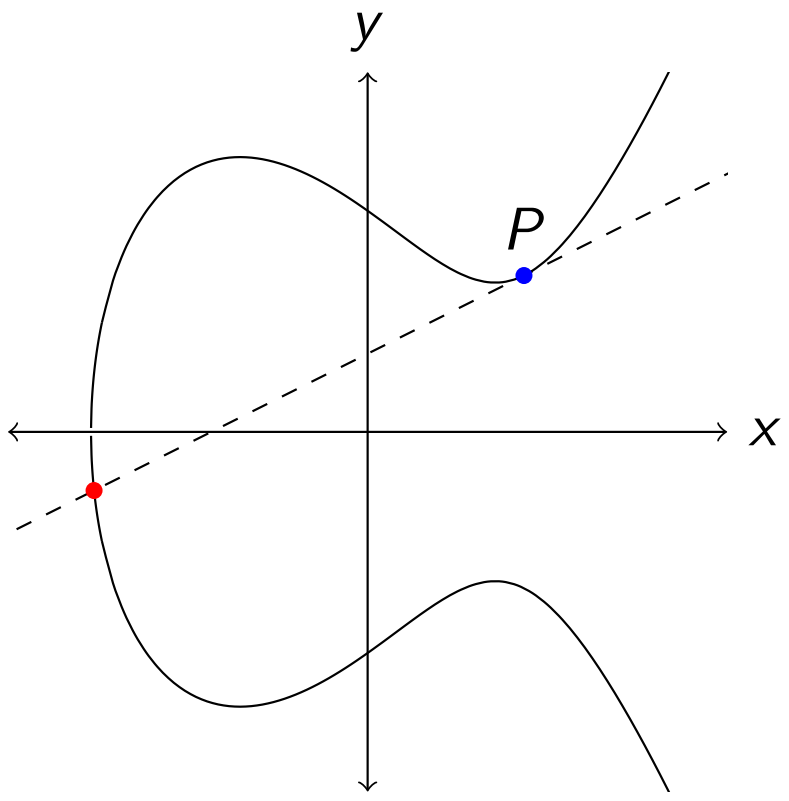




An *elliptic curve*, for our needs, is a smooth curve E of the form $y^2 = x^3 + ax + b$.

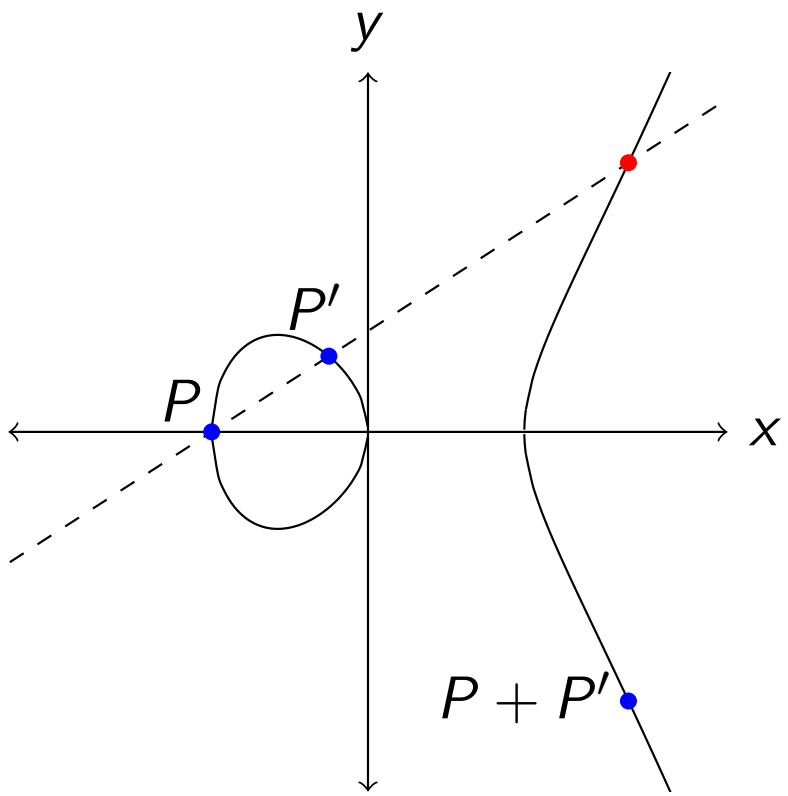
Elliptic curves

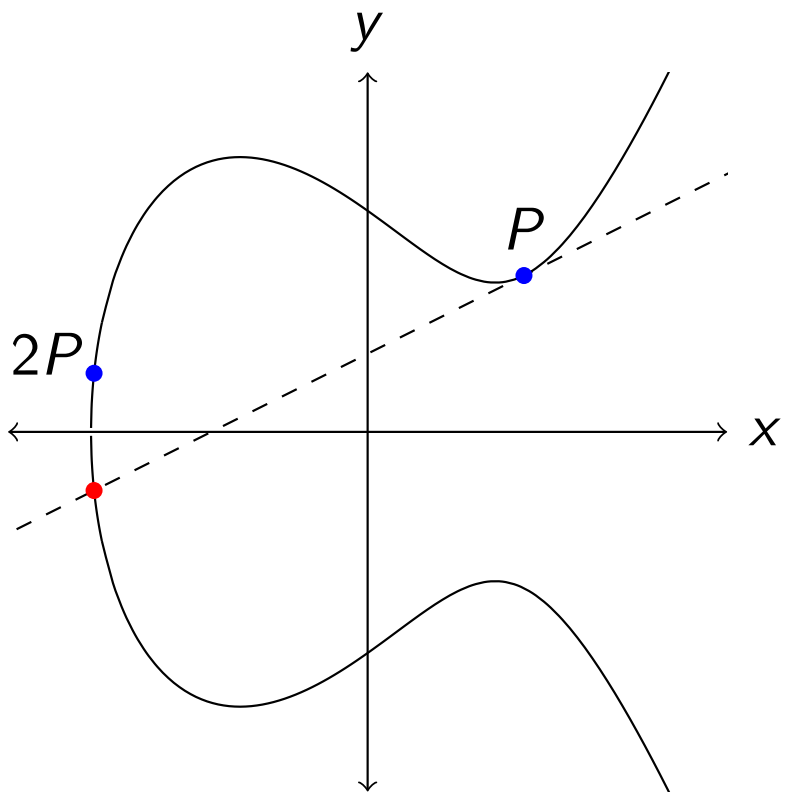




An *elliptic curve*, for our needs, is a smooth curve E of the form $y^2 = x^3 + ax + b$. Since degree is 3, line through points P and P' on E (if $P = P'$, use tangent at P) has a third point on E: when $y = mx + b$, $(mx + b)^2 = x^3 + ax + b$ has sum of roots equal to m^2, so for two known roots r and r', the third root is $m^2 - r - r'$.

