TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Homi Bhabha Road, Bombay 400 005

School of Mathematics 7 January 1988

# NOTICE

Professor D. Zagier of Max Planck Institut fur Mathematik, West Germany and University of Maryland, USA, will give a course of lectures on 'Elliptic curves' on Wednesdays and Fridays from 4.00 p.m. to 5.45 p.m. in the Lecture Room AG-77 of the Institute. However, the first two lectures will be given in room No. AG 69 and these will be in the nature of a survey and are meant to be comprehensible to mathematicians without any special background in Number theory. The first lecture will be given on Tuesday, 12 January at 4.00 p.m.

SECRETARY
SCHOOL OF MATHEMATICS

kps

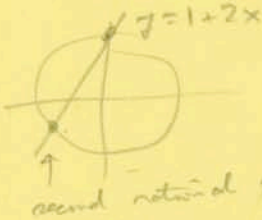
Zagier, Elliptic curves, 1/12/88

Historical overview

Diophantos, 150 A.D. ± 100, lived 84 years, Alexandria, book Arithmetica in 13 vols., copy discovered in 1570, studied by Fermat 100 years later. First books: linear eq'ns, introduced algebraic notations + equations + negative numbers.

Quadratic equations: To solve $x^2+y^2=1$. Method: Take particular sol'n $x=0, y=1$. Choose straight line solution $y=1+2x$, $x^2+(1+2x)^2=1$, $5x^2+4x+1=1$, $5x+4=0$, $x=-\frac{4}{5}$, $y=-\frac{3}{5}$, nontrivial solution. Effectively $y=1+tx$ works for $t$ rational. These eq'ns are always solvable in so many ways, and there is a parametric solution (if there is some solution).

Modern point of view – rational curve. Essentially




(real point of view – Newton)

Over $\mathbb{C}$, we get Riemann sphere. Rational curve is an eq'n whose complex sol'ns give Riemann sphere.

Cubic eq'ns. – example from Diophantos. Problem: Given a number (6), divide it into 2 pieces whose product is a cube diminished by its root. Use $y, 6-y$. Want $y(6-y)=x^3-x$. $y=0$, $x=-1$ is solution, $x=2y-1$. Substitute $6y-y^2=(2y-1)^3+(2y-1)=8y^3-12y^2+4y$. Divide by $y$. Quadratic eq'n with rational root. Change 4 (2× choice) to match 6. $x=3y-1$. But $6y-y^2=27y^3-27y^2+6y$, $27y=28$, $y=\frac{28}{27}$, $x=3y-1=\frac{19}{9}$. Still a systematic method.

Newton: Geometric context


Rotate lines to be tangent but double rational sol'n. So near solution is rational.

Iterate to get as many. Need to say they are "growing". Denom get bigger. "Height" = measure of this. Need a notion of this more generally.

Siegel. Cubic + certain quartics — elliptic curves. Result: There is a systematic method to generate new solutions from old. So after ∞ many solutions systematically, but not given by parametric families. Actually can be parametrized by elliptic fcns — conjecturally by modular fcns.

Fermat: 1601-1655 method of infinite descent — formalization of above, used in 2 different ways:
- show certain eq'ns have no solutions $x^4+y^4=z^4$
- solve certain eq'ns as above but more subtly

Problem posed to Mersenne (1643): Find an integer sided Pythagorean triangle


$(a^2+b^2=c^2)$ such that the hypotenuse = □ and sum of sides = □

Solution: $c = 4687298610289$

$a = 1061652293520$

$b = 4565486027761$

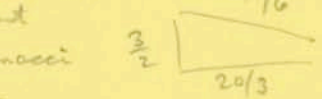
and this is the smallest solution.

Fibonacci (1225), Liber quadratorum, Ljubljana 1986.

Congruent numbers, had been studied in 984.

n is congruent if n is the area of a rational right triangle ⇔ ∃ 3 squares in arith. prog. with diff. n

1 ← not congruent (Fermat)
2 ← also not congruent
3 ←
5 — solved by Fibonacci
6 — congruent 3, 4, 5




$(3\frac{5}{12})^2, (2\frac{7}{12})^2, (4\frac{1}{12})^2$

(1, 25, 49)

Newton – geometric context as above

Poincaré – gave complex interpretation

rational – degree 1, 2 – corresponds to sphere $g=0$

elliptic – degree 3, some 4 – corresponds to torus $g=1$

general type (degree $\geq 5$) – seems to be no algorithm, $g \geq 2$.

Also Diophantus, Fermat method was turned out to give an addition for solutions


If P and Q are rational pts, so is R

Origin is at $\infty$. Degree $P+Q+R=0$.

$P+(-P)+0=0$ says symmetry gives $-P$.

So 

. This is a group operation (Poincaré), clearly abelian.

Conjecture (Poincaré about 1900). The group of rational solutions is finitely generated. Proved by Mordell ~ 1917.

Mordell conjecture (1917), proved by Faltings 1983. For a curve of general type (i.e., $g \geq 2$) has only finitely many rational solutions.

Mordell Weil – finitely generated

$E$ given by nonsingular $f(x,y)=0$, elliptic curve, all coefs in $\mathbb{Q}$.

$E$ is the eq'n. $E(\mathbb{Q})$ = set of rat'l solutions, possibly with $\infty$.

Similarly define $E(\mathbb{R})$, $E(\mathbb{C})$.

Weil $\Rightarrow$ grp is f.g. abelian $= \mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_r \oplus \underbrace{F}_{\text{finite abelian}}$, $F = \{Q_1, \ldots, Q_N\}$.

Questions:

1) What can $r$ be? $r$ = rank

2) What can $F$ be?

Answer: $r$ can be $0, 1, 2, 3, \ldots, 14$ (13 values) ^ maximum

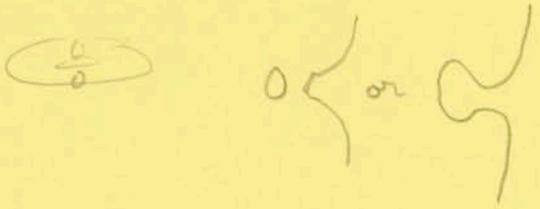
Néron $r \geq 9$ earlier.
$\geq 10$?
$\geq 11$??

Néron method: Write arbitrary cubic $ax^3 + bx^2y + \ldots + j$. Set equal to 9 points.

Usually 0 or 1. Until recently, experts thought $\geq 2$ was probably 0.

Computer check on $x^3+y^3=N$ suggests otherwise

Group $F$. $E(\mathbb{R}) \subseteq E(\mathbb{C})$ will be one or two circles.



$\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

So $F = C_n$ or $C_{2n} \times C_2$

Mazur $n = 1, 3 \to 10, 12$ and $n = 1, 2, 3, 4$ only.

Application: Fermat triples. $a, b, c$ distinct nonzero rational given.
Does there exist $x \neq 0$ such that $1+ax$, $1+bx$, $1+cx$ are $\square$ ?

Usually the answer is "yes". Only in special cases does this fail.

Theorem There are $\infty$ many $x$ unless

a) $1 = \sqrt{\frac{a}{c}} + \sqrt{\frac{b}{c}}$ with $\frac{a}{c} = \square$, $\frac{b}{c} = \square$ (e.g., 1, 4, 9)

b) $1 = \frac{a}{c} + \frac{b}{c}$ ? up to permutation

c) $1 = \sqrt{1-\frac{a}{c}} + \sqrt{1-\frac{b}{c}}$

d) $2 = \left(1+\sqrt{\frac{c-a}{b}}\right)\left(1+\sqrt{\frac{c-b}{a}}\right)$

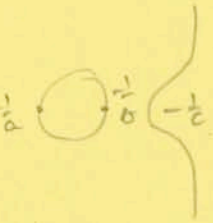
$3P=0$
$4P=0$
$6P=0$
$8P=0$

Proof. $y^2 = (1+ax)(1+bx)(1+cx) : E$

$T_1 : (-\frac{1}{a}, 0)$

$T_2 : (-\frac{1}{b}, 0)$

$T_1+T_2 : (-\frac{1}{c}, 0)$




Generalizations from $y^2 = Ax^3 + Bx^2 + Cx + D$ can make $A = 1$ (or 4), $B = 0$

$2T_1 = 0$, $2T_2 = 0$ - Get $C_2 \times C_2$ torsion

If $x=0$, get $P=(0,1)$. If $P$ is $\infty$ order, get $\infty$ many sol'n.

$nP = (x, y)$ for $n$ odd. Possibilities for $P$ of finite order:
$3P=0$, $4P=0$, $6P=0$, $8P=0$ by Mazur. Here are the cases in the theorem.

Q: show $1+ax$, etc. are squares later.

Birch - Swinnerton-Dyer: $r = \rho$ (defined later). (Get criterion for $r=0$, hence $E(\mathbb{Q})$ is finite.

Application to congruent numbers if conjecture true. We use Waldspurger Thm.

Small observed we get an answer: Assume $n$ is square-free.

$n$ even: Let $N_{\substack{\text{even}\\\text{odd}}}(n)$ = # sol'ns of writing $n$ as $a^2+b^2+c^2$, $c = 4\cdot\begin{smallmatrix}\text{even}\\\text{odd}\end{smallmatrix}$

$n$ odd: ---------- , $b+c = 4\cdot\begin{smallmatrix}\text{even}\\\text{odd}\end{smallmatrix}$

Example:) $n=3$. $3 = (\pm1)^2+(\pm1)^2+(\pm1)^2$, 8 ways.

$N_{even}(n) = 4$, $N_{odd}(n) = 0$.

If $n=157$. Then $N_{even}(n) = N_{odd}(n) = 0$ because $n \equiv 5 \bmod 8$.

Answer: $n$ is congruent (mod conjecture) $\Leftrightarrow N_{even}(n) = N_{odd}(n)$.

Actually $\Rightarrow$ is a theorem (Coates + Wiles)

Next time:
- descent
- heights
- Mordell's Thm.

More about the BSD conjecture:

Based on computer calculations

$E$ elliptic curve

$y^2 = x^3+5$ (maybe $r=0$)

$y^2 = 4x^3 - 28x + 25$ ($r=3$)

What about rank? Look for more solutions.

