Elliptic curves and Hilbert's Tenth Problem

Karl Rubin, UC Irvine

MAA @ UC Irvine
October 16, 2010

Elliptic curves

An elliptic curve is a curve defined by an equation

$$E : y^2 = x^3 + ax + b$$

with integers (constants) a, b such that $4a^3 + 27b^2 \neq 0$.

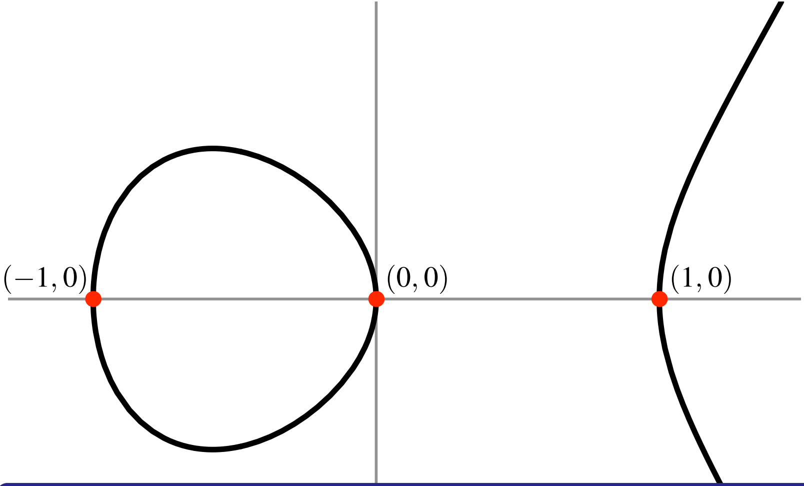
A rational point on E is a pair (x, y) of rational numbers satisfying this equation. There is also one "point at infinity" on E.

Basic Problem

Given an elliptic curve, find all solutions in rational numbers (x, y). In other words, find

$$E(\mathbf{Q}) := \{\textit{rational points on } E\} \cup \{\infty\}$$

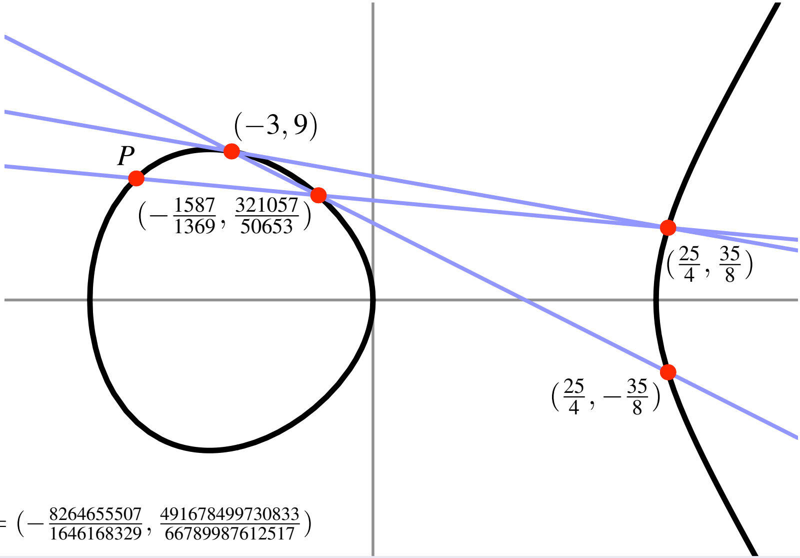
$E : y^2 = x^3 - x$



Example (Fermat)

If E *is* $y^2 = x^3 - x$, *then* $E(\mathbf{Q}) = \{(0,0),(1,0),(-1,0),\infty\}$.

$E : y^2 = x^3 - 36x$

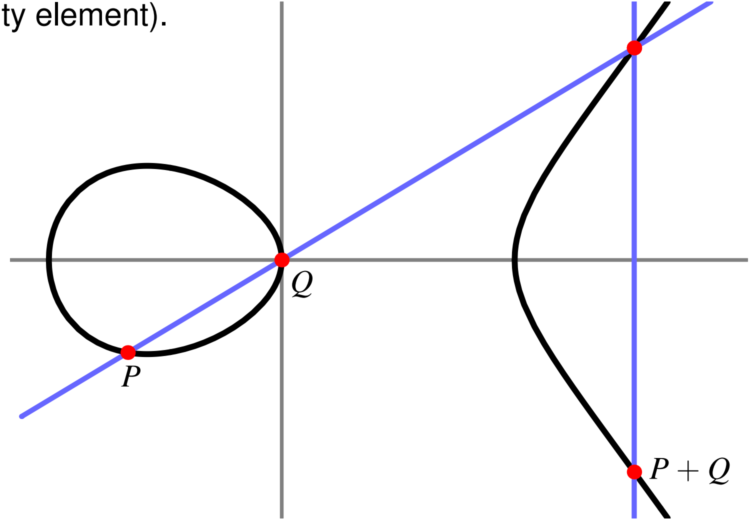


$P = (-\frac{8264655507}{1646168329}, \frac{491678499730833}{66789987612517})$

This procedure gives infinitely many rational points (x, y) on E.