Elliptic curves



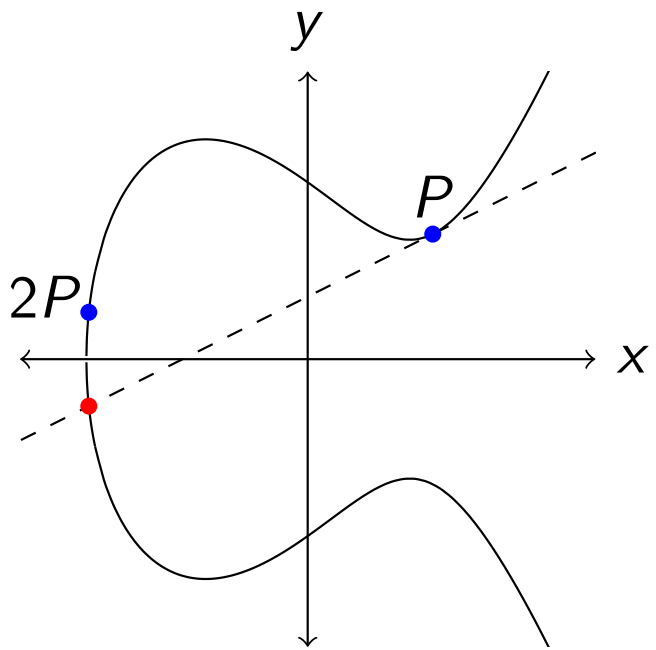


An *elliptic curve*, for our needs, is a smooth curve E of the form $y^2 = x^3 + ax + b$. Since degree is 3, line through points P and P' on E (if $P = P'$, use tangent at P) has a third point on E: when $y = mx + b$, $(mx + b)^2 = x^3 + ax + b$ has sum of roots equal to m^2, so for two known roots r and r', the third root is $m^2 - r - r'$. Set reflection of 3rd point to be $P + P'$: comm. and *associative*.

Elliptic curves over Q

When $E : y^2 = x^3 + ax + b$ has $a, b \in \mathbf{Q}$ and P and P' are in $E(\mathbf{Q})$ then $P + P' \in E(\mathbf{Q})$ because calculations only need $\mathbf{Q}$.

Example. Consider $y^2 = x^3 - 2x + 2$ and $P = (1, 1)$.



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

$$\Rightarrow 2yy' = 3x^2 - 2$$

$$\Rightarrow 2\frac{dy}{dx}\bigg|_{(1,1)} = 1$$

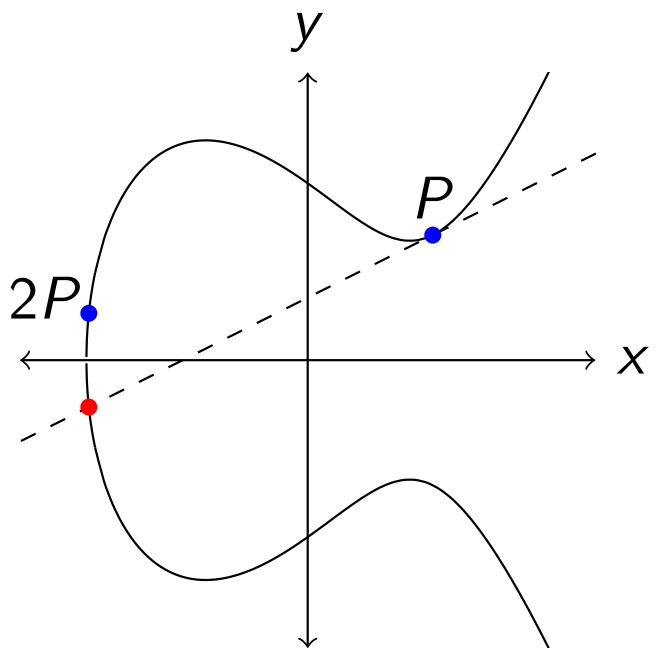
$$\Rightarrow \frac{dy}{dx}\bigg|_{(1,1)} = \frac{1}{2}.$$

Tangent line at P is $y = (1/2)(x - 1) + 1 = (x + 1)/2$.

Elliptic curves over Q

When $E : y^2 = x^3 + ax + b$ has $a, b \in \mathbf{Q}$ and P and P' are in $E(\mathbf{Q})$ then $P + P' \in E(\mathbf{Q})$ because calculations only need $\mathbf{Q}$.

Example. Consider $y^2 = x^3 - 2x + 2$ and $P = (1, 1)$.



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

$$\Rightarrow 2yy' = 3x^2 - 2$$

$$\Rightarrow 2\frac{dy}{dx}\bigg|_{(1,1)} = 1$$

$$\Rightarrow \frac{dy}{dx}\bigg|_{(1,1)} = \frac{1}{2}.$$

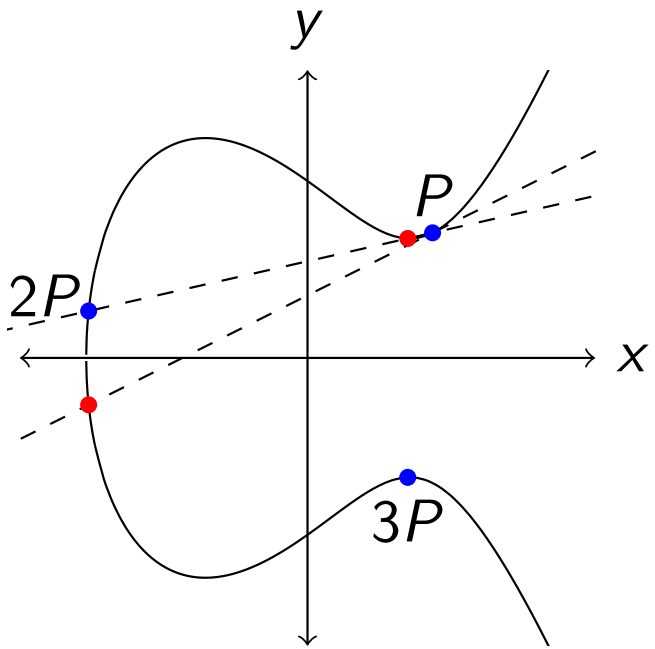
Tangent line at P is $y = (1/2)(x - 1) + 1 = (x + 1)/2$. Solutions of $((x + 1)/2)^2 = x^3 - 2x + 2$ are $x = 1$, 1, and $-7/4$. Then $(-7/4, y) \in E(\mathbf{Q})$ for $y = (-7/4 + 1)/2 = -3/8$, which makes $2P = (-7/4, 3/8)$.