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | ... | -1 | -2 | -3 | then neg. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $4x^3-28x+25$ | 25 | 1 | 1 | 49 | 169 | 385 | | 49 | 49 | 1 | |

Idea: $E(\mathbb{Q}) \subseteq E(\mathbb{R})$ but also $E(\mathbb{Q}) \subseteq E(\mathbb{Q}_p)$ and then reduce to $E(\mathbb{Z}/p\mathbb{Z})$.

Study sol'ns mod $p$ for many $p$'s. This is a finite procedure.

Here $p \neq 2, 5077$. Let $N(p)$ = # sol'ns mod $p$, including $\infty$)

$1 \leq N(p) \leq 2p+1$

$x = 1, \ldots p$
$y^2 = f(x)$

$N(3) = 7$ (maximal)

$N(5) = 10$

$N(7) = 12$

$|p+1 - N(p)| \leq p$

Theorem (Hasse, 1932).

$$|p+1 - N(p)| < 2\sqrt{p}$$

so $N(p) \leq p+1 + [2\sqrt{p}]$.

| | |
|---|---|
| 2 | 5 |
| 3 | 7 |
| 5 | 10 |
| 7 | 12 |

Hence above $N(p)$'s are all maximal.

BSD conjecture (rough version). $\prod_{p \leq B} \frac{N(p)}{p} \sim \underset{\neq 0}{\text{const}} (\log B)^r$

Actual version: Define L series for $\mathrm{Re}(s) > \frac{3}{2}$ by

$$L(s) = \prod_p \frac{1}{1 - \frac{p+1-N(p)}{p^s} + \frac{p}{p^{2s}}}$$

($p \neq 2, 5077$ of this form)

Conjecture that $L(s)$ is entire. Let $\rho$ = order of vanishing at $s=1$.

Conjecture $r = \rho$.

$$\left[ \text{so } L(s) \text{ "}=\text{"} \prod_p \frac{1}{1 - 1 - \frac{1}{p} + \frac{N(p)}{p} + \frac{1}{p}} = \prod_p \frac{p}{N(p)} \right]$$

Definition of rank. Let $E$ = elliptic curve.

Thm. $\#\{(x,y) \in E(\mathbb{Q}) \mid \text{numerator + denominator of } x \text{ and } y \leq B\}$

$= \left(\underset{\neq 0}{\text{const}}\right)(\log B)^{r/2}$ for an integer $r$.

We let $r$ be the rank.

Plan:

Method of descent – two historical examples
– theory and another example

Notion of height – properties
– Mordell Theorem

## Method of descent

Theorem $x^4+y^4=z^2$ has no solutions.

Idea: If solution, get a smaller one. Method does not work directly for $x^4+y^4=z^4$.

Proof: WLOG $x, y, z$ are integers, $(x,y)=1$, $x$ odd, $y$ even.

$(x^2)^2+(y^2)^2=\square$. So $x^2=m^2-n^2$, $y^2=2mn$ with $(m,n)=1$.

$m^2=x^2+n^2$, $x$ odd. $m=p^2+q^2$, $x=p^2-q^2$, $n=2pq$, $(p,q)=1$.

$\square=\frac{1}{2}mn=pq(p^2+q^2)$. So each is a square. $p=\square$, $q=\square$, $p^2+q^2=\square$
(positive $>0$)

Hence $p=r^2$, $q=s^2$, $r^4+s^4=\square$. Backwards,

$(r,s)\to(p,q)=(r^2,s^2)\to(m,n)=(p^2+q^2,2pq)\to(x,y)=(p^2-q^2,\ 2rs\sqrt{r^4+s^4})$
$=(r^4-s^4,\ 2rs\sqrt{r^4+s^4})$

So $r^4-s^4=\square \rightsquigarrow (x,y)=(r^4-s^4,\ 2rs\sqrt{r^4+s^4})$, etc.

(Number of digits has gone up by factor of 4. This corresponds to doubling a point on an elliptic curve.)

Example 2: $\triangle$ with hypotenuse $z$, $x+y=a^2$, $z=b^2$, $x^2+y^2=z^2$. Get a solution.

Set $e=x-y$, $x,y=\frac{a^2\pm e}{2}$, $b^4=x^2+y^2=\frac{a^4+e^2}{2}$, $\boxed{2b^4-a^4=e^2}$

$x=m^2-n^2$
$y=2mn$
$b^2=z=m^2+n^2$
$a^2=x+y=(m+n)^2-2n^2$

$m=r^2-s^2$
$n=2rs$
$b=r^2+s^2$

$m=t^2-2tu+2u^2$
$n=2tu$
$(a=t^2-2u^2)$

Duplicates parametrization

$n = r$ says $rs = tu$, $\frac{r}{t} = \frac{u}{s} = \frac{d}{c}$, say, with $c > 0$, $(c,d) = 1$

$$\begin{aligned} r &= kd \\ t &= kc \\ u &= ld \\ s &= lc \end{aligned}$$

$$r^2 - s^2 = m = t^2 - 2tu + 2u^2$$

$$k^2d^2 - l^2c^2 = k^2c^2 + 2l^2d^2 - 2klcd$$

Divide by $k^2$

$$0 = (c^2 + 2d^2)\left(\frac{l}{k}\right)^2 - 2cd\left(\frac{l}{k}\right) + (c^2 - d^2), \text{ quadratic in } \left(\frac{l}{k}\right)$$

So this is soluble $\Leftrightarrow$

$$c^2d^2 - (c^2 + 2d^2)(c^2 - d^2) = \square$$

$$2d^4 - c^4 = \square, \text{ which is the original equation.}$$

This is much easier to do if there are no solutions. But there is a better one $d = 1, c = 1$.

$$3\left(\frac{l}{k}\right)^2 - 2\left(\frac{l}{k}\right) + 0 = 0$$

$\frac{l}{k} = 0$ gives nothing

$\frac{l}{k} = 0$ or $\frac{2}{3}$

So $l = 2$, $k = 3$.

$r = 3$
$t = 3$
$u = 2$
$s = 2$

$m = 5$
$n = 12$
$a = 1$
$b = 13$

$x = -119$
$y = 120$
$z = 169$
$e = -239$

$169^2 - 119^2 = 120^2$

This is the most basic solution.

Just do the whole thing again. We have seen from

$$2 \cdot 1^4 - 1^4 = 1^2$$

$$2 \cdot 13^4 - 1^4 = (239)^2$$

Thus $\frac{l}{k}$ is from $d = 13$, $c = 1$. But $\frac{l}{k} = \frac{13 \pm 239}{1 + 2 \cdot 169}$. $-$ gives $-\frac{2}{3}$, $+$ gives $\frac{84}{113}$

Else $\frac{l}{k} = -\frac{2}{3}$, $l = -2$, $k = 3$.

$r = 39$, $s = -2$, $t = 3$, $u = -26$

$m = 1517$, $n = -156$, $b = 155$, $a = -1343$

$x = 2276953$
$y = -473304$
$z = 2325625$

again a $-$ sign.

But $\frac{84}{113}$ works.

Why smallest? Original = poly of degree 4 in one var. Repeat. Have to get to very small solution. So get tree to recover matters

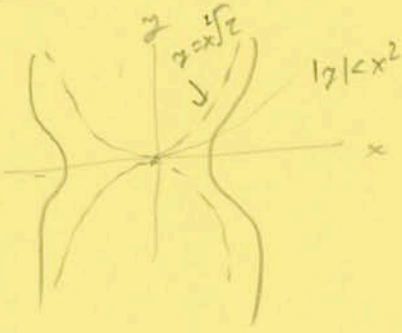
Height will formalize the notion of size.

Why did a > 0 solution have to occur

$2\left(\frac{b}{a}\right)^4 - 1 = \left(\frac{c}{a^2}\right)^4$ , $y^2 = 2x^4 - 1$ , $(x, y) \in \mathbb{Q}$.

This is equivalent

Graph




Condition for $x > 0, y > 0$.

$x, y = \frac{a^2 \pm c}{2} > 0 \iff |c| < a^2$

$\left|\frac{c}{a^2}\right| < \left(\frac{a}{2}\right)^2$

$|y| < x^2$

So we get a bounded open nonempty set.

If we have a dense set of $\infty$ order, rational point are dense in the component. So a solution exists with $x > 0, y > 0$.

Equation studied: $y^2 = x^4 + 1$

$y^2 = 2x^4 - 1$

Fact. $y^2 = f_4(x)$ or $y^2 = f_3(x)$ is an elliptic curve (if not rational)

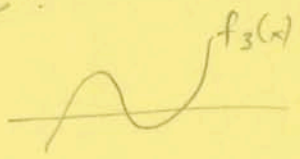
Conversely (by Weierstrass-Riemann-Roch) any elliptic curve is $y^2 = f_3(x) = x^3 + ax + b$ with $a, b \in \mathbb{Z}$.

This is not so easy. Finite birational substitutions.

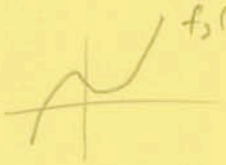
Discussion of $y^2 = f_3(x)$.

Assume 3 roots of $f_3(x)$ are $\mathbb{Q}$, say are in $\mathbb{Z}$.

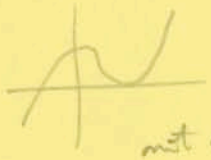
Pictures:




$\Delta > 0$




$\Delta < 0$



not elliptic curve

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

$$\Delta = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$$

$\Delta > 0$ give

$\Delta < 0$ give

$$E(\mathbb{R}) = \mathbb{R}/\mathbb{Z} \times C_2 \qquad E(\mathbb{R}) = \mathbb{R}/\mathbb{Z}$$

Rationality of roots: Those are the 2-torsion points

Now $E(\mathbb{Q})_{\text{torsion}} = C_{2m-1}$, $C_{2m}$ or $C_m \times C_2$

Mazur says $C_{2m-1}$, $1 \le m \le 5$

$C_{2m}$, $1 \le m \le 6$

$C_m \times C_2$, $1 \le m \le 4$.