Addition law

The chord-and-tangent process defines an addition law on $E(\mathbf{Q})$, that makes $E(\mathbf{Q})$ a commutative group (with ∞ as the identity element).



Addition law

If E is the elliptic curve $y^2 = x^3 + ax + b$, and

$$P = (x_1, y_1), \quad Q = (x_2, y_2)$$

with $x_1 \neq x_2$, then $P + Q = (x_3, y_3)$ where

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

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

Elliptic curves

Theorem (Mordell, 1922)

$E(\mathbf{Q})$ is finitely generated.

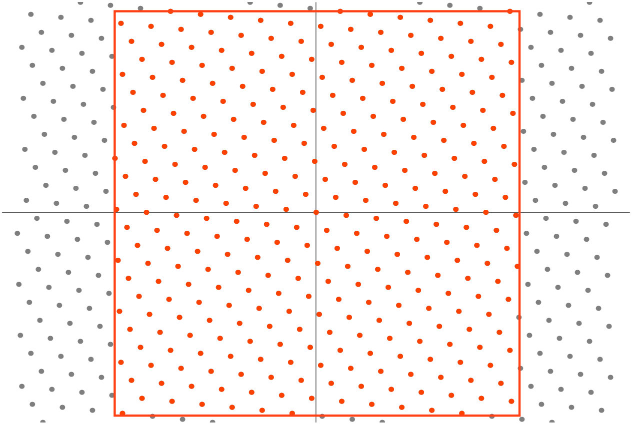
In other words, even though $E(\mathbf{Q})$ might be infinite, there is always a finite set of points $\{P_1, P_2, \ldots, P_r\}$ that generates all rational points using the chord-and-tangent process.

$$E(\mathbf{Q}) = \mathbf{Z}^r \times F = \underbrace{\mathbf{Z} \times \cdots \times \mathbf{Z}}_{r \text{ times}} \times F$$

with a finite commutative group F. The nonnegative integer r is called the rank of $E(\mathbf{Q})$, and F is called the torsion subgroup.

$$E(\mathbf{Q}) \text{ is finite} \iff \mathrm{rank}(E(\mathbf{Q})) = 0.$$

$E(\mathbf{Q}) = \mathbf{Z}^r \times F$



$E(\mathbf{Q})$ can be viewed in a natural way as an r-dimensional lattice Euclidean space. The dimension r determines the rate of growth of the number of lattice points in larger and larger boxes.

$E(\mathbf{Q}) = \mathbf{Z}^r \times F$

If $x = m/n$ is a rational number (where the integers m, n have no common factor), define the height of x to be

$$H(x) = \max\{m, n\}.$$

Theorem

There is a real number $C > 0$ such that

$$\#\{(x, y) \in E(\mathbf{Q}) : H(x), H(y) < B\} \sim C \log(B)^{r/2}.$$

(Here "$\sim$" means that the ratio of the two sides converges to 1 as B goes to infinity.)

$E : y^2 = x^3 - 36x, \quad P = (-3, 9)$

$$2P = \left(\frac{25}{4}, \frac{-35}{8}\right)$$

$$3P = \left(\frac{-1587}{1369}, \frac{-321057}{50653}\right)$$

$$4P = \left(\frac{1442401}{19600}, \frac{1726556399}{2744000}\right)$$

$$5P = \left(\frac{-8264655507}{1646168329}, \frac{491678499730833}{66789987612517}\right)$$

$$6P = \left(\frac{60473718955225}{6968554599204}, \frac{-339760634079313268605}{18395604368087917608}\right)$$

$$7P = \left(\frac{-583552361658258723}{402304176344820456 1}, \frac{-18433964971574382270849196761}{8069224743013821217381442809}\right)$$

$$8P = \left(\frac{4386303618090112563849601}{2337101647159432205584 00}, \frac{870436910908558082827593565062625440 1}{1129838585124636197372166844964480 00}\right)$$