Elliptic curves over Q: finite and infinite order points

Say $P \in E(\mathbf{Q})$ has *infinite order* if $\{P, 2P, 3P, 4P, \ldots\}$ does not repeat, and *finite order* if $\{P, 2P, 3P, 4P, \ldots\}$ cycles.

Example. On $E : y^2 = x^3 - 2x + 2$, let $P = (1, 1)$. Then P has infinite order: already saw $2P = (-7/4, 3/8)$, and can show

$$3P = (97/121, -1271/1331),\ 4P = (13729/144, -1608463/1728).$$



Nagell–Lutz theorem (1930s) says if $(x, y) \in E(\mathbf{Q})$ has finite order then $x, y \in \mathbf{Z}$: $2P = (-7/4, 3/8)$ has infinite order, so P does too!

Elliptic curves over Q: Mordell(-Weil) theorem

If E has rational coefficients then $E(\mathbf{Q})$ has finitely many points of finite order (Nagell–Lutz). Poincaré (1901) suggested, and Mordell (1922) proved, that $E(\mathbf{Q})$ is *finitely generated*.

Geometric meaning: there is a finite set of points in $E(\mathbf{Q})$ such that the rest of $E(\mathbf{Q})$ is obtained from it by repeated intersections of secant and tangent lines with E.

Algebraic meaning: there is a finite list $P_1, \ldots, P_r$ in $E(\mathbf{Q})$, each with infinite order, such that

$$E(\mathbf{Q}) = \{T_j + n_1 P_1 + \cdots + n_r P_r : n_i \in \mathbf{Z}\}$$

where T_j has finite order (finitely many of these) and $P_1, \ldots, P_r$ are independent:

$$m_1 P_1 + \cdots + m_r P_r = n_1 P_1 + \cdots + n_r P_r \Longrightarrow m_i = n_i \text{ for all } i.$$

Compare to units in $\mathbf{Z}[\sqrt[4]{2}]$: $\pm(1+\sqrt{2})^n(1+\sqrt[4]{2})^{n'}$ for $n, n' \in \mathbf{Z}$.

Examples of minimal generating sets for $E(\mathbf{Q})$

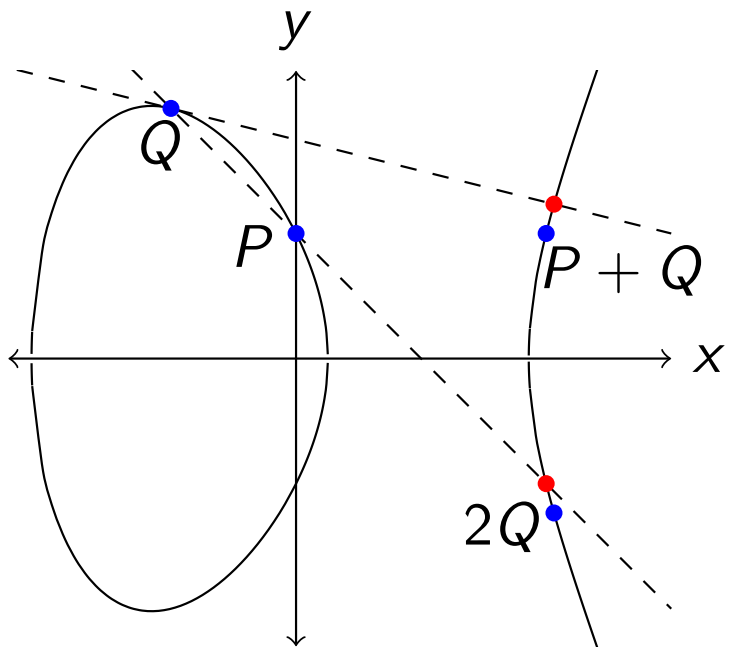
$E : y^2 = x^3 + 1$ has rank 0: $E(\mathbf{Q}) = \{n(2,3) : n = 0, 1, \ldots, 5\}$.

$E : y^2 = x^3 - 2x + 2$ has rank 1: $E(\mathbf{Q}) = \{n(1,1) : n \in \mathbf{Z}\}$.

$E : y^2 = x^3 - 4x + 1$ has rank 2:

$$E(\mathbf{Q}) = \{n\underbrace{(0,1)}_{P} + n'\underbrace{(-1,2)}_{Q} : n, n' \in \mathbf{Z}\}.$$

$$P + Q = (2,1), \quad 2P = (4,7), \quad 2Q = (33/16, -79/64).$$



Finding the Rank

How to find the rank of an elliptic curve over Q?

Unlike Dirichlet's theorem about the rank of units, there is **no known simple formula** for the rank of $E(\mathbf{Q})$ from E's coefficients.

In the 1960s, a rank "formula" was conjectured using behavior of

$$N_p(E) = |\{(x, y) \bmod p : y^2 \equiv x^3 + ax + b \bmod p\}| + 1.$$

Example. $E : y^2 = x^3 - 4x + 1$.