Anyway $\{P \in E(\mathbb{Q}) \mid 2P = 0\} = \begin{cases} \{0\} & \leftarrow f_3(x) \text{ irred. over } \mathbb{Q}. \\ \{0, T\} & \leftarrow f_3(x) = \text{linear} \times \text{irred. quadratic} \\ \{0, T_1, T_2, T_3\} & \leftarrow f_3(x) = \text{linear} \times \text{linear} \times \text{linear} \end{cases}$

So we take just the last case. This is not really a loss, since it holds in an extension.

Recall $1+ax = \square$
$1+bx = \square$
$1+cx = \square$

$E: y^2 = (1+ax)(1+bx)(1+cx)$

$P = (0,1)$

$P' \equiv P \bmod 2E(\mathbb{Q}) \Rightarrow$ $(P' = P + 2Q)$

$1+ax(P') = \square$
$1+bx(P') = \square$
$1+cx(P') = \square$

Write eq'n as $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, $\alpha, \beta, \gamma \in \mathbb{Q}$, distinct

Claim: $P' \equiv P \bmod 2E(\mathbb{Q}) \implies x' - \alpha = (x-\alpha)\square$ and similarly for $\beta, \gamma$.

Better claim: $E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \{\pm 2^a 3^b 5^c 7^d \cdots \mid a,b,c,\ldots \in \{0,1\}\}$

$$= \bigoplus_{\infty,2,3,5,7,\ldots} (\mathbb{Z}/2\mathbb{Z}).$$

Map is $P = (x,y) \longrightarrow (x-\alpha)\mathbb{Q}^{\times 2}$ except for $x = 0, \alpha$

$$(\alpha, 0) \longrightarrow (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{\times 2}$$

$$(\infty) \longrightarrow \mathbb{Q}^{\times 2}$$

Claim this map is a group homomorphism.

If so, $P' \equiv P \Rightarrow P' = P + 2Q$. And $2Q \to 0$ under this.

So $x-\alpha$ and $x-\alpha'$ are the same up to square.

Proof of claim: We must show $P_1 + P_2 + P_3 = 0$ implies

$(x_1-\alpha)(x_2-\alpha)(x_3-\alpha) = \square$ (ignore exceptional cases)


$P_i = (x_i, y_i)$ lies on $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$

$y = \lambda x + \mu$

Thus the polynomial $(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2$

vanishes for $x_1, x_2, x_3$. So they are the only roots.

So it is $(x-x_1)(x-x_2)(x-x_3) = (x-\alpha)(x-\beta)(x-\gamma) - (\lambda x+\mu)^2$

Put $x = \alpha$. $-(\lambda\alpha+\mu)^2 = (\alpha - x_1)(\alpha - x_2)(\alpha - x_3)$ QED

**Theorem.** Let $E$ be $y^2=(x-\alpha)(x-\beta)(x-\gamma)$. We have the map

$E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ given generally by $P=(x,y) \to (x-\alpha)\mathbb{Q}^{\times 2}$

Form $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ with $\alpha,\beta$.

Then the map is injective.

Idea. Imagine $(x_3,y_3)$

$x_3-\alpha=\square^2$, $x_3-\beta=b^2$, $x_3-c=c^2$

Want $P_1=P_2$, $P_1+P_2+P_3=0$. Solve. (Egenic.)

To simplify the image:

$$(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2 = \bigoplus_{\infty,2,3,5,7,\dots} (C_2\times C_2)$$

Fix $p$. $p^a \| x-\alpha$, $p^b \| x-\beta$, $p^c \| x-\gamma$, $a+b+c\equiv 0 \ (2)$.

divide evenly

Say $\alpha,\beta,\gamma \in \mathbb{Z}$ (WLOG)

$p^a \| x-\alpha$, $a<0 \Rightarrow p^{|a|} \|$ denom of $x$ via $\alpha\in\mathbb{Z}$

So $p^a \| x-\alpha, x-\beta, x-\gamma$. $a=b=c$, $a+b+c\equiv 0 \ (2)$

$a\equiv b\equiv c\equiv 0 \ (2)$.

If $p$ in denom, image is $(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^2$ is 0.

$p^a \| x-\alpha$, $a>0$. Then $\begin{cases} p\nmid x-\beta \text{ if } p\nmid \alpha-\beta. \\ p\nmid x-\gamma \text{ if } p\nmid \alpha-\gamma. \end{cases}$

$\Rightarrow b=c=0$ if $p\nmid \Delta=(\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2$

= integer polynomial in coeffs of $f_3$

$f_3=x^3+ax+b$, $a,b\in\mathbb{Z}$

$\Delta=-(4a^3+27b^2)$

$\Rightarrow a$ even

Assume: $p \nmid \Delta \Rightarrow a=b=c \le 0$ or $a>b=c=0$ } all even.

**Result:** $\delta : E(\mathbb{Q})/2E(\mathbb{Q}) \to \prod_{\pm 1,\, p\mid\Delta} (C_2 \times C_2)$ is injective.

We can improve this. Call $p$ fairly bad if $p \mid$ one of $\alpha-\beta, \alpha-\gamma, \beta-\gamma$, exactly.

Call $p$ very bad if $p \mid$ all three. Call $p$ good if $p \nmid \Delta$.

$y^2 = f_3(x)$. Bad primes are ones where reduction mod $p$ makes curve become rational. Improvement is that the image is in

$$\bigoplus_{\substack{p \text{ fairly} \\ \text{bad}}} C_2 \;\oplus\; \bigoplus_{\substack{p \text{ very} \\ \text{bad}}} (C_2 \times C_2) \oplus \text{"(-1) part"}$$

**Corollary.** $|E(\mathbb{Q})/2E(\mathbb{Q})| \le 2^{m_1+2m_2+1}$

$m_1 = \#$ of fairly bad primes

$m_2 = \#$ of very bad primes

[The +1 here comes from prime $-1$. Invariant is # of negatives $x-\alpha, y-\beta, z-\gamma$.

$\delta$ possibilities. But product $= \square$. Now $\alpha, \beta, \gamma$ are real. So

$x-\alpha > x-\beta > x-\gamma \Rightarrow +++, +--$ $\quad \alpha \; \beta \; \gamma \{ \; . \; ]$ ]

**Corollary** If $E(\mathbb{Q})$ is finitely generated, with

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus C_{2^n} \oplus C_2 \quad \text{for some } n \ge 1,\ r \ge 0,$$

then $r \le m_1 + 2m_2 - 1$.

Proof. $E/2E = (\mathbb{Z}/2\mathbb{Z})^r + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$ and use above.

Remaining example of descent: Case of congruent numbers, $p$ odd prime.

$p$ congruent $\Leftrightarrow$ 3 squares in arithmetic progression, difference $p$.

$$x = \square, \quad x-p = \square, \quad x+p = \square$$

Yes, $y^2 = x(x-p)(x+p)$. If there is some $x$, we double out each factor is a square.

$\Delta = 4p^6$. Bad primes are $2, p$.

Here 2 is fairly bad, $p$ is very bad.

So $n \leq 2$. Actually more careful descent gives $n \leq \begin{cases} 2 & \text{if } p \equiv 1 \ (8) \\ 0 & 3 \ (8) \\ 1 & 5,7 \ (8) \end{cases}$

$$\begin{array}{l} x \\ x-p \\ x+p \end{array} \left( \begin{pmatrix} + & 1 & - \\ + & & - \\ + & & + \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & p & p \\ 1 & p & 1 & p \\ 1 & p & p & 1 \end{pmatrix} \times \text{squares} \right.$$

at $\infty$ — all ways

16 possibilities a priori

So reduce this further for certain $p$.

Here $(0,0)$, $(p,0)$, $(-p,0)$ on curve, torsion.

$$\left.\begin{array}{l} x = -\square \\ x-p = -p\square \\ x+p = p\square \end{array}\right\} \text{ gives } \begin{pmatrix} - \\ - \\ + \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ p \\ p \end{pmatrix}$$

$$\begin{array}{l} x = p\square \\ x-p = 2\square \\ x+p = 2p\square \end{array} \qquad \begin{pmatrix} + \\ + \\ + \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} p \\ 1 \\ p \end{pmatrix}$$

After possibly replacing $p$ if necessary by $p+T_1$, $p+T_2$, $p+T_3$,

where $T_1 = (0,0)$, $T_2 = (p,0)$, $T_3 = (-p,0)$ (2-torsion),

there are 4 possibilities

$$\begin{array}{llll} x = \square & x = -\square & x = \square & x = -\square \\ x-p = \square & \text{or} \quad x-p = -\square & \text{or} \quad x-p = 2\square & \text{or} \quad x-p = -2\square \\ x+p = \square & x+p = \square & x+p = 2\square & x+p = 2\square \end{array}$$

So $n \leq 2$.

Consider $x = -\square$

$x - p = -\square$ . Then $2p = \square + \square$, $p \equiv 1 \ (4)$ , $p \equiv 1 \text{ or } 5 \ (8)$

$x + p = \square$

$x = \square$

$x - p = 2\square$ $\Big\}$ $p = 2\square - \square \Rightarrow p \equiv 1 \text{ or } 7 \ (8)$

$x + p = 2\square$

$x = -\square$

$x - p = -2\square \Rightarrow p \equiv 1 \ (8)$

$x + p = 2\square$

If $p \equiv 3 \bmod 8$, get just $\{0\}$, so $r = 0$

$p \equiv 5 \bmod 8$, get $r \leq 1$.

Take $p \equiv 5 \bmod 8$. Is $p$ always congruent ? (Unknown but conjectural)

Examples: 5, 157 congruent.

Idea of calculation = smallest solution (often adding 2 torsion point)

may be assumed of form $x = -a^2$ (1)

$x - p = -b^2$ (2)

$x + p = c^2$ (3)

From (2) and (3), $c^2 - b^2 = -2a^2$ : parametrize as $a = 2rs \cdot \lambda$

$b = (r^2 + 2s^2) \cdot \lambda$

$c = (r^2 - 2s^2) \cdot \lambda$

Then $(r, s) = 1$, $\lambda \in \mathbb{Q}$. Then $\lambda = \frac{1}{n}$.