$$9P = \left(\frac{-38588308319846692331485009382883}{6433437028050748454240723606641}, \frac{6056228937102241081991642356775948265805217721}{16317911804506723620780282462635842443354311689}\right)$$

$$10P = \left(\frac{339623358722762426094451563298394625625}{19652221475511578582811254387824437604}, \frac{-5869544619324614780595892276791057797695461715964593892675}{871199213782997348607543268339134452455771772027863928 08}\right)$$

$$11P = \left(\frac{-2512776550703017851462002707141301981572730067}{2469380428548761245880995690250860620694461520 9}, \frac{7425979074210113673657917982788245778472213771855848368670943739722447}{3880449202583286201483684978743391154828721407443504941067779207054677}\right)$$

$$12P = \left(\frac{292168118796034529076545406855282629394493624046414 61601}{3217724189948388661397795704743707676716077672251056400}, \frac{1185326491826201343003759777335779513897177176490252104343415624677280629}{577195880906504107332728319804818500712870376921838292316291709846918453}\right.$$

$$13P = \left(\frac{-316201127357824410367418035302071126309291938514702260650926563827}{61184403732733446451852573707104162463990295806262667569316972089}, \frac{-10487483632369961972739306064290828898283677484744501609922}{15134256770846398391550680361225920344918831298146269968145}\right.$$

$$14P = \left(\frac{4196098227570015536181717307056998500537202867254564476717797975116438531225}{67509832319007616089031696842305848128857748695637998060454233577970795204}, \frac{-270542500222440876153818235148011851121299426089967}{554690265001984276834717127701010275608151014051574}\right.$$

$$15P = \left(\frac{-326323187135694809972784367371266172424012278677531085743337805707290355439047007391043}{316223166012923607256727765926494680077042982884129292116373508542581225616984993596321}, \frac{3376359248175257622253956693440245342035}{562329055096600632261604857289516140527}\right.$$

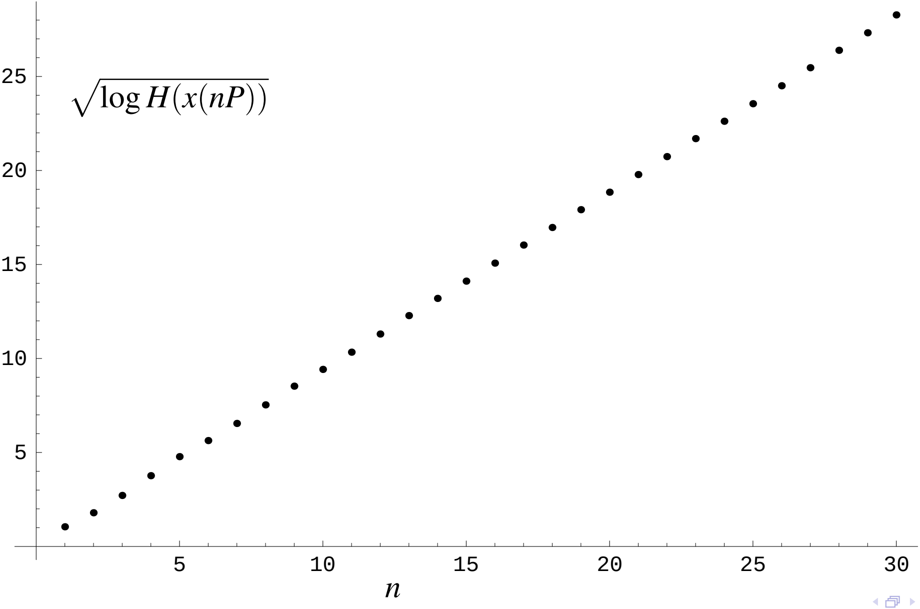
$$16P = \left(\frac{449694237060866843762380349168814474651681212183233022035313594048287173659552111551208111024678401}{70829176236881157057028857786312342915175978142395358722885216836927586836054230045112363033913600}, \frac{311815448681385123889964216125}{596098853167031897174213952215}\right.$$

$$17P = \left(\frac{-44184506836459721465991576317238856020714499252679664970555879486866646117427804847809553166207611892923783495363}{1386630513029380907378997915130655277611829156099736456432476600527207819434467679505923440331200528020017488481}, \frac{-4685933166732}{5163463709828}\right.$$

$$18P = \left(\frac{109565823147330584355436543609555997002300337870400316735151301054200012054832916698483032458986447331013838759107613707952025}{116525934556556861252601938878468055774248594619406169659205222456904519842803776158557153391730507135535765461336355920 04}, \frac{-3}{}\right.$$

$$19P = \left(\frac{-243900944682881311545938630933606024384706193598834577292503536694820667828298032629745605679382443075987518720477456230912644026}{8662964695416756327622400522501024384478081298830914462830903689387949914745202488635345504888341041205194955707453910993822286712}\right.$$