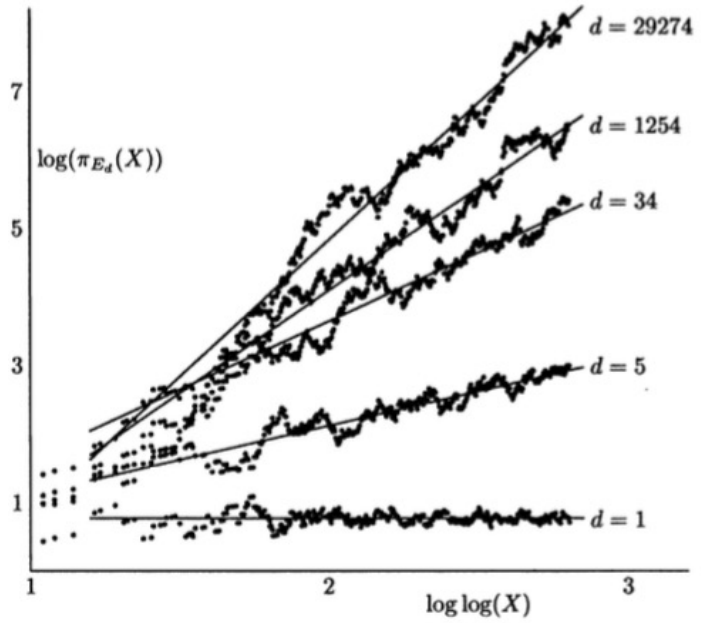
p	2	3	5	7	11	13	17	19	23	29	31	37
$N_p(E)$	3	8	10	13	16	19	26	26	31	23	31	45

Conjecture. *For each* E,

$$\prod_{p \le X} \frac{N_p(E)}{p} \overset{?}{\sim} C(\log X)^{\mathrm{rk}(E(\mathbf{Q}))}.$$

Original data used $X \le 1000$.

Graphs are for $y^2 = x^3 - d^2x$, taken from Rubin & Silverberg *BAMS*, 2002.



How to find the rank of an elliptic curve over Q?

Due to Tate's influence, conjecture about $\prod_{p \le X} N_p(E)/p$ turned into a conjecture about how much $L(E,s)$ vanishes at $s=1$, where

$$L(E,s) = \prod_p \frac{1}{1 - a_p(E)/p^s + p/p^{2s}} = \sum_{n \ge 1} \frac{a_n(E)}{n^s}$$

for $\mathrm{Re}(s) > \frac{3}{2}$, with $a_p(E) = p + 1 - N_p(E)$. Formally,

$$\begin{aligned} L(E,1) \quad \text{“=”} \quad & \prod_p \frac{1}{1 - (p+1-N_p(E))/p + 1/p} \\ = \quad & \prod_p \frac{1}{N_p(E)/p} \;=\; \prod_p \frac{p}{N_p(E)}, \end{aligned}$$

so believing $\prod_{p \le X} N_p(E)/p \sim C(\log X)^{\mathrm{rank}(E(\mathbf{Q}))}$ suggests that

$$\mathrm{rank}(E(\mathbf{Q})) \stackrel{?}{=} \mathrm{ord}_{s=1}(L(E,s)) \quad \text{(BSD conjecture)}$$

How to find the rank of an elliptic curve over Q?

Why does $E : y^2 = x^3 - 4x + 1$ have rank 2? Upper/lower bounds.

Lower: show $P = (0, 1)$ and $Q = (-1, 2)$ are of infinite order and independent, so $E(\mathbf{Q})$ has rank *at least* 2.

Upper: use more advanced techniques (*e.g.*, Galois cohomology) to show the rank is *at most* 2.

Prove points independent by ideas from linear algebra.

Toy example. Show $1 + \sqrt{2}$ and $1 + \sqrt[4]{2}$ are mult. independent:

$$(1 + \sqrt{2})^n (1 + \sqrt[4]{2})^{n'} = 1 \Rightarrow n \log(1 + \sqrt{2}) + n' \log(1 + \sqrt[4]{2}) = 0.$$

How to find the rank of an elliptic curve over Q?

Why does $E : y^2 = x^3 - 4x + 1$ have rank 2? Upper/lower bounds.

Lower: show $P = (0, 1)$ and $Q = (-1, 2)$ are of infinite order and independent, so $E(\mathbf{Q})$ has rank *at least* 2.

Upper: use more advanced techniques (*e.g.*, Galois cohomology) to show the rank is *at most* 2.

Prove points independent by ideas from linear algebra.

Toy example. Show $1 + \sqrt{2}$ and $1 + \sqrt[4]{2}$ are mult. independent:

$$(1 + \sqrt{2})^n (1 + \sqrt[4]{2})^{n'} = 1 \Rightarrow n \log(1 + \sqrt{2}) + n' \log(1 + \sqrt[4]{2}) = 0.$$

Replacing $\sqrt[4]{2}$ with $-\sqrt[4]{2}$ sends $\sqrt{2} = \sqrt[4]{2}^2$ to $(-\sqrt[4]{2})^2 = \sqrt{2}$, so

$$\begin{aligned} (1 + \sqrt{2})^n (1 + \sqrt[4]{2})^{n'} = 1 \quad &\Rightarrow \quad (1 + \sqrt{2})^n (1 - \sqrt[4]{2})^{n'} = 1 \\ &\Rightarrow \quad (1 + \sqrt{2})^n |1 - \sqrt[4]{2}|^{n'} = 1 \\ &\Rightarrow \quad n \log(1 + \sqrt{2}) + n' \log |1 - \sqrt[4]{2}| = 0. \end{aligned}$$

How to find the rank of an elliptic curve over Q?

The relations

$$\begin{aligned} n\log(1+\sqrt{2}) + n'\log(1+\sqrt[4]{2}) &= 0 \\ n\log(1+\sqrt{2}) + n'\log|1-\sqrt[4]{2}| &= 0 \end{aligned}$$

can be written as

$$\begin{pmatrix} \log(1+\sqrt{2}) & \log(1+\sqrt[4]{2}) \\ \log(1+\sqrt{2}) & \log|1-\sqrt[4]{2}| \end{pmatrix} \begin{pmatrix} n \\ n' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and the matrix has determinant $-2.158\ldots \neq 0$, so $n = n' = 0$.

Similar ideas prove independence of points on $E(\mathbf{Q})$, replacing logarithms of units with a *height pairing* on points to linearize the problem.

This is how Elkies showed in 2006 that an E with coefficients of over 80 digits has $\text{rank}(E(\mathbf{Q})) \geq 28$: find 28 points and check the 28×28 height pairing matrix has nonzero determinant. (In 2016, Klagsbrun, Sherman, and Weigandt proved this example would have rank exactly 28 if GRH is true.)

How to find high rank elliptic curves over Q?