Next $p = c^2 + a^2 = (r^4 + 4s^4)\lambda^2$

To solve $r^4 + 4s^4 = pn^2$.

| $p$ | $r$ | $s$ | $m$ | $a$ | $b$ | $c$ | $x$ | $x-5$ | $x+5$ | the double |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | 1 | 1 | 2 | 3 | −1 | −4 | −9 | 1 | |
| 13 | 1 | 3 | 5 | | | | | | | |
| 29 | 7 | 5 | 13 | | | | | | | |
| 37 | 1 | 21 | 145 | | | | | | | |
| 53 | more for a long way | | | | | | | | | |
| 61 | 41 | 39 | 445 | | | | | | | |

101 Lagr

Now once again $r^4 + 4s^4 = pm^2$

$$\left(\frac{r^2}{m}\right)^2 + \left(\frac{2s^2}{m}\right)^2 = p. \qquad p = x^2 + y^2$$

$7^2 + 2^2 = 53$. Diophantos, etc.

and set $r^2 = 7a^2 + 4ab - 7b^2$

$s^2 = a^2 - 7ab - b^2$

$$a = \lambda^2 + n^2$$

$$b = 2\lambda n - 7n^2$$

$$\Rightarrow s = -\lambda^2 + 7\lambda n + n^2$$

Search in $\lambda$ and $n$ on computer. $n = 3$, $\lambda = 10$.

Then $s = 119$, $r = 286$, $4 \cdot 119^4 + 286^4 = 53 \cdot \square$

$\square = 11890^2$

$\Leftrightarrow E(\mathbb{Q})_2 = C_2 \times C_2$

Review

$E$ elliptic curve $/\mathbb{Q}$. Standard form $y^2 = x^3 + ax^2 + bx + c = (x-\alpha)(x-\beta)(x-\gamma)$.

Exercise: $a^3 + b^3 = c^3$, Weierstrass normal form $y^2 = x^3 - 432$, $432 = 27 \cdot 16$

Note in top curve $\alpha, \beta, \gamma \to \lambda^2\alpha, \lambda^2\beta, \lambda^2\gamma$ is okay. So $y^2 = x^3 - 432$ has 432 defined only up to a $6^{th}$ power. $y^2 = 4x^3 - 27$ is the case.

Solution $x = 12\,\frac{c}{a+b}$

$y = 36\,\frac{a-b}{a+b}$

Exercise: 1) $a^4 + b^2 = c^4$ $\leftarrow$ $y^2 = x^3 + 4x$

2) $a^4 + b^4 = c^2$ $\leftarrow$ $y^2 = x^3 - 4x$

3) $a^2 + b^2 = c^2$, $a+b = \square$, $c = \square$ $\Leftrightarrow$ $v^2 = 2u^4 - 1$, $y^2 = x^3 + 8x$.

Solution to third $(x, y) = \left( 2\,\frac{v + 2u^2 - 1}{(u-1)^2},\ 4\,\frac{(2u-1)v + 2u^3 - 1}{(u-1)^3} \right)$

Inverse $u = \frac{y - 2x - 8}{y - 4x + 8}$

4) No 4 squares in arith progression

$\Leftrightarrow y^2 = x^3 - 351x + 1890$ has rank 0.

Theorem $E(\mathbb{Q})/2E(\mathbb{Q})$ under our normalization and assumption is finite, of order $2^t$ with $t \le m_1 + 2m_2 + 1$, $m_1$ = # of $p$ dividing one of $\alpha-\beta, \alpha-\gamma, \beta-\delta$, $m_2$ = # of $p$ dividing all 3. Mp on $x \to (x-\alpha)(x-\beta) = (\ )\prod_{p \mid \Delta} p^{(p)}$ □

---

Height (in Silverman book)

Let $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.

Let $P = (x, y) \in E(\mathbb{Q})$, $x = \frac{p}{q}$, $(p, q) = 1$. Naive Height $h_0(P) = \log \max(|p|, |q|)$

$\ge 0$

Notice $P=0 \in E(\mathbb{Q})$ has $x=\infty$, $p=1, q=0$, $h_0(\infty)=1$.

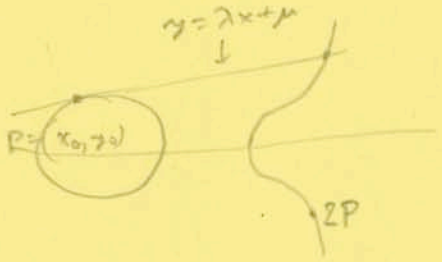
**Proposition 1.** $h_0(2P) = 4h_0(P) + O(1)$, where $O(1)$ is bounded independent of $P$ (actually a finite even if $E(\mathbb{Q})$ is infinite).

Note: (Cassels) there are only finitely many points $P$ with $h_0(P) \le C$.

Proof. Write $P^* = 2P$, $P=(x,y)$, $P^*=(x^*,y^*)$, $x^* = \frac{p^*}{q^*}$.

Claim $x^* = \dfrac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3+Ax+B)}$ (y not needed)

Picture




$\lambda = \left.\frac{\partial y}{\partial x}\right|_P$

$y^2 = x^3+Ax+B$

$2y\,dy = (3x^2+A)\,dx$

$\lambda = \dfrac{3x_0^2+A}{2y_0}$

Intersection of tangent with $E$:

$$y^2 = (\lambda x+\mu)^2 = x^3+Ax+B$$

This has 3 roots, $x_0, x_0, x^* = x(2P)$. $x^* + x_0 + x_0 =$ sum of roots

$$x^* = \lambda^2 - 2x_0 = \frac{(3x_0^2+A)^2}{4(x_0^3+Ax_0+B)} - 2x_0 \quad \text{as required for claim}$$

Write $x^* = \dfrac{P}{Q}$

$$P = p^4 - 2Ap^2q^2 - 8Bpq^3 + A^2q^4$$

$$Q = 4q(p^3 + Apq^2 + Bq^3)$$

Now let $\delta = GCD(P,Q)$. $p^* = P/\delta$, $q^* = Q/\delta$.

Have to be sure not just cancellation with signs or prime divisors.

Now $\max(|p^4|, |g^4|) \le \max(|P|, |Q|) \le C(A,B) \max(|p|,|g|)^4$ (*)

So $h_0(2P) \le$ const $+ 4 h_0(P)$. Here $C(A,B) = (|A|+1)^2 + 8|B| + 2$

$\log C(A,B)$

Recall $\Delta = -4A^3 - 27B^2 \neq 0$

Identities: $4\Delta g^7 = (3p^3 - 5Apg^2 - 27Bg^3)Q - 4(3p^2g + 4Ag^3)P$

$$4\Delta p^7 = -(A^2Bp^3 + (5A^4 + 32AB^2)p^2g + (26A^3B + 192B^3)pg^2 - 3(A^5 + 8A^2B^2)g^3)Q$$

$$-4((4A^3 + 27B^2)p^3 - A^2Bpg^2 + (3A^4 + 22AB^2)pg^2 + 3(A^3B + 8B^3)g^3)P$$

(These can be verified directly. Or we can take the coefficients as unknown and solve.)

Thus $\max(|p|,|g|)^7 \le C \max(|p|,|g|)^3 \cdot \max(|P|,|Q|)$

So this gives a reverse estimate for the second $\le$ in (*).

This is the archimedean part. For finite primes, the identities say $\delta$ divides $4\Delta p^7$, $4\Delta g^7$. So $\delta \mid 4\Delta$ and $\delta$ is bounded. QED

Define the actual Height (or canonical height) (or Neron-Tate height) to be

$$h(P) = \lim_{n\to\infty} \frac{h_0(2^n P)}{4^n}$$

Corollary to Prop. 1. There exists a unique function $h : E(Q) \to \mathbb{R}$ satisfying

(i) $h(P) - h_0(P)$ is bounded

(ii) $h(2P) = 4h(P)$

Proof. $h(P)=h$, $h(2^n P) = 4^n h$

$$\left| h_0(2^n P) - 4^n h \right| \le C$$

$$\left| h - \frac{h_0(2^n P)}{4^n} \right| \le \frac{C}{4^n}$$ shows uniqueness.

Existence is clear from the properties.

Corollary. $h(P) > 0$ unless $P$ is a torsion point.

(Note converse is clear.)

Proof. (i) above says only finitely many pts have $h(P) \le C$. If $P$ has $\infty$ order, $P, 2P, \dots$ have unbounded heights. So some $2^n P$ has height $> 0$.

By (ii), $h(P) > 0$.

Prop. 2. $h$ is a (positive definite) quadratic form on $E(\mathbb{Q})/\text{torsion}$ or $E(\mathbb{Q}) \otimes \mathbb{R}$.

Equivalently $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q)$ for all $P$ and $Q$.

I.e., there exists a positive definite symmetric bilinear form for $\langle P, Q \rangle$ on $\dots$ such that $h(P) = \langle P, P \rangle$.

Proof shortly.

Theorem (Mordell 1922). $E(\mathbb{Q})$ is finitely generated of rank $\le n_1 + 2n_2 - 1$.

Proof. Since $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, we have: For some (big) $C$, the set $S = \{ P \in E(\mathbb{Q}),\ h(P) \le C \}$ contains a representative for each class of $E(\mathbb{Q})/2E(\mathbb{Q})$. ($C$ is ineffective.) Now $S$ is finite. Claim $S$ generates $E(\mathbb{Q})$. In fact, let $P \in E(\mathbb{Q})$ be arbitrary. By definition $\exists Q \in S$ such that $P \equiv Q \bmod 2E(\mathbb{Q})$. By Prop 2, either $P+Q$ or $P-Q$ has height $\le h(P) + h(Q)$. Also $P \pm Q$ is twice a point.

$P \pm Q = 2P'$, $P' \in E(\mathbb{Q})$, $4h(P') = h(P \pm Q) \le h(P) + h(Q) \le h(P) + C <$ $2h(P)$. So $h(P') \le \frac{1}{2} h(P)$. So $P = 2P' \pm Q$, $h(P') \le \frac{1}{2} h(P)$, $Q \in S$. Iterate to get $P'''' \dots$ in $S$.