$E : y^2 = x^3 - 36x, \quad P = (-3, 9)$



The torsion subgroup

Theorem (Nagell, Lutz 1937)

If $(x, y) \in F$, then x and y are integers and either $y = 0$ or y^2 divides $16(4a^3 + 27b^2)$.

Theorem (Mazur 1977)

The order of F is at most 16.

It follows from the Nagell-Lutz Theorem that if E is $y^2 = x^3 - d^2x$, then

$$F = \{(0,0), (d,0), (-d,0), \infty\}.$$

The torsion subgroup

$$E : y^2 = x^3 - 33339627x + 73697852646$$

$$\begin{aligned} 16(4a^3 + 27b^2) &= -2535992741993014886400 0 \\ &= -2^{24} \cdot 3^{18} \cdot 5^3 \cdot 7^4 \cdot 13 \end{aligned}$$

$$\begin{aligned} P &= (-4533, -362880) & 7P &= (3027, 22680) \\ 2P &= (10587, 952560) & 8P &= (4107, -77760) \\ 3P &= (1515, -163296) & 9P &= (1515, 163296) \\ 4P &= (4107, 77760) & 10P &= (10587, -952560) \\ 5P &= (3027, -22680) & 11P &= (-4533, 362880) \\ 6P &= (3531, 0) & 12P &= \infty \end{aligned}$$

$$E(\mathbf{Q}) = \mathbf{Z}/12\mathbf{Z}$$

The rank

- There is no known algorithm that is *guaranteed* to compute the rank of E. (There are methods for computing lower bounds, and methods for computing upper bounds. Often these bounds are the same.)
- It is not known which integers r occur as ranks of elliptic curves over $\mathbf{Q}$. (It is not known whether r can be arbitrarily large.)

Rank record (Elkies 2006)

$$
\begin{aligned}
y^2 + xy + y = x^3 - x^2 &- 20067762415575526585033208209338542750930230312178956502x \\
&+ 34481611795030556467032985690390720374855944359319180361266008296291939448732243429
\end{aligned}
$$

has rank at least 28, with independent points:

$$
\begin{array}{l}
(-2124150091254381073292137463, 259854492051899599030515511070780628911531) \\
(2334509866034701756884754537, 18872004195494469180868316552803627931531) \\
(-1671736054062369063879038663, 251709377261144287808506947241319126049131) \\
(2139130260139156666492982137, 36639509171439729202421459692941297527531) \\
(1534706764467120723885477337, 85429585346017694289021032862781072799531) \\
(-2731079487875677033341575063, 262521815484332191641284072623902143387531) \\
(2775726266844571649705458537, 12845755474014060248869487699082640369931) \\
(1494385729327188957541833817, 88486605527733405986116494514049233411451) \\
(1868438228620887358509065257, 59237403214437708712725140393059358589131) \\
(2008945108825743774866542537, 47690677880125552882151750781541424711531) \\
(2348360540918025169651632937, 17492930006200557857340332476448804363531) \\
(-1472084007090481174470008663, 246643450653503714199947441549759798469131) \\
(2924128607708061213363288937, 28350264431488878501488356474767375899531) \\
(5374993891066061893293934537, 286188908427263386451175031916479893731531) \\
(1709690768233354523334008557, 71898834974686089466159700529215980921631) \\
(2450954011353593144072595187, 4445228173532634357049262550610714736531) \\
(2969254709273559167464674937, 32766893075366270801333682543160469687531) \\
(2711914934941692601332882937, 2068436612778381698650413981506590613531) \\
(20078586077996854528778328937, 2779608541137806604656051725624624030091531) \\
(2158082450240734774317810697, 34994373401964026809969662241800901254731) \\
(2004645458247059022403224937, 48049329780704645522439866999888475467531) \\
(2975749450947996264947091337, 33398989826075322320208934410104857869131) \\
(-2102490467686285150147347863, 259576391459875789571677393171687203227531) \\
(311583179915063034902194537, 16810438522998060354010947291566015347393 1) \\
(2773931008341865231443771817, 12632162834649921002414116273769275813451) \\
(2156581188143768409363461387, 35125092964022908897004150516375178087331) \\
(3866330499872412508815659137, 121197755655944226293036926715025847322531) \\
(2230868289773576023778678737, 28558760030597485663387020600768640028531)
\end{array}
$$