Let $E_T : y^2 = x^3 + A(T)x + B(T)$ be elliptic curve over $\mathbf{Q}(T)$. Then $E(\mathbf{Q}(T))$ is finitely generated (Lang–Néron) and for all but finitely many $t \in \mathbf{Q}$, $E_t : y^2 = x^3 + A(t)x + B(t)$ is elliptic curve over $\mathbf{Q}$ and

$$\mathrm{rank}(E_t(\mathbf{Q})) \geq \mathrm{rank}(E_T(\mathbf{Q}(T))).$$

Ex: On $E_T : y^2 = x^3 - T^2x + 1$ let $P_T = (0, 1)$, $Q_T = (-1, T)$.

$$\begin{aligned} P_T + Q_T &= (T^2 - 2T + 2, T^3 - 3T^2 + 4T - 3), \\ 2P_T &= \left(\frac{T^4}{4}, \frac{T^6 - 8}{8}\right), \\ 2Q_T &= \left(\frac{T^4 + 2T^2 + 9}{4T^2}, \frac{T^6 - 5T^4 - 9T^2 - 27}{8T^3}\right). \end{aligned}$$

At $T = 2$ get $E_2 : y^2 = x^3 - 4x + 1$ with points $P_2 = (0, 1)$ and $Q_2 = (-1, 2)$ in $E_2(\mathbf{Q})$, and recover earlier sums of these points:

$$P_2 + Q_2 = (2, 1), \quad 2P_2 = (4, 7), \quad 2Q_2 = \left(\frac{33}{16}, -\frac{79}{64}\right).$$

How to find high rank elliptic curves?

Nagao's heuristic: if E is an elliptic curve over $\mathbf{Q}$ then a heuristic formula for the rank of $E(\mathbf{Q})$ is

$$\frac{1}{2} - \frac{1}{X}\sum_{p \leq X} a_p(E)\log p = \frac{1}{2} - \frac{1}{X}\sum_{p \leq X}(p + 1 - N_p(E))\log p$$

for large X. This is motivated by calculations with $L'(E,s)/L(E,s)$ based on BSD (residue at $s = 1$ should equal the rank of $E(\mathbf{Q})$: $f(s) = c(s-1)^r + \cdots \Rightarrow f'(s)/f(s) = r/(s-1) + \cdots$).

If E_T is an elliptic curve over $\mathbf{Q}(T)$ and, for a **particular** $t \in \mathbf{Q}$, Nagao's heuristic suggests

$$\text{rank}(E_t(\mathbf{Q})) > \text{rank}(E_T(\mathbf{Q}(T))),$$

then do an explicit search for more points on $E_t(\mathbf{Q})$ for that particular t and verify independence with height pairing matrix.

Nagao (1990s) used this idea to discover record (at the time) elliptic curves over $\mathbf{Q}$ with rank at least 17, 20, and 21.

The Parity Conjecture

Functional equation and its sign

For each elliptic curve E over $\mathbf{Q}$, there is $N_E \in \mathbf{Z}^+$ such that

$$\Lambda(E,s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

for $\mathrm{Re}(s) > 3/2$ extends to all $s \in \mathbf{C}$ (analytic) and there is a *functional equation*

$$\Lambda(E,s) = w_E\Lambda(E,2-s), \quad w_E = \pm 1.$$

- The piece $N_E^{s/2}(2\pi)^{-s}\Gamma(s)$ is nonvanishing at $s = 1$.
- The sign w_E has a purely algebraic description using representation theory.
- Letting $L(E,s)$ have order of vanishing r at $s = 1$, so

  $$L(E,s) = c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots, \quad c_r \neq 0$$

  we have $c_r = L^{(r)}(E,1)/r! \neq 0$.
- Differentiating the functional equation k times (any k),

  $$\Lambda^{(k)}(E,s) = (-1)^k w_E \Lambda^{(k)}(E,2-s),$$

  Thus $\Lambda^{(r)}(E,1) = (-1)^r w_E \Lambda^{(r)}(E,1) \Rightarrow \boxed{w_E = (-1)^r}$.

Parity conjecture

Since w_E can be computed purely algebraically, the formula

$$\boxed{w_E = (-1)^r = (-1)^{\mathrm{ord}_{s=1}(L(E,s))}}$$

tells us $\mathrm{ord}_{s=1}(L(E,s))$ mod 2, so knowing w_E should also tell us $\mathrm{rank}(E(\mathbf{Q}))$ mod 2. That this works is called the *parity conjecture*.

The parity conjecture is weaker than BSD, but already gives us interesting information: if $w_E = -1$ then $\mathrm{ord}_{s=1}(L(E,s))$ is odd, so we *expect* $\mathrm{rank}(E(\mathbf{Q}))$ is odd and thus positive, so $E(\mathbf{Q})$ is infinite.

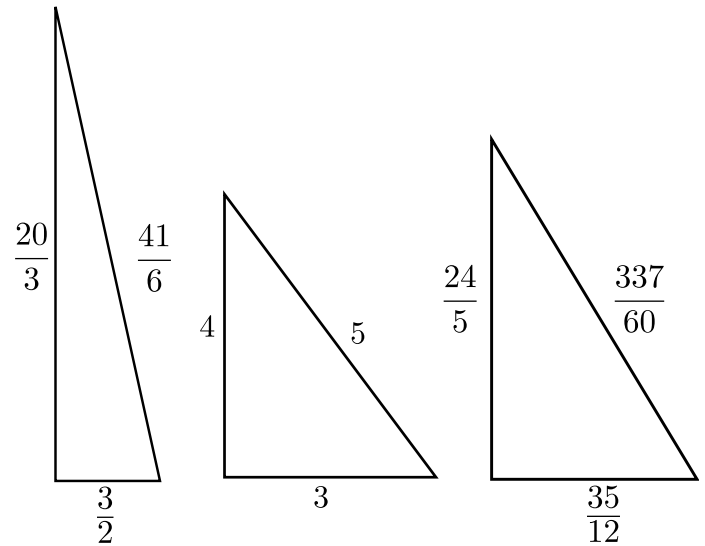
The parity conjecture was proved by Nekovar for elliptic curves over $\mathbf{Q}$, conditional on finiteness of $Ш_{E/\mathbf{Q}}$ (still an open problem).

That the condition $w_E = -1$ should imply $E(\mathbf{Q})$ is infinite will be seen later to have applications to several elementary questions that are not initially about elliptic curves.