Proof of Prop 2: First we show

$$h(P+Q) + h(P-Q) \le 2h(P) + 2h(Q) \qquad (*)$$

Applying this to $P' = P+Q$, $Q' = P-Q$ gives the reverse inequality since $h(2P) = 4h(P)$. To prove $(*)$, it is enough to prove

$$h_0(P+Q) + h_0(P-Q) \le 2h_0(P) + 2h_0(Q) + O(1).$$

Let the points be $P$ and $P'$. Write $P = (x, y)$, $x = \frac{p}{q}$, $P' = (x', y')$, $x' = \frac{p'}{q'}$.

$x_\pm = x(P \pm P')$. We compute this in the same style as in the special case earlier. The result is

$$x_\pm = x(P+Q) = \left(\frac{y' \pm y}{x' - x}\right)^2 - x - x'$$

Then $$x_+ + x_- = 2\,\frac{xx'(x+x') + A(x+x') + B}{(x-x')^2}$$

$$x_+ x_- = \frac{(xx' - A)^2 - 4B(x+x')}{(x-x')^2}$$

If $|p| = |\mathrm{num}(x)|$ and $|q| = |\mathrm{den}(x)|$ are $\le M$ and similarly for $p', q'$, then $x_+ + x_- = \frac{Q}{S}$, $x_+ x_- = \frac{R}{S}$ with $|Q|, |R|, |S| \le \mathrm{Const}\, M^2 M'^2$

Now $x_+$ and $x_-$ are roots of $Sz^2 - Qz + R = 0$ with both roots rational.

Then it follows that $|\mathrm{num}(x_\pm)|, |\mathrm{den}(x_\pm)| \le \mathrm{const}\, M^2 M'^2$ (exercise)

Actually it follows that $\log \max(|p_+|, |q_+|) + \log \max(|p'_+|, |q'_+|)$

$$\le O(1) + 2h(P) + 2h(Q).$$

Common factors can be seen to divide $\Delta$.

We now know $E(\mathbb{Q}) = \mathbb{Z}^r \oplus C_{2m} \oplus C_2$ with $r+2 \le n_1 + 2n_2 + 1$. So we get the bound on the rank.

Second version: $\#\{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 + Ax + B \text{ with } |\mathrm{num}\, x|, |\mathrm{den}\, x| \le T\} \sim \underset{\neq 0}{\mathrm{const}} (\log T)^{\frac{r}{2}}$

as $T \to \infty$

Prop. If $Q$ is a torsion pt, $h(P+Q) = h(P)$ (easy). So $h$ is defined on $E(\mathbb{Q})/\text{tors}$. Write

$$E(\mathbb{Q}) = \mathbb{Z}P_1 + \cdots + \{Q_1, \ldots, Q_s\}$$

$$P = m_1 P_1 + \cdots + m_r P_r + Q_i$$

$$h(P) = \sum c_{ij} m_i m_j \quad \text{where } (c_{ij}) = C \text{ is pos def symmetric of size } r.$$

The est in the statement is

$$\simeq \{P \mid h_0(P) \le \log T\} \subseteq \{P \mid h(P) \le \log T + \text{const}\}$$

$$\subseteq \{P \mid h(P) \le \log T - \text{const}\}.$$

So $\#\{P \mid h(P) \le t^2 = \log T\} = S \cdot \#\{(m_1, \ldots, m_r) \in \mathbb{Z}^r \mid \sum c_{ij} m_i m_j \le t\}$

$\cdot$ (fixed ellipsoid scaled by $\sqrt{t}$). So we get $S \cdot ct^{\frac{r}{2}} + \text{much smaller}$. Etc.

Formula that results: $C_r$ = vol. of $r$ ball $= \frac{\pi^{r/2}}{(r/2)!}$.

$$\#\{P \in E(\mathbb{Q}) \mid h_0(P) \le \log T\}$$

$$= |E_{\text{tors}}| \cdot C_r \cdot R^{-\frac{1}{2}} (\log T)^{\frac{r}{2}} + O(\log^{\frac{r-1}{2}} T)$$

where $R$ = regulator $= \det \langle P_i, P_j \rangle_{i,j=1,\ldots,r}$.

Numerical example: $y^2 = 4x^3 - 28x + 25$, $r = 3$.

$P_1, P_2, P_3 = (0,2), (1,0), (2,0)$

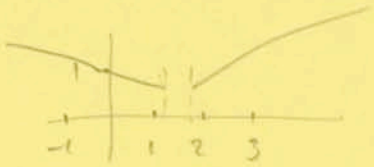
$E(\mathbb{Q}) = \mathbb{Z}P_1 + \mathbb{Z}P_2 + \mathbb{Z}P_3$.

$$\langle P_i, P_j \rangle = \begin{pmatrix} .9909 & -.2365 & -.2764 \\ -.2365 & .6682 & .0333 \\ -.2764 & .0333 & .7670 \end{pmatrix}$$

$R = .41714355\ldots$ Numbers are highly computable.

Recipe for height in this curve.

Let $P=(x,y)$ solve $y^2+y = x^3-7x+6$, $x = \frac{p}{q}$ coprime, $q>0$

$F(x)$: 


Theorem: $h(P) = \log q + F(x)$. Here $F(x) = \log x + O(1)$

This makes $h(P) - h_0(P)$ bounded

To get $h(2P) = 4h(P)$, use $F(x) = \log|x| + \sum_{m=0}^{\infty} \frac{\log z_m}{4^{m+1}}$

$x_0 = x$

$x_{m+1} = \dfrac{x_m^4 + 14x_m^2 - 50x_m + 49}{4x_m^3 + 28x_m + 25}$ (x coordinate of double)

$z_m = 1 + \frac{14}{x_m^2} - \frac{50}{x_m^3} + \frac{49}{x_m^4}$

No cancellation - uses 5077.

Zagier, 1/20/88

## $\mathbb{C}$ - theme

So far we have worked over $\mathbb{Q}$.

Another thing is to look at extension $\mathbb{Q} \to K \subseteq \overline{\mathbb{Q}}$. This was needed for a full proof of Mordell's Theorem.

Can pass to $\mathbb{R}$ or $\mathbb{C}$, to $\mathbb{Q}_p$, or to $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_q$. Need to study to various purposes.

Also might study $\mathbb{Z}$ solutions.

For the $\mathbb{C}$ theme, to consider elliptic functions and $\mathbb{C}/\text{Lattice} = E(\mathbb{C})$. Also to bring in modular forms. $\bar{\mathfrak{H}}/\Gamma_0(N) \to E(\mathbb{C})$.

Most important topics

1) Using the modular parametrization to understand the arithmetic of $E/\mathbb{Q}$.

2) Complex multiplication

Elliptic curves over $\mathbb{C}$.

Let $E/k$ be a curve of genus 1 with a $k$-rational point $O$

1) Weierstrass form (1st modification):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in k$$

If 2 and 3 are invertible, $y^2 = x^3 + ax + b = 4x^3 - g_2x - g_3$.

(Proof uses Riemann-Roch)

2) $(E(k), O)$ is an abelian group. $p_1 + \cdots + p_n = 0 \Leftrightarrow$ $p_1 + \cdots + p_n - n(O)$ is a principal divisor (exists global fct.)

$E(\mathbb{C})$ is a torus $= \mathbb{C}/L$, $L$ has generators $\omega_1, \omega_2$. $L$ and $\lambda L$ give the same $E$ if $\lambda \in \mathbb{C}^\times$. So may assume $\omega_1 = 1$, $\omega_2 = \tau$.

Write $E = E_\tau = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$ $(\tau \in \mathfrak{H})$

$E_\tau \cong E_{\tau'} \iff \tau' = \frac{a\tau+b}{c\tau+d}$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Easy proof.

Classification

$$\left\{ \begin{matrix} \text{elliptic curves} \\ \text{over } \mathbb{C} \end{matrix} \right\}/\cong \quad \overset{1\text{-}1}{\longleftrightarrow} \quad \mathfrak{H}/SL_2(\mathbb{Z})$$

$$E_\tau \longleftrightarrow \tau.$$

$$E \longrightarrow j(E) \in k^\times, \quad j(E) = \frac{\text{poly of degree } 12 \text{ in } a_1, \dots, a_6}{\Delta \text{ (degree } 12 \text{ in } a_1, \dots, a_6)}$$

in such a way that $E \cong E' \Rightarrow j(E) = j(E')$

If $y^2 = x^3 + ax + b$,

$$j = \frac{4a^3}{4a^3 + 27b^2} \cdot 1728$$

If $k = \bar{k}$, $j(E)$ is a complete invariant. We set

$$E_\tau \longleftrightarrow \tau$$

$$j \searrow \quad \swarrow j(\tau)$$

$$\text{analytic} \quad \mathbb{C}$$

$$j(\tau) = e^{-2\pi i \tau} + 744 + 196884 e^{2\pi i \tau}$$

$$= \frac{E_4(\tau)^3}{\Delta(\tau)},$$

$$\Delta(\tau) = q \prod_1^\infty (1-q^n)^{24}$$

$$q = e^{2\pi i \tau}$$

$$\mathbb{C}/L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

$$E_4(\tau) = 1 + 240 \sum_1^\infty \frac{n^3 q^n}{1-q^n}$$

Weierstrass model

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

$\wp(z)$ has a double pole at $\omega \in L$.