Rank of $E_d : y^2 = x^3 - d^2x$

d	$\mathrm{rank}(E_d)$	
1	0	Fermat (∼1640)
5	1	$(-4, 6)$
34	2	$(-2, 48), (-16, 120)$
1254	3	$(-98, 12376), (1650, 43560), (109554, 36258840)$
29274	4	Wiman (1945)
205015206	5	Rogers (1999)
61471349610	6	Rogers (1999)
797507543735	7	Rogers (2003)
?	≥ 8	

Birch and Swinnerton-Dyer conjecture

Conjecture (Birch and Swinnerton-Dyer)

$$\mathrm{rank}(E(\mathbf{Q})) = \mathrm{ord}_{s=1} L(E,s)$$

$L(E,s)$ is the L-function attached to E, an entire complex-analytic function.

Parity Conjecture (consequence of BSD)

$$\mathrm{rank}(E(\mathbf{Q})) \equiv \mathrm{ord}_{s=1} L(E,s) \pmod{2}$$

The parity of $\mathrm{ord}_{s=1} L(E,s)$ is computable, thanks to a functional equation that relates $L(E,s)$ to $L(E,2-s)$.

Birch and Swinnerton-Dyer conjecture

Example

The Parity Conjecture predicts that if d is squarefree and E_d is the curve $y^2 = x^3 - d^2x$, then

$$\operatorname{rank}(E_d(\mathbf{Q})) \text{ is } \begin{cases} \textit{even} & \text{if } d \equiv 1, 2, \text{ or } 3 \pmod 8, \\ \textit{odd} & \text{if } d \equiv 5, 6, \text{ or } 7 \pmod 8. \end{cases}$$

Note in particular that if $\operatorname{rank}(E_d(\mathbf{Q}))$ is odd, then it is positive, so $E_d(\mathbf{Q})$ is infinite.

Average rank

Conjecture (Goldfeld 1979, . . .)

The "average rank of elliptic curves" is $1/2$*. More precisely*

- 50% *of all elliptic curves have rank zero,*
- 50% *of all elliptic curves have rank one,*
- 0% *of all elliptic curves have rank two or more.*

Theorem (Bhargava & Shankar 2010)

- *The average rank of elliptic curves is at most* $7/6$*.*
- *A positive proportion of all elliptic curves have rank zero.*

Hilbert's 10th Problem

Hilbert's 10th Problem

Suppose $F_1, \ldots, F_m \in \mathbf{Z}[X_1, X_2, \ldots, X_n]$ are polynomials in several variables.

Is there an algorithm to decide whether or not the F_i have a common zero, i.e., whether there are $k_i, \ldots, k_n \in \mathbf{Z}$ such that

$$F_1(k_1, \ldots, k_n) = F_2(k_1, \ldots, k_n) = \cdots = F_m(k_1, \ldots, k_n) = 0?$$

Theorem (Matiyasevich, Robinson, Davis, Putnam 1970)

No.

What if $\mathbf{Z}$ is replaced by some other ring?

Hilbert's 10th Problem over a ring R

Hilbert's 10th Problem over R

Suppose R is a ring, and $F_1, \ldots, F_m \in R[X_1, X_2, \ldots, X_n]$ are polynomials in several variables.

Is there an algorithm to decide whether or not the F_i have a common zero, i.e., whether there are $k_i, \ldots, k_n \in R$ such that

$$F_1(k_1, \ldots, k_n) = F_2(k_1, \ldots, k_n) = \cdots = F_m(k_1, \ldots, k_n) = 0?$$

- $R = \mathbf{Q}$: unknown
- $R = \mathbf{C}$: yes
- R a finite field: yes
- $R = \mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}, i^2 = -1\}$: no
- other rings of algebraic integers…

Reducing from R to $\mathbf{Z}$

Definition

A subset $D \subset R$ *is* diophantine over R *if there is a polynomial* $G(X, Y_1, \ldots, Y_k) \in R[X, Y_1, \ldots, Y_k]$ *such that for every* $x \in R$*,*

$x \in D \iff$ *there exist* $y_1, \ldots, y_k \in R$ *such that* $G(x, y_1, \ldots, y_k) = 0.$