Applications of ranks

Application of ranks: congruent number problem

For which n in $\mathbf{Z}^+$ is there a rational right triangle with area n? Below are $n = 5, 6, 7$.



If $a^2 + b^2 = c^2$ with $\frac{1}{2}ab = n$ then $y^2 = x^3 - n^2x$ where

$$x = \frac{nb}{c-a}, \quad y = \frac{2n^2}{c-a} \neq 0$$

and this is a bijection preserving rationality and positivity.

Ex. For area 5, triangle $(a, b, c) = (3/2, 20/3, 41/6)$ corresponds to $(x, y) = (25/4, 75/8)$ with $y^2 = x^3 - 25x$.

Application of ranks: congruent number problem

Let $E_n : y^2 = x^3 - n^2x = x(x+n)(x-n)$. Points (x, y) on $E_n(\mathbf{Q})$ with $y \neq 0$ have infinite order, so one rational right triangle with area n implies *infinitely many* such right triangles.

Ex ($n = 5$). From a triangle to a point, doubling it, and then back,

$$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right) \rightsquigarrow P = \left(\frac{25}{4}, \frac{75}{8}\right),$$

$$2P = \left(\frac{1681}{144}, -\frac{62279}{1728}\right) \rightsquigarrow \left(-\frac{1519}{492}, -\frac{4920}{1519}, -\frac{3344161}{747348}\right).$$

In 1975, Stephens showed for squarefree $n > 0$ that

$$w_{E_n} = \begin{cases} 1, & \text{if } n \equiv 1, 2, 3 \bmod 8, \\ -1, & \text{if } n \equiv 5, 6, 7 \bmod 8, \end{cases}$$

so if $n \equiv 5, 6, 7 \bmod 8$ then we *expect* $E_n(\mathbf{Q})$ to have odd (so positive) rank. Monsky (1990) proved this unconditionally for prime $p \equiv 5, 7 \bmod 8$.

Application of ranks: congruent number problem

Example. The number 157 is prime and $157 \equiv 5 \bmod 8$. Thus there is definitely a rational right triangle with area 157.

The triangle corresponds to a rational point on $y^2 = x^3 - 157^2 x$ with $y \neq 0$.

Application of ranks: congruent number problem

Example. The number 157 is prime and $157 \equiv 5 \bmod 8$. Thus there is definitely a rational right triangle with area 157.

The triangle corresponds to a rational point on $y^2 = x^3 - 157^2 x$ with $y \neq 0$.

Here are the simplest rational point and triangle, which were found by Zagier (1990):

$$
\begin{aligned}
x &= \frac{6964897098259649425445822 5}{166136231668185267540804}, \\
y &= \frac{53896243508960461507800430725878521833 5}{6771681655607745599922849543574240 8}, \\
a &= \frac{41134051922771614938320 3}{21666555693714761309610}, \\
b &= \frac{68032984878264350512175 40}{41134051922771614938320 3}, \\
c &= \frac{22440351770433696992455751309067486316094847204 1}{89123322689288595880255351789671635700164808 30}.
\end{aligned}
$$

Application of ranks: Sylvester's conjecture

Which n in $\mathbf{Z}^+$ are x^3+y^3 for $x, y \in \mathbf{Q}$? Yes for $n = 1$ and 2, no for $n = 3$. Sylvester (really Selmer) conjectured for primes $p \geq 5$,

- if $p \equiv 2, 5 \bmod 9$ then it is not x^3+y^3 (false at $p = 2$),
- if $p \equiv 4, 7, 8 \bmod 9$ then it is x^3+y^3.

If $p \equiv 1 \bmod 9$ it can go either way. Data for $p < 200$: 19, 37, 127, and 163 are x^3+y^3 while 73, 109, 181, and 199 are not.

On $E_p : x^3+y^3 = p$ each $(x, y) \in E_p(\mathbf{Q})$ has infinite order, so if p is x^3+y^3 with $x, y \in \mathbf{Q}$ at least once then it is infinitely often.

It can be shown that

$$w_{E_p} = \begin{cases} -1, & \text{if } p \equiv 4, 7, 8 \bmod 9, \\ 1, & \text{otherwise,} \end{cases}$$

$$\begin{aligned} p \equiv 2, 5 \bmod 9 &\implies \operatorname{rank}(E_p(\mathbf{Q})) = 0, \\ p \equiv 4, 7, 8 \bmod 9 &\implies \operatorname{rank}(E_p(\mathbf{Q})) = 1, \\ p \equiv 1 \bmod 9 &\implies \operatorname{rank}(E_p(\mathbf{Q})) = 0 \text{ or } 2. \end{aligned}$$

Application of ranks: Hilbert's 10th problem

H10: is there an algorithm that, for *every* polynomial equation with coefficients in $\mathbf{Z}$ (in finitely many variables), determines if it has a solution in $\mathbf{Z}$?

Answer: NO. This is the MRDP theorem (1970).

What if we replace $\mathbf{Z}$ with ring of integers of a number field?

Application of ranks: Hilbert's 10th problem

H10: is there an algorithm that, for *every* polynomial equation with coefficients in $\mathbf{Z}$ (in finitely many variables), determines if it has a solution in $\mathbf{Z}$?

Answer: NO. This is the MRDP theorem (1970).

What if we replace $\mathbf{Z}$ with ring of integers of a number field?

- Denef (1980) showed that for each totally real number field K (*e.g.*, $K = \mathbf{Q}(\sqrt{2})$), if there is elliptic curve E over $\mathbf{Q}$ such that $E(K)$ and $E(\mathbf{Q})$ have rank 1, then H10 has answer NO for the integers of K. The argument uses denominators of x-coordinates of points on E.

Application of ranks: Hilbert's 10th problem

H10: is there an algorithm that, for *every* polynomial equation with coefficients in $\mathbf{Z}$ (in finitely many variables), determines if it has a solution in $\mathbf{Z}$?

Answer: NO. This is the MRDP theorem (1970).

What if we replace $\mathbf{Z}$ with ring of integers of a number field?