$\wp'(z)$ has a triple pole at $\omega \in L$.

$$\wp(z+\omega) = \wp(z), \quad \omega \in L$$

$p'(z)^2 = 4p(z)^3 - g_2 p(z) - g_3$ has no poles for

discriminate $g_2$ and so is const

So we get a map

$$\mathbb{C}/L \to \{(x,y) \mid y^2 = x^3 + ax + b\}$$

under $z \to (p(z), \frac{1}{2}p'(z))$

So $E(\mathbb{C}) = \mathbb{C}/L$, both of {holomorphic differentials locally $f(z)dz$}.

$$= \mathbb{C}\,dz$$

If $\omega$ is such, then $\{\int_\gamma \omega \mid \gamma = \text{closed curve in } E(\mathbb{C})\}$

$$\int_0^\omega dz = \omega \in L.$$

So $\mathbb{C}/\{\int_\gamma \omega\} = \mathbb{C}/L$

In particular if $y^2 = x^3 + ax + b$

$$2y\,dy = (3x^2 + a)\,dx$$

$y$ and $3x^2+a$ cannot both vanish. So

$$\frac{dy}{3x^2+a} = \frac{dx}{2y} = \omega \text{ is a holo diff.}$$

Pass to $\{\int \omega\}$.

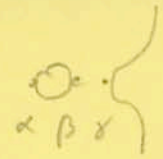
Arithmetic-geometric mean (arithmetic mean) of basis

$a, b > 0$, $M(a,b) = \lim a_n = \lim b_n$ where

$$(a_0, b_0) = (a, b)$$

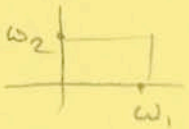
$$(a_i, b_i) \to (a_{i+1}, b_{i+1}) = \left(\frac{a_i + b_i}{2}, \sqrt{a_i b_i}\right)$$

$a_0 > a_1 > \dots > b_2 > b_1 > b_0$ rapidly convergent

Example. Over $\mathbb{R}$ 


$$y^2 = (x-\alpha)(x-\beta)(x-\gamma).$$

$$\omega_1 = \int_\gamma^\infty \frac{dx}{\sqrt{(x-\alpha)(x-\beta)(x-\gamma)}}$$

Here other period is $\int_\alpha^\beta$ and is imaginary. 


Theorem (Gauss). $\omega_1 = \dfrac{\pi}{M(\sqrt{\gamma-\alpha}, \sqrt{\gamma-\beta})}$

Idea: $a = \sqrt{\gamma-\alpha}$, $b = \sqrt{\gamma-\beta}$

$\sqrt{x-\gamma} = a\tan\theta$. Integral $\rightsquigarrow$ $2\int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2\sin^2\theta + b^2\cos^2\theta}} = I(a,b)$.

Need this $= \frac{\pi}{2} M(a,b)^{-1}$

Just show $I(a,b) = I\left(\frac{a+b}{2}, \sqrt{ab}\right)$ by making the substitution

$$\sin\theta \rightarrow \frac{2b\sin\theta}{a+b+(b-a)\sin^2\theta}$$

So $I(a_1,b_1) = I(a_2,b_2) = \cdots = I(M,M) = \dfrac{\pi/2}{M}$

↑ by direct calculation

Numerical example: E: $y(y-1) = (x+1)x(x-1)$

Weierstrass $y_1^2 = 4x^3 - 4x + 1$ where $y_1 = 2y-1$

$j$-invariant $\quad$ or $x^3 - x + \frac{1}{4}$

$\hookrightarrow = \dfrac{2^{12}3^3}{37}$. $\quad \Delta = 37$ for original

Roots of $4x^3 - 4x - 1 = 0$: $\quad \alpha = -1.107\ldots$
$\beta = .2695\ldots$
$\gamma = .8395\ldots$

$$\omega_1 = \int_\gamma^\infty \frac{dx}{\sqrt{4x^3-4x+1}} = 2.9934586 44\ldots \text{ from above}$$

$$\omega_2 = 2\int_\rho^\gamma \cdots = 2.45138938 1\ldots\, i$$

So $E(\mathbb{C}) = \mathbb{C} \Big/ \{2.99\ldots, 2.45i\}$

$$g_2 = 60 \sum_{\substack{\omega \in \Omega \\ \omega \neq 0}} \frac{1}{\omega^4}$$

Write $L = \omega_2 \cdot \underbrace{\left(\mathbb{Z} + \mathbb{Z}\left(\frac{-\omega_1}{\omega_2}\right)\right)}_{\tau}$

$$= \frac{4\pi^4}{3\omega_2^4}\left(1 + \sum_{m=1}^{\infty} \frac{240\, m^3}{e^{2\pi i m \omega_1/\omega_2} - 1}\right) = 4.000\ldots$$

rapidly convergent $= 4$

Finally $g_3 = 140 \sum \omega^{-6} = \frac{8\pi^6}{27\omega_2^6}\left(1 - \sum \frac{504\, m^5}{e^{2\pi i m \omega_1/\omega_2} - 1}\right) = -1.00\ldots$

Application

Poncelet's theorem. Take two ~~conics~~ ellipses 

. Starts tangents as in picture. Suppose this closes for the first point in $n$ steps. Then it closes in $n$ steps independently of the starting point.

Proof: Inner $= C$, outer $= C'$. $E = \{(c, c') \in C \times C' \mid$ ~~that through~~ $c$ goes through $c'\}$.

Then $E \xrightarrow[\tau]{2:1} C$. So $\tau : (c, c') \to (c, c'$ second$)$

$2:1 \downarrow \tau'$ $\quad \tau' : (c, c') \to (c$ second$, c')$

$C'$

Map is $\tau\circ\tau'$. Question is that if $(\tau\circ\tau')^n$ has a fixed point, then $(\tau\circ\tau')^n = 1$. Now $E$ is an elliptic curve.

$E \xrightarrow{\pi} \mathbb{C}$ double cover of $S^2$ with ramification at 4 pts.
is a torus

Consider $E \xrightarrow{\tau} E$ with 4 fixed points, $E = \mathbb{C}/L$ is $x \to a - x$, $a \in \mathbb{C}$.

Similarly $\tau'$ is $a' - x$. $\tau\circ\tau'$ is $(a - a') + x$.

$(\tau\circ\tau')^n$ is $n(a-a') + x$. QED

## Theorem, part 2

$E(\mathbb{C}) = \{(x,y) \in \mathbb{C}^2 \mid y^2 = x^3 + ax + b\}$

Part 1 said this can always be parametrized by elliptic functions $x = \wp(z)$
$y = \frac{1}{2}\wp'(z)$.

Part 2: $E(\mathbb{C})$ can sometimes be parametrized by $x = \xi(\tau)$, $y = \eta(\tau)$, $\tau \in \mathfrak{h}$,

$\xi\left(\frac{a\tau+b}{c\tau+d}\right) = \xi(\tau)$, $\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \eta(\tau)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ finite index in $SL_2(\mathbb{Z})$.

Here $\mathfrak{h}/\Gamma \xrightarrow{\text{onto}} E(\mathbb{C})$.

In one direction start with $\Gamma$. Say $\Gamma = SL_2(\mathbb{Z})$. Then $\mathfrak{h}/\Gamma \cong \mathbb{C}$ by $j$.

Hence $\mathbb{C}(\mathfrak{h}/\Gamma \cup \{\infty\}) = \mathbb{C}(j)$. Here $\bar{\mathfrak{h}}/\Gamma \cong \mathbb{P}^1$. In general $\Gamma$,
it is still true that any two fcns are alg. related.

Conjecture ("Weil - Taniyama"). If $E$ is defined over $\mathbb{Q}$, then there exists
a modular parametrization, and $\xi(\tau), \eta(\tau) \in \mathbb{Q}$ (fixed $q$, power series $q_\tau$),
$\eta(\tau)^2 = \xi(\tau)^3 + a\xi(\tau) + b$, $\xi(\gamma\tau) = \xi(\tau)$, $\eta(\gamma\tau) = \eta(\tau)$, $\gamma \in \Gamma_0(N)$,
$N$ = conductor of $E = \prod_{p \nmid \Delta} p^{f_p}$. (Corollary: If such parametrization, then this $\Gamma_0(N)$)

Corollary of conjecture (Ribet, Serre, Frey). Fermat's Last Theorem holds.

Geometry: $\mathbb{H}/\Gamma$ $X =$ 

$J(X) \to E$

$\|$

$J_0(N)$ ↗

Table.

| $N=$ | 1 | 2 | 3 | 10 | 11 | 12 | 37 |
|---|---|---|---|---|---|---|---|
| $\dim J_0(N)$ | 0 | 0 | 0 | 0 | 1 | 0 | 1 ⋯ 2 |

$= g(X_0(N))$

$= \dim S_2(\Gamma_0(N))$

$J_0(11) = X_0(11) = E$

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

For 37, we get a product up to

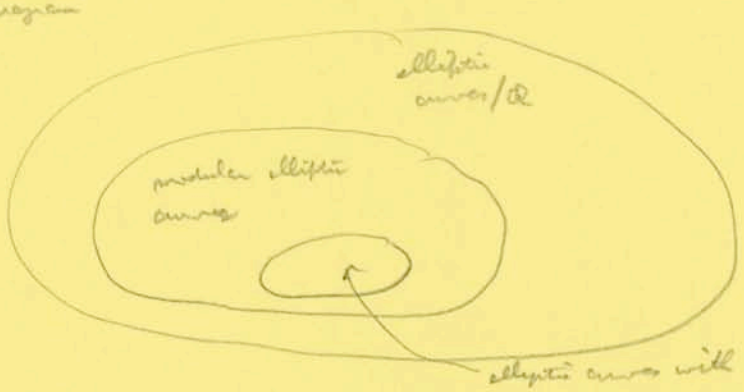
wrong: $y^2 - y = x^3 - x$ $\quad r=1$

$y^2 = x^3 + \cdots$ $\quad r=0$

Note: The conjecture will be decidable for any $E$.

True dependent statement: $\{ j(E) \mid$ conjecture is known for $E \}$ is finite.

Venn diagram




modular: $E$ is parametrized by modular forms

Each property depends only on $j(E)$.

Small set is known exactly: $\{j\} = \{0, 1728, -3375, 8000, 9$ more values$\}$ all integers

Big set: $\{j\} = \mathbb{Q}$ trivially

Weil-Taniyama: Middle = big. So middle has $\{j\} = \mathbb{Q}$. But we just know a few hundred points.

Frey's contribution (maybe known earlier)

$x^n + y^n = z^n$, $n \geq 3$ (maybe 7), counterexample (*)

Form $E_{(*)}$ $\quad y^2 = x(x-\alpha^n)(x-\beta^n)$. Differences of roots are $\alpha^n, \beta^n, \gamma^n$.