Easy examples

- *The set of squares is diophantine over* $\mathbf{Z}$*:* $G(X, Y) = X - Y^2$*.*
- $\mathbf{Z}_{\geq 0}$ *is diophantine over* $\mathbf{Z}$*:* $X - Y_1^2 - Y_2^2 - Y_3^2 - Y_4^2$*.*
- $\mathbf{Q}_{\geq 0}$ *is diophantine over* $\mathbf{Q}$*:* $X - Y_1^2 - Y_2^2 - Y_3^2 - Y_4^2$*.*
- *If* D_1 *and* D_2 *are diophantine over* R*, then so is* $D_1 \cup D_2$*:*

  $$G_1(X, Y_1, \ldots, Y_k)G_2(X, Y_1, \ldots, Y_k).$$

  . . . and $D_1 \cap D_2$*, if* $R \subset \mathbf{R}$*:*

  $$G_1(X, Y_1, \ldots, Y_k)^2 + G_2(X, Y_{k+1}, \ldots, Y_{k+k'})^2.$$

Reducing from R to $\mathbf{Z}$

Definition

A subset $D \subset R$ *is* diophantine over R *if there is a polynomial* $G(X, Y_1, \ldots, Y_k) \in R[X, Y_1, \ldots, Y_k]$ *such that for every* $x \in R$*,*

$$x \in D \iff \text{there exist } y_1, \ldots, y_k \in R \text{ such that } G(x, y_1, \ldots, y_k) = 0.$$

Less easy examples

- *The set of positive nonsquares is diophantine over* $\mathbf{Z}$*:*
$$G(X, Y_1, \ldots, Y_5) = Y_1^2 - X(1 + Y_2^2 + Y_3^2 + Y_4^2 + Y_5^2)^2 - 1.$$
- *The set of positive composite (nonprime) numbers is diophantine over* $\mathbf{Z}$*:*
$$G(X, Y_1, \ldots, Y_8) = X - (2 + Y_1^2 + \cdots + Y_4^2)(2 + Y_5^2 + \cdots + Y_8^2).$$

Reducing from R to $\mathbf{Z}$

Definition

A subset $D \subset R$ *is* diophantine over R *if there is a polynomial* $G(X, Y_1, \ldots, Y_k) \in R[X, Y_1, \ldots, Y_k]$ *such that for every* $x \in R$*,*

$x \in D \iff$ *there exist* $y_1, \ldots, y_k \in R$ *such that* $G(x, y_1, \ldots, y_k) = 0$.

Hard examples

- $\mathbf{Z}$ *is diophantine over* $\mathbf{Z}[i]$.
- *The set of primes is diophantine over* $\mathbf{Z}$.
- *Is* $\mathbf{Z}$ *diophantine over* $\mathbf{Q}$*?*

Reducing from R to $\mathbf{Z}$

Theorem

If $\mathbf{Z}$ is diophantine over R, then Hilbert's 10th Problem has a negative answer over R.

Proof.

Let G be the polynomial that shows $\mathbf{Z}$ is diophantine over R, and suppose $F_1, \ldots, F_m \in \mathbf{Z}[X_1, \ldots, X_n]$. The collection

$$F_1, \ldots, F_m, G(X_1, Y_{1,1}, \ldots, Y_{1,k}), \ldots, G(X_n, Y_{n,1}, \ldots, Y_{n,k}) \in R[X_i, Y_{j,j'}]_{1 \le i,j \le n, 1 \le j' \le l}$$

is solvable in R if and only if the collection $F_1, \ldots, F_m$ is solvable in $\mathbf{Z}$. Thus if we *can* decide the solvability of polynomials over R, then we *can* decide the solvability of $F_1, \ldots, F_m$ over $\mathbf{Z}$. This contradicts Matiyasevich's theorem. □

Reducing from R to $\mathbf{Z}$

This is why we would like to know if $\mathbf{Z}$ is diophantine over $\mathbf{Q}$.

Theorem

More generally, If S is a subring of R that is diophantine over R, and Hilbert's 10th Problem has a negative answer over S, then Hilbert's 10th Problem has a negative answer over R.

Proof.

Same. □

Rings of algebraic integers

- An algebraic number is a root of a polynomial in one variable with coefficients in $\mathbf{Q}$.
- An algebraic integer is a root of a monic polynomial in one variable with coefficients in $\mathbf{Z}$.
- A number field is an extension of $\mathbf{Q}$ generated by finitely many algebraic numbers.
- The ring of integers $\mathcal{O}_K$ of a number field K is the set of all algebraic integers in K.