- Denef (1980) showed that for each totally real number field K (*e.g.*, $K = \mathbf{Q}(\sqrt{2})$), if there is elliptic curve E over $\mathbf{Q}$ such that $E(K)$ and $E(\mathbf{Q})$ have rank 1, then H10 has answer NO for the integers of K. The argument uses denominators of x-coordinates of points on E.
- By work of Poonen, Shlapentokh, *et al.* if there is an elliptic curve E over $\mathbf{Q}$ such that $E(K)$ and $E(\mathbf{Q})$ have same *positive* rank, then H10 has answer NO for integers of K.
- Existence of suitable elliptic curves follows from conjectures about Tate–Shafarevich groups (Mazur–Rubin) or from rank aspects of the BSD conjecture (Murty–Pasten).

Application of ranks: class numbers of imaginary quadratic fields

For squarefree $d > 0$, let h_d be class number of $\mathbf{Q}(\sqrt{-d})$. By Hecke and Heilbronn, $h_d \to \infty$ as $|d| \to \infty$, but not effectively.

- 1935: Siegel showed that for all $\varepsilon > 0$ there's $c_\varepsilon > 0$ such that $h_d > c_\varepsilon d^{1/2-\varepsilon}$ for all d, but c_ε can't be explicitly determined.
- 1952/1966-67: Heegner and then Baker and Stark determine when $h_d = 1$: 9 examples.
- 1971: Baker & Stark determine when $h_d = 2$: 18 examples.

Application of ranks: class numbers of imaginary quadratic fields

For squarefree $d > 0$, let h_d be class number of $\mathbf{Q}(\sqrt{-d})$. By Hecke and Heilbronn, $h_d \to \infty$ as $|d| \to \infty$, but not effectively.

- 1935: Siegel showed that for all $\varepsilon > 0$ there's $c_\varepsilon > 0$ such that $h_d > c_\varepsilon d^{1/2-\varepsilon}$ for all d, but c_ε can't be explicitly determined.
- 1952/1966-67: Heegner and then Baker and Stark determine when $h_d = 1$: 9 examples.
- 1971: Baker & Stark determine when $h_d = 2$: 18 examples.
- 1976: Goldfeld showed $h_d \geq c_\varepsilon (\log d)^{1-\varepsilon}$ with computable c_ε, provided there is *some* elliptic curve E over $\mathbf{Q}$ such that

$$\mathrm{ord}_{s=1}(L(E,s)) \geq 3.$$

This condition makes the exponent on $\log d$ at least $1 - \varepsilon$.

Application of ranks: class numbers of imaginary quadratic fields

For squarefree $d > 0$, let h_d be class number of $\mathbf{Q}(\sqrt{-d})$. By Hecke and Heilbronn, $h_d \to \infty$ as $|d| \to \infty$, but not effectively.

- 1935: Siegel showed that for all $\varepsilon > 0$ there's $c_\varepsilon > 0$ such that $h_d > c_\varepsilon d^{1/2-\varepsilon}$ for all d, but c_ε can't be explicitly determined.
- 1952/1966-67: Heegner and then Baker and Stark determine when $h_d = 1$: 9 examples.
- 1971: Baker & Stark determine when $h_d = 2$: 18 examples.
- 1976: Goldfeld showed $h_d \geq c_\varepsilon (\log d)^{1-\varepsilon}$ with computable c_ε, provided there is *some* elliptic curve E over $\mathbf{Q}$ such that

$$\mathrm{ord}_{s=1}(L(E,s)) \geq 3.$$

  This condition makes the exponent on $\log d$ at least $1 - \varepsilon$.
- Mid-1980s: Gross and Zagier constructed an explicit example of the elliptic curve Goldfeld needed: an E where $w_E = -1$ and provably $L'(E,1) = 0$ (not just $L'(E,1) \approx .000000001$).

Behavior of ranks

Elevated rank

Let's return to elliptic curves E_T over $\mathbf{Q}(T)$. Recall from before

$$\text{rank}(E_t(\mathbf{Q})) \geq \text{rank}(E_T(\mathbf{Q}(T)))$$

for all but finitely many $t \in \mathbf{Q}$. **Question**: Could this inequality be strict all the time? If so, say E_T has *elevated rank*. The parity conjecture suggests a strategy to find examples of elevated rank.

Example (Cassels, Schinzel) The elliptic curve

$$E_T : y^2 = x^3 - (7(1+T^4))^2 x$$

over $\mathbf{Q}(T)$ has the following properties:

$$E_T(\mathbf{Q}(T)) \text{ has rank 0 (it is finite)}, \quad \text{for all } t \in \mathbf{Q},\ w_{E_t} = -1.$$

The parity conjecture would imply $E_t(\mathbf{Q})$ has odd rank from $w_{E_t} = -1$, so we should have

$$\text{rank}(E_t(\mathbf{Q})) > \text{rank}(E_T(\mathbf{Q}(T))) \quad \text{for all } t \in \mathbf{Q}.$$

Elevated rank

Let's return to elliptic curves E_T over $\mathbf{Q}(T)$. Recall from before

$$\operatorname{rank}(E_t(\mathbf{Q})) \geq \operatorname{rank}(E_T(\mathbf{Q}(T)))$$

for all but finitely many $t \in \mathbf{Q}$. **Question**: Could this inequality be strict all the time? If so, say E_T has *elevated rank*. The parity conjecture suggests a strategy to find examples of elevated rank.

Example (Cassels, Schinzel) The elliptic curve

$$E_T : y^2 = x^3 - (7(1+T^4))^2 x$$

over $\mathbf{Q}(T)$ has the following properties:

$$E_T(\mathbf{Q}(T)) \text{ has rank 0 (it is finite)}, \quad \text{for all } t \in \mathbf{Q},\ w_{E_t} = -1.$$

The parity conjecture would imply $E_t(\mathbf{Q})$ has odd rank from $w_{E_t} = -1$, so we should have

$$\operatorname{rank}(E_t(\mathbf{Q})) > \operatorname{rank}(E_T(\mathbf{Q}(T))) \quad \text{for all } t \in \mathbf{Q}.$$

An elliptic curve $y^2 = x^3 - A(T)^2 x$ is not "truly" defined over $\mathbf{Q}(T)$: by the change of variables $x \mapsto A(T)x$ and $y \mapsto A(T)^{3/2}y$ the curve becomes $y^2 = x^3 - x$, which is defined over $\mathbf{Q}$.