So $\Delta = (\alpha\beta\gamma)^{2n}$

Ribet's theorem: [$E_*$, (*) is a counterexample] is contained in big-modular.

$E/\mathbb{Q}$ given. $E$ is parametrized by modular functions $\Gamma_0(N)$, natural curves.

$N$ = conductor

$\Updownarrow$ Eichler-Shimura

$$L(E,s) = \prod_{p \nmid N} \frac{1}{1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}} \cdot \prod_{p \mid N} \frac{1}{1 - \frac{\varepsilon_p}{p^s}}$$

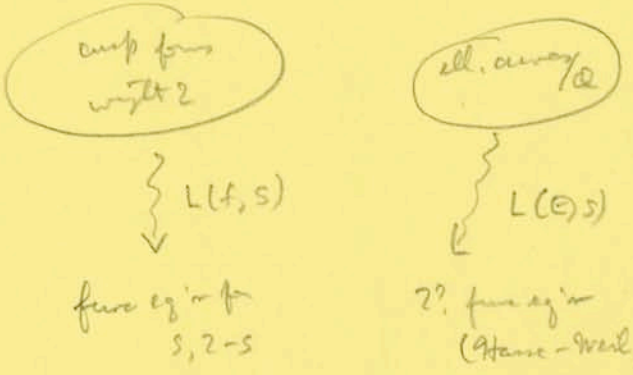
$a_p = p + 1 - \#E(\mathbb{F}_p)$, $\varepsilon_p = 0, 1, -1$

$$= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \Rightarrow \sum_{1}^{\infty} a_n e^{2\pi i n \tau} = f(\tau) \text{ is in}$$

$S_2(\Gamma_0(N))$

$\left(\Leftrightarrow f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau) \right.$

$\left. \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right)$




Expect cusp forms weight 2 that are Hecke eigenforms in $\mathbb{Z}[[q]]$ $\quad\longleftrightarrow\quad$ ell. curves over $\mathbb{Q}$

WT goes $\leftarrow$ $\rightarrow$ is Eichler-Shimura 1959-1962.

Enough for $\leftarrow$: Weil Converse Thm. If $L$-satisfies func eq'n, then is in image.

Example: $y^2 - y = x^3 - x$, $N = 37$, $\Delta = 37$

L series. Compute $a_p$ and the $a_m$. $\varepsilon_{37} = -1$

$$a_p = p - \#\{x, y \bmod p \mid y(y-1) \equiv x(x+1)(x-1) \bmod p\}.$$

count $\infty$

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_m$ | 1 | -2 | -3 | 2 | -2 | 6 | -1 | 0 | 6 | 4 | -5 | -6 | -2 | 2 | 6 |

Consider $S_2(\Gamma_0(37))$, 2-dim, $= \mathbb{C} f(\tau) \oplus \mathbb{C} g(\tau)$.

$f(\tau) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + \cdots$ just as above

Looks good for conjecture. Now have 3 models for $E(\mathbb{C})$

$\mathbb{C}/L$ ↑ $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ as before

$y^2 = 4x^3 - 4x + 1$

$\mathfrak{h}/\Gamma$, $\Gamma = \Gamma_0^*(37)$ $= \Gamma_0(37)$ and $\frac{1}{\sqrt{37}}\begin{pmatrix} 0 & -1 \\ 37 & 0 \end{pmatrix}$

$\longrightarrow$ $z \to (\wp(z), \frac{\wp'(z)}{2})$

$\longleftarrow$ $(x, y) \to \int_x^\infty \frac{dx}{\sqrt{4x^3 - 4x + 1}}$ mod lattice

$f(\tau) = \sum a_n q^n$. Let $\varphi(\tau) = \sum \frac{a_n}{n} q^n$, $q = 2\pi i \tau$

$\varphi'(\tau) = 2\pi i f(\tau)$

$$\frac{d}{d\tau}\left[\varphi\left(\tfrac{a\tau+b}{c\tau+d}\right)\right] = \frac{1}{(c\tau+d)^2} 2\pi i f\left(\tfrac{a\tau+b}{c\tau+d}\right) = 2\pi i f(\tau) = \varphi'(\tau)$$

So $\varphi\left(\tfrac{a\tau+b}{c\tau+d}\right) \equiv \varphi(\tau) + C_\gamma$

Then $C_{\gamma_1\gamma_2} = C_{\gamma_1} + C_{\gamma_2}$.

$C : \Gamma \to \mathbb{C}$ is a homomorphism

So $C(\Gamma) \subseteq \mathbb{C}$ is a subgroup.

Then $C(\Gamma)$ is a lattice $L \subseteq \mathbb{C}$ (?)

$$\begin{array}{ccc} \mathfrak{H} & \xrightarrow{\varphi} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathfrak{H}/\Gamma & \dashrightarrow^{\varphi} & \mathbb{C}/L \end{array}$$

↑ This is the modular parametrization.

This gives the correspondence second → first

In the other direction, need $\xi(\tau)$, $n(\tau)$ such that

1) $\Gamma$ invariant
2) $n^2 - n = \xi^3 - \xi$ (so we get a parametrization)
3) $\dfrac{\xi'(\tau)\,d\tau}{2n(\tau)} = \varphi'(\tau)\,d\tau = 2\pi i f(\tau)\,d\tau$

So $\dfrac{1}{2\pi i}\xi'(\tau) = 2n(\tau) f(\tau)$

Start with $\xi(\tau) = q^{-2} + A_1 q^{-1} + A_2 + A_3 q + \cdots$

$n(\tau) = q^{-3} + B_1 q^{-2} + B_2 q^{-1} + \cdots$

Equations (2) and (3) inductively give all $A_i$ and $B_i$.

Compute some more. $\xi(\tau) f(\tau)^2 \in M_4(\Gamma)$

$n(\tau) f(\tau)^3 \in M_6(\Gamma)$

Find candidates in spaces. Define $\xi(\tau) = \dfrac{\text{const} + c_4 f_4}{f(\tau)^2}$, etc.

Then have invariance. (2) and (3) hold to high power, hence hold exactly.

Zagier, 1/22/88

Illustrations not directly on main line of discussion

Modular parametrizations

Set-up: $E/\mathbb{Q}$ elliptic curve $\longleftrightarrow$ (conjectured) $f(z) \in S_2(\Gamma_0(N))$

$= \{ f : \mathfrak{H} \to \mathbb{C} \mid f(z)dz$ is $\Gamma_0(N)$-invariant $\}$ + cusp condition

Cusp condition

$\int_{\Gamma\backslash\mathfrak{H}} |f(z)dz|^2 < \infty$ or $f(z) = O(y^{-1})$ for all $z = x+iy$ $\Big| f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$

Note $|f(z)y|$ is invariant under $\Gamma$

$q = e^{2\pi i z}$

For $S_{2k}$, $f(z)(dz)^k$ is $\Gamma$-invariant, $f(z) = O(y^{-k})$.

Another way of saying it: $f(z) = \sum_{n=1}^{\infty} a_n q^n$, $a_n = O(n^{\frac{k}{2}})$

Correspondence: $\sum L(E,s) = \sum \frac{a_n}{n^s}$, $f$ is to be $f = \sum a_n q^n$

Hasse's Thm: $|a_p| \le 2\sqrt{p}$, $a_n \le n^{\frac{1}{2}} \sum_{d|n} 1$

$a_p = p+1-N(\beta)$, $N(\beta) \le 2p$. So $|a_p| \le p$.

Actually $S_2(\Gamma_0(N)) = S_2^+ \oplus S_2^-$. Namely $\Gamma_0(N) \subseteq \Gamma_0(N)^*$ with $\frac{1}{\sqrt{N}}\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ $= W_N$ since 2

$S_2^{\pm} = \Gamma_0^{\pm}(N)$.

$f \in S_2^{\pm} \iff f\left(-\frac{1}{Nz}\right) = \pm Nz^2 f(z)$

$f \in S_2$, $L(f,s)$ has a func. eq'n $\iff f \in S_2^+$ or $f \in S_2^-$

$f \in S_2^{\pm} \iff L^*(f,s) := (2\pi)^{-s} N^{s/2} \Gamma(s) L(f,s) = \mp L^*(f, 2-s)$

If it is true that $E \leftrightarrow f$, then automatically

(1) $f$ is a Hecke eigenform

(2) (and level) $f|W_N = \pm f$ $\quad \left(f|W_N(z) = \frac{1}{Nz^2} f\left(\frac{-1}{Nz}\right)\right.$

$\left. \in S_N(\Gamma_0(N))\right)$

(Note $W_N^2 = 1$. So $S_2^+$ and $S_2^-$ are eigenspaces.

Under the correspondence, $f \in S_2^+ \Rightarrow \operatorname{ord}_{s=1} L(f,s)$ is odd

$f \in S_2^- \Rightarrow$ ..... even

Recall Birch - Swinnerton-Dyer conjecture says

$$\operatorname{order}_{s=1} L(E/\mathbb{Q}, s) = \operatorname{rank} E(\mathbb{Q})$$

(This makes sense only if modularity where $L$ series makes sense.)

Thus $f \in S_2^{(-1)^{n+1}}$.

Exact WT statement:

$$\left\{\begin{array}{l}\text{elliptic curves over } \mathbb{Q} \text{ of} \\ \text{conductor } N\end{array}\right\} / \text{isog} \quad \overset{\text{conjecturally}}{\underset{\text{(-1 correspondence)}}{\longleftrightarrow}} \quad \bigcup_{N \geq 1} \{f \in S_2(\Gamma_1(N))\}$$

($f$ eigenform, $N$ as small as possible)

(conj of $f \in \mathbb{Z}$, want to be $a_p = p+1-N(p)$)

↑ definition

Direction $\leftarrow$ is known (Shimura)

Direction $\rightarrow$ is conjecture (Weil proved Hasse-Weil implies this)

Example: $y^2 + y = x^3 - x$, $N = 37$. Find what $f$ should work.