Rings of algebraic integers

Example

If $K = \mathbf{Q}$, *then* $\mathcal{O}_K = \mathbf{Z}$.

Example (Quadratic fields)

If $K = \mathbf{Q}(\sqrt{d})$ *with* $d \in \mathbf{Z}$ *squarefree, then*

$$\mathcal{O}_K = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\} \qquad \text{if } d \equiv 2 \text{ or } 3 \pmod 4,$$
$$\mathcal{O}_K = \{a + b\tfrac{1+\sqrt{d}}{2} : a, b \in \mathbf{Z}\} \qquad \text{if } d \equiv 1 \pmod 4$$

($\frac{1+\sqrt{d}}{2}$ *is a root of* $x^2 - x - (d-1)/4 \in \mathbf{Z}[x]$ *if* $d \equiv 1 \pmod 4$).

Example (Cyclotomic fields)

If $K = \mathbf{Q}(e^{2\pi i/n})$ *with* $n \geq 1$, *then* $\mathcal{O}_K = \mathbf{Z}[e^{2\pi i/n}]$.

H10 and elliptic curves

Theorem (Poonen 2002)

Suppose K is a number field. If there is an elliptic curve E over $\mathbf{Q}$ with $\mathrm{rank}(E(\mathbf{Q})) = \mathrm{rank}(E(K)) = 1$, then $\mathbf{Z}$ is diophantine over $\mathcal{O}_K$.

Corollary

Suppose K is a number field. If there is an elliptic curve E over $\mathbf{Q}$ with $\mathrm{rank}(E(\mathbf{Q})) = \mathrm{rank}(E(K)) = 1$, then Hilbert's 10th Problem has a negative answer over $\mathcal{O}_K$.

Example

Let $K = \mathbf{Q}(\sqrt{2}, \sqrt{17})$. If the Parity Conjecture is true, then for every elliptic curve E over $\mathbf{Q}$, then $\mathrm{rank}(E(K))$ is even.

H10 and elliptic curves

Theorem (Poonen 2002)

Suppose that $F \subset K$ are number fields. If there is an elliptic curve E over F with $\mathrm{rank}(E(F)) = \mathrm{rank}(E(K)) = 1$, then $\mathcal{O}_F$ is diophantine over $\mathcal{O}_K$.

Corollary

Suppose that $F \subset K$ are number fields, and Hilbert's 10th Problem has a negative answer over $\mathcal{O}_F$.

If there is an elliptic curve E over F with $\mathrm{rank}(E(F)) = \mathrm{rank}(E(K)) = 1$, then Hilbert's 10th Problem has a negative answer over $\mathcal{O}_K$.

H10 and elliptic curves

Example

Let $F = \mathbf{Q}(\sqrt{2})$, $K = \mathbf{Q}(\sqrt{2}, \sqrt{17})$, so $\mathbf{Q} \subset F \subset K$.

$E_1 : y^2 = x^3 + x + 1$

$\Longrightarrow \mathrm{rank}(E_1(\mathbf{Q})) = \mathrm{rank}(E_1(F)) = 1$, generated by $(0, 1)$

$\Longrightarrow \mathbf{Z}$ is diophantine over $\mathcal{O}_F$

$\Longrightarrow$ Hilbert's 10th Problem has a negative answer over $\mathcal{O}_F$.

$E_2 : y^2 = x^3 + \sqrt{2}\,x + (\sqrt{2} - 1)$ over F

$\Longrightarrow \mathrm{rank}(E(F)) = \mathrm{rank}(E(K)) = 1$,

generated by $(3/2 - \sqrt{2}, 5/2(1 - 1/\sqrt{2}))$

$\Longrightarrow \mathcal{O}_F$ is diophantine over $\mathcal{O}_K$

$\Longrightarrow$ Hilbert's 10th Problem has a negative answer over $\mathcal{O}_K$.

H10 and elliptic curves

Theorem (Mazur & Rubin 2010)

Suppose $F \subset K$ are number fields, and K is a Galois extension of F of prime degree. If the BSD Conjecture holds for all elliptic curves over all number fields, then there is an elliptic curve E over F such that

$$\mathrm{rank}(E(F)) = \mathrm{rank}(E(K)) = 1.$$

Corollary

If the BSD Conjecture holds, then Hilbert's 10th Problem has a negative answer over $\mathcal{O}_K$ for every number field K.

Quadratic twists of elliptic curves

If $E : y^2 = x^3 + ax + b$ is an elliptic curve over K (i.e., $a, b \in K$) then the quadratic twists of E are the curves

$$E_d : y^2 = x^3 + ad^2x + bd^3$$

with $d \in K^\times$.