Elevated rank

Assuming standard conjectures about elliptic curves over $\mathbf{Q}$ and polynomials in $\mathbf{Z}[T]$, every elliptic curve over $\mathbf{Q}(T)$ with elevated rank can be turned into an elliptic curve over $\mathbf{Q}$ by a change of variables.

Elevated rank

Assuming standard conjectures about elliptic curves over $\mathbf{Q}$ and polynomials in $\mathbf{Z}[T]$, every elliptic curve over $\mathbf{Q}(T)$ with elevated rank can be turned into an elliptic curve over $\mathbf{Q}$ by a change of variables.

Now consider the "function field" case: $\mathbf{Z} \rightsquigarrow \mathbf{F}_p[u]$, $\mathbf{Q} \rightsquigarrow \mathbf{F}_p(u)$.

$\mathbf{Z}$	$\mathbf{F}_p[u]$
units: ± 1	units: $\mathbf{F}_p^\times = \mathbf{F}_p - \{0\}$
prime	irreducible
$\lvert m \rvert$	$\deg g$
Div. Algorithm	Div. Algorithm
$\mathbf{Z}/(m)$	$\mathbf{F}_p[u]/(g)$

Theorem. *For $m \neq 0$, $|\mathbf{Z}/(m)| = |m|$; for $g \neq 0$, $|\mathbf{F}_p[u]/(g)| = p^{\deg g}$.*

Theorem. *For $m \geq 1$, $\mathbf{Z}/(m)$ is a field if and only if m is prime. For any $g \neq 0$, $\mathbf{F}_p[u]/(g)$ is a field if and only if g is irreducible.*

Theorem. *For every prime p, $\mathbf{F}_p^\times$ is cyclic. For every irreducible π, $(\mathbf{F}_p[u]/(\pi))^\times$ is cyclic.*

Elevated rank

Recall: standard conjectures about elliptic curves over $\mathbf{Q}$ and polynomials in $\mathbf{Z}[T]$ imply every elliptic curve over $\mathbf{Q}(T)$ with elevated rank can be turned into an elliptic curve over $\mathbf{Q}$ by a change of variables.

Elevated rank

Recall: standard conjectures about elliptic curves over $\mathbf{Q}$ and polynomials in $\mathbf{Z}[T]$ imply every elliptic curve over $\mathbf{Q}(T)$ with elevated rank can be turned into an elliptic curve over $\mathbf{Q}$ by a change of variables.

However... the analogue for $\mathbf{F}_p[u][T]$ of one of the conjectures about $\mathbf{Z}[T]$ is *false*.

Elevated rank

Recall: standard conjectures about elliptic curves over $\mathbf{Q}$ and polynomials in $\mathbf{Z}[T]$ imply every elliptic curve over $\mathbf{Q}(T)$ with elevated rank can be turned into an elliptic curve over $\mathbf{Q}$ by a change of variables.

However... the analogue for $\mathbf{F}_p[u][T]$ of one of the conjectures about $\mathbf{Z}[T]$ is *false*.

Theorem (BC, KC, HH) *For each odd prime p there is an elliptic curve E_T over $\mathbf{F}_p(u)(T)$ that is not convertible into an elliptic curve over $\mathbf{F}_p(u)$ by a change of variables and has the following properties:*

- *$E_T(\mathbf{F}_p(u)(T))$ has rank 1,*
- *For all $t \in \mathbf{F}_p(u)$, $w_{E_t} = 1$ and $\mathrm{rank}(E_t(\mathbf{F}_p(u))) > 0$.*

The parity conjecture over $\mathbf{F}_p(u)$, if true, would imply here that

$$\mathrm{rank}(E_t(\mathbf{F}_p(u))) > \mathrm{rank}(E_T(\mathbf{F}_p(u)(T)))$$

for all $t \in \mathbf{F}_p(u)$ since the left side should be even, right side is 1.

Values of ranks

Unlike Dirichlet's theorem about the rank of units, we don't know **which integers** are ranks of some $E(\mathbf{Q})$.

1950s: Néron conjectured ranks of $E(\mathbf{Q})$ are bounded.

1960s-recently: believe ranks of $E(\mathbf{Q})$ are unbounded.

Why did the conventional wisdom change?

1. Known examples of lower bound on rank$(E(\mathbf{Q}))$ kept getting bigger: at least 4 (1945), 7 (1975), 12 (1982), 20 (1993), and 28 (2006).
2. For elliptic curves over $\mathbf{F}_p(u)$, where Mordell–Weil theorem is true, examples of Tate and Shafarevich, and later Ulmer, have unbounded ranks.

Values of ranks

Unlike Dirichlet's theorem about the rank of units, we don't know **which integers** are ranks of some $E(\mathbf{Q})$.

1950s: Néron conjectured ranks of $E(\mathbf{Q})$ are bounded.

1960s-recently: believe ranks of $E(\mathbf{Q})$ are unbounded.

Why did the conventional wisdom change?

1. Known examples of lower bound on rank$(E(\mathbf{Q}))$ kept getting bigger: at least 4 (1945), 7 (1975), 12 (1982), 20 (1993), and 28 (2006).
2. For elliptic curves over $\mathbf{F}_p(u)$, where Mordell–Weil theorem is true, examples of Tate and Shafarevich, and later Ulmer, have unbounded ranks.

In 2017, Park, Poonen, Voight, and Wood introduced a heuristic probabilistic model for elliptic curve ranks that suggests ranks are *bounded*

Values of ranks

Unlike Dirichlet's theorem about the rank of units, we don't know **which integers** are ranks of some $E(\mathbf{Q})$.

1950s: Néron conjectured ranks of $E(\mathbf{Q})$ are bounded.

1960s-recently: believe ranks of $E(\mathbf{Q})$ are unbounded.

Why did the conventional wisdom change?

1. Known examples of lower bound on rank$(E(\mathbf{Q}))$ kept getting bigger: at least 4 (1945), 7 (1975), 12 (1982), 20 (1993), and 28 (2006).
2. For elliptic curves over $\mathbf{F}_p(u)$, where Mordell–Weil theorem is true, examples of Tate and Shafarevich, and later Ulmer, have unbounded ranks.

In 2017, Park, Poonen, Voight, and Wood introduced a heuristic probabilistic model for elliptic curve ranks that suggests ranks are *bounded*: finitely many elliptic curves over $\mathbf{Q}$ have rank ≥ 22. The current record for infinitely many ranks is 19.

Thanks!