$f(z) = \sum a_n e^{2\pi i n z}$, $\varphi(z) = \sum \frac{a_n}{n} e^{2\pi i n z}$

$\varphi(\gamma z) = \varphi(z) + c_\gamma$

**Thm** If $f$ is in newform of weight 2, then there $\gamma \to c(\gamma) \in \mathbb{C}$ is a lattice $L$ with $\mathbb{C}/L = E(\mathbb{C})$, $E$ is defined over $\mathbb{Q}$, and $L(E/\mathbb{Q}, s) = L(f, s)$.

Basic idea:

$$\begin{array}{ccc} \mathfrak{h} & \xrightarrow{\varphi} & \mathbb{C} \\ \downarrow & & \downarrow \\ \Gamma\backslash\mathfrak{h} & \dashrightarrow^{\varphi} & \mathbb{C}/L \\ \text{comp} & & \| \\ \| & & E(\mathbb{C}) \\ X_0(N)(\mathbb{C}) & & \\ 2\pi i f(\tau)\,d\tau & & dz \end{array}$$

$f(\tau) = \sum a_n q^n$, $q = e^{2\pi i \tau}$

$z = \varphi(\tau) = \sum \frac{a_n}{n} q^n$

$dz = 2\pi i \sum a_n q^n \, d\tau$

$= 2\pi i f(\tau)\, d\tau$ ←

Key property: $dz$ pulls back to $2\pi i f(\tau)\, d\tau$, namely ↑

Similarly $X_0(N) \to E$ is defined over $\mathbb{Q}$.

Applications and comments

1) Construction of a map $X_0(N) \to E$, i.e. algorithm to find functions $\exists$ an $n : \Gamma_0(N)\backslash\mathfrak{h} \xrightarrow{\text{Belo.}} \mathbb{C}$ with $n(\tau)^2 = \wp(\tau)^3 + a\wp(\tau) + b$ (a)

so that $\Gamma_0(N)\backslash\mathfrak{h} \to E(\mathbb{C})$ by $\tau \to (\wp(\tau), n(\tau))$

$$\frac{\wp'(\tau)}{2n(\tau)} = 2\pi i f(\tau). \quad (b)$$

We say this for $N = 37$.

(a) and (b) define $\wp$ and $n$.

Find which newform they should be.

Then show the newform satisfies (a) + (b) by clearing enough terms.

2) Understanding $X_0(N) \xrightarrow{\varphi} E/\mathbb{C}$, degree of $\varphi$ (to be discussed)

3) Using $\varphi$ to get interesting info about $E$.

Degree: Ref: Jagier, Cardinal.

Formula for degree of $\varphi$


Has to be even number of sides sides identified in pairs — then can compute genus.

$n$ sides, even. Number vertices $1, 2, \dots, n$, $n+1 = 1$.

$e_j$ = edge from $b_j$ to $b_{j+1}$. $e_j \to e_j^*$ is a fixed fpit free involution. $T: j \to j^* + 1$ gives identification on vertices.

Vertices of $X_0(N)$ = orbits of $\{1, \dots, n\}/T$

Genus: $\nu = |\{1, \dots, n\}/T|$

$$2 - 2g = \nu - \tfrac{1}{2} n + 1$$

Let $\gamma_j \in \Gamma$ such $e_j \to e_j^*$. Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Write $C(\gamma_j) = a_j \omega_1 + b_j \omega_2$, $a_j$ and $b_j \in \mathbb{Z}$.

Then $\deg \varphi = \frac{1}{2} \sum_{j \prec j'} (a_j b_{j'} - a_{j'} b_j)$

$j, j'$ in same $T$ orbit

$j$ to "left" of $j'$ in orbit

↑ $x, Tx, T^2x, \dots, T^{m-1}x$.

Explicit thing when $N$ = prime.

$$f(\tau) = \sum a_n e^{2\pi i n \tau}$$

$$\sum_{n=1}^{\infty} \frac{a_n}{n} e^{-\pi n \sqrt{3}/N} e^{(2j-1)\pi i n/N} = A_j \omega_1 + B_j \omega_2$$

↑ this is a $C(\delta)$ for a certain $\gamma$

Can do this on computer – $A_j$ and $B_j$ are integers

Put $T: j \to 1 - \frac{1}{j}$
$S: j \to 1 - j$
} gp of order 6 generated

Then $$\deg \Phi = \sum_{j \in \mathbb{F}_N - \{0,1\}/\langle T,S\rangle} \begin{vmatrix} 1 & A_j & B_j \\ 1 & A_{Tj} & B_{Tj} \\ 1 & A_{T^2 j} & B_{T^2 j} \end{vmatrix}$$

↑ sign gp on 3 letters

How to use the modular parametrization

Suppose we have a map $X_0(N)' \to E$ defined over $\mathbb{Q}$.

Principle: Any info. about modular curves can be applied to elliptic curves.

Example: Ribet proved a theorem about modular curves that implies that the Frey curve cannot be modular.

Theorem (Ribet). Suppose $E \longleftrightarrow f \in S_2(\Gamma_0(N))$, $E$ with discriminant $\Delta \in \mathbb{Z}$.

Let $N = \prod_{p \mid \Delta} p^{f_p}$, $\Delta = \prod_{p \mid \Delta} p^{\delta_p}$, $\delta_p, f_p \geq 1$. Let $\ell$ = prime.

Let $N_1 = N / \prod_{\substack{f_p = 1 \\ \text{and } \ell \mid \delta_p}} p$. Then $f \equiv f_1 \in S_2(\Gamma_0(N_1))$.
$\mod \ell$

Now take $\alpha^\ell + \beta^\ell = \gamma^\ell$ nontrivially. Frey: $E: y^2 = x(x-\alpha^\ell)(x-\gamma^\ell)$.

Then $\Delta = 16 \alpha^{2\ell} \beta^{2\ell} \gamma^{2\ell}$. Here $N = \prod_{p \mid \alpha\beta\gamma} p$ (condition known if $f_p = 1$)

Then we check directly $N_1 = 2$. But $S_2(\Gamma_0(2)) = \{0\}$. So $f_1$ cannot exist since ord of $q$ in $f$ is 1.

$\mathfrak{H}/SL_2(\mathbb{Z})$ ← 1) $D<0$, $D\equiv 0,1 \pmod 4$

$a,b,c \in \mathbb{Z}$, $b^2-4ac=D$, $a>0, c>0$

Think of $az^2+bz+c=0$. Then $z=\frac{-b+i\sqrt{|D|}}{2a} \in \mathfrak{H}$

Number of pairs $a,b,c$ with $b^2-4ac=D$, is finite
$= h(D)$ = class number. $(a,b,c)=1$

Summary. To each $D$ we above have a finite set of points
$\subseteq X_0(1) = \mathfrak{H}/SL_2(\mathbb{Z})$.

Can work with $X_0(N)$ also. Assume $a\equiv 0(N)$, $b\equiv \beta(N)$,

$\beta \in \mathbb{Z}/2N\mathbb{Z}$, $\beta^2 \equiv D \pmod{4N}$.

Get finite set of points for $D<0$, $\beta \pmod{2N}$, $\beta^2 \equiv D \pmod{4N}$, set $P_{D,\beta} \subseteq \mathfrak{H}_0/\Gamma_0(N)$ have condition if $(D,N)=1$.

If have map $\mathfrak{H}/\Gamma_0(N) \to E$,

get an interesting set of points from $P_{D,\beta}$ in $E(\mathbb{C})$.

Actually these points are in $E(\overline{\mathbb{Q}})$.

$P_{D,\beta}$ = sum of images is in $E(\mathbb{Q})$ - Heegner point.

2) $D>0$, $D\equiv 0,1 \pmod 4$, $a,b,c \in \mathbb{Z}$, $b^2-4ac=D$, $a>0$, $(a,b,c)=1$.

$z=\frac{-b\pm\sqrt{D}}{2a}$ roots of $az^2+bz+c=0$ (on $\mathbb{R}$)

Connect by geodesic in $\mathfrak{H}$, $C_{(a,b,c)}$. Check easily that

$C=\{z\in\mathfrak{H} \mid a|z|^2+bx+c=0$, where $x=\mathrm{Re}\, z\}$

Number of such curves in $\mathfrak{H}/SL_2(\mathbb{Z})$ is finite, $h(D)$.

The curves are compact: Namely $K=\mathbb{Q}(\sqrt{D})$ is real quadratic

Idea a matrix unit, $\frac{t+u\sqrt{D}}{2}$, $t^2-Du^2=4$, $t>0, u>0$.

$$\begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Fixed point are our endpoints. Hence this maps our curve to itself. So image of curve in $\mathfrak{H}/SL_2(\mathbb{Z})$ closes on itself.

Summary. If $D>0$, get a finite set of closed geodesics $\in \mathfrak{H}_0/\Gamma_0(N)$

Map to $E$. Closed curve has a homology class in

$$H^1(E(\mathbb{C}), \mathbb{Z}) = \mathbb{Z}\oplus\mathbb{Z}.$$

Sample application:

Sums of two cubes. If $m \in \mathbb{N}$, is $m = r^3+s^3$ with $r, s \in \mathbb{Q}$.

Conjecture: If $m$ is a prime $p \equiv 4, 7, 8 \bmod 9$, then rank $\leq 1$.

If $p \equiv 5, 2 \bmod 9$, then rank $\equiv 0$. If $p \equiv 1 \bmod 9$, then

$r \geq 2$.

Example: $13\cdot 27 = 351 = 343+8$, $13 = \left(\frac{7}{3}\right)^3 + \left(\frac{2}{3}\right)^3$

Theorem (Satgé, Zwartsius). If $p \equiv 2 \bmod 9$, then $2p = r^3+s^3$.

Idea. Curve has CM, so above applies. Use Heegner point for $D=-3p^2$. Call the up: $P_D \in E(\mathbb{Q})$. Prove $P_D \neq 0$ somehow.

Namely replace $E$: $x^3+y^3+2pz^3=0$ by $C$: $x^3+2y^3+pz^3=0$, not obviously elliptic curve. We add up our points on $C$ in a certain way, which has an inverse $\neq 0$ in $E$.