The curves E and E^d are geometrically very similar (over $K(\sqrt{d})$, or over $\mathbf{C}$, a simple change of variables transforms one into the other), but $E(K)$ and $E_d(K)$ are in general very different.

We would like to study how $\mathrm{rank}(E_d(K))$ varies as d varies (but that's still too hard...)

Selmer groups

The Selmer group $\mathrm{Sel}(E/K)$ is an effectively computable finite dimensional vector space over $\mathbf{F}_2$, that contains $E(K)/2E(K)$.

Let $s(E/K) = \dim_{\mathbf{F}_2} \mathrm{Sel}(E/K)$. Then

- $\mathrm{rank}(E(K)) \leq s(E/K)$
- $s(E/K)$ is effectively computable

Conjecture (Consequence of BSD)

$\mathrm{rank}(E(K)) \equiv s(E/K) \pmod 2$.

Theorem

- *If* $s(E/K) = 0$, *then* $\mathrm{rank}(E(K)) = 0$.
- *If* $s(E/K) = 1$ *and BSD holds, then* $\mathrm{rank}(E(K)) = 1$.

Selmer groups of twists

Theorem (Heath-Brown, Swinnerton-Dyer, Kane)

Suppose E *is* $y^2 = x^3 + ax + b$*, where* $a, b \in \mathbf{Q}$ *and* $x^3 + ax + b$ *has three rational roots. Then the proportion of* d *with* $s(E_d/\mathbf{Q}) = r$ *is*

$$\prod_{i=0}^{\infty}(1 - 2^{-2i-1}) \frac{2^{r-1}}{\prod_{i=1}^{r}(2^i - 1)}$$

Corollary

With E *as above,*

- *the proportion of* d *with* $\mathrm{rank}(E_d(\mathbf{Q})) = 0$ *is at least* $.2$
- *if BSD holds, then the proportion of* d *with* $\mathrm{rank}(E_d(\mathbf{Q})) = 1$ *is at least* $.4$

Selmer groups of twists

Theorem (Mazur & Rubin 2010)

Under mild hypotheses on E (hypotheses that remain valid if we replace E by one of its quadratic twists),

- *there are many primes $\pi \in \mathcal{O}_K$ such that*
$$s(E_\pi/K) = s(E/K) + 1,$$
- *there are many primes $\pi \in \mathcal{O}_K$ such that*
$$s(E_\pi/K) = s(E/K),$$
- *if $s(E/K) \geq 1$, then there are many primes $\pi \in \mathcal{O}_K$ such that*
$$s(E_\pi/K) = s(E/K) - 1.$$

("many" means a positive proportion)

Selmer groups of twists

Apply this inductively (the twist of a twist is again a twist)...

Corollary

Under mild hypotheses on E, for every $r \geq 0$ there are many d such that $s(E_d/K) = r$. In particular:

- *there are many d with $\mathrm{rank}(E_d(K)) = 0$,*
- *if BSD holds, then there are many d with $\mathrm{rank}(E_d(K)) = 1$.*

Selmer groups of twists

Theorem

Suppose that L/K is a Galois extension of number fields of prime degree, and E is an elliptic curve over K satisfying (the usual) mild hypotheses.

- *If $s(E/L) > s(E/K)$, then there are primes $\pi \in \mathcal{O}_K$ such that*

$$s(E_\pi/L) - s(E_\pi/K) = s(E/L) - s(E/K) - 1.$$

- *If $s(E/L) = s(E/K) > 0$ then there are primes $\pi \in \mathcal{O}_K$ such that*

$$s(E_\pi/L) = s(E_\pi/K) = s(E/K) - 1.$$

- *If $s(E/L) = s(E/K)$ then there are primes $\pi \in \mathcal{O}_K$ such that*

$$s(E_\pi/L) = s(E_\pi/K) = s(E/K) + 1.$$

Selmer groups of twists

Corollary

Suppose that L/K is a Galois extension of number fields of prime degree, and E is an elliptic curve over K satisfying (the usual) mild hypotheses. Then E has many quadratic twists E_d such that

$$s(E_d/L) = s(E_d/K) = 1,$$

and if BSD holds,

$$\mathrm{rank}(E_d(L)) = \mathrm{rank}(E_d(K)) = 1.$$

Elliptic curves and Hilbert's Tenth Problem

Karl Rubin, UC Irvine

MAA @ UC Irvine
October 16, 2010