Complexity of rational solutions to polynomial equations.

· Rational ~~points~~ solutions are hard.

Examples: · 'Fermat': $x^n+y^n=z^n$ for $n\geq 3$ has only trivial sol'ns ($xyz=0$) – Taylor, Wiles, '95.

(K3)
· The CY given by $1+2x^4=y^4+4z^4$. Known sol'ns:
· $(0,\pm 1,0)$
· $\left(\pm\frac{1203120}{1484801}, \pm\frac{1169407}{1484801}, \pm\frac{1157520}{148401}\right)$ (Elsenhans & Jahnel, '05)

· Are there any others? Unknown.
· Does $\exists$ eqn of this form ($a+bx^4=cy^4+dz^4$) with finite nonzero # of sol'ns? Unknown

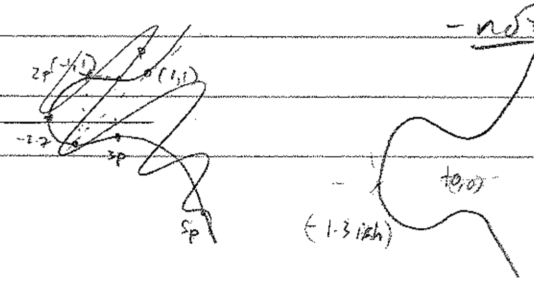
· Fibonacci: $F_0=0$, $F_1=1$, $F_{n+2}=F_n+F_{n+1}$.
Thm: Only perfect powers are:
$F_0=0$, $F_1=1$, $F_2=1$, $F_6=8$ & $F_{12}=144$
(Bugeaud, Mignotte, Siksek, '06)
– used modularity (à la Wiles), + classical stuff
(Baker, lin. forms in logs).

From now on, focus on
Elliptic Curves
Fix $a,b\in\mathbb{Q}$ s.t. $4a^3+27b^2\neq 0$ (else easy but different). Then the eqn

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

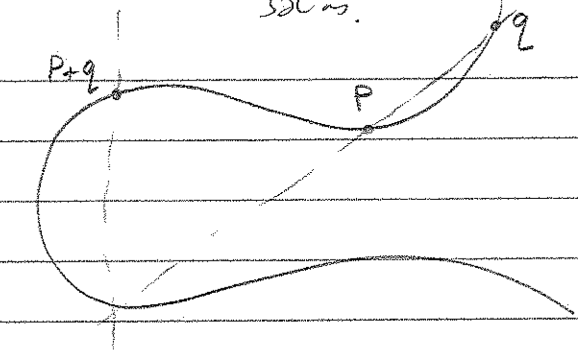
is called an elliptic curve

eg: $a=-1$, $b=1$, $y^2=x^3-x+1$ (real root -1.3ish)
Draw sketch of real pts – looks like a curve
– not like an ellipse (cf. arc lengths)



Main tool for understanding rat. pts on EC: ↑ pt at ∞.
sol'ns.

<u>Group law</u>;



(tangent for $2p$).

This makes $\{$rat. sol'ns to ~~...~~ $E\} \cup \{\infty\}$ into an abelian gp, $E(\mathbb{Q})$

<u>Thm</u> [Mordell, Weil, 1922]: $E(\mathbb{Q})$ is a <u>finitely generated</u>.

(so $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, T torsion
$r =$ rank, $\in \mathbb{Z}_{\geq 0}$)

- Was hard then, now in 1st EC course for master's students;
- Analogue for K3 surfaces ($\dim CH^2(X)_{\mathbb{Q}} < \infty$) <u>unknown</u>.
(even $=1$)

(for $y^2 = x^3 - x + 1$, $E(\mathbb{Q}) \simeq \mathbb{Z}$).

<u>How do T & r vary as we vary a&b?</u>
torsion rank

- Thm (Mazur 1977) $\# T \leq 12$, (sharp)
- <u>Analogue</u> for abelian varieties (higher dim. generalisations of ECs).
still open - 'strong torsion conjecture'

- Unknown if r bounded - not even a decent conjecture.
- $\exists$ algorithm to compute T.
- BSD $\Rightarrow$ $\exists$ algorithm for r.

Arithmetic complexity of sol'ns.

- Back to $1+2x^4=y^4+4z^4$: the sol'ns $(0,\pm1,0)$ are much 'simpler' than $\left(\frac{\pm 1203120}{1484801}, \ldots\right)$
- 'Size' not good, $\frac{1}{2}$ vs $\frac{1000}{2001}$.
- To make precise:

Def: Given $x \in \mathbb{Q}^*$, write $x=\frac{a}{b}$ with a,b coprime, & define

$$h(p) = \log \max(|a|,|b|)$$

Set $h(0)=0$.

On elliptic curves, extra useful. Given $p=(x_p,y_p) \in E(\mathbb{Q})$, define $h(p)=h(x_p)$.

Eg on $y^2=x^3-x+1$, ~~$p=(-1,1)$, so $h(p)=0$~~

$p=(3,-5)$, so $h(-p)=\log 5$

$2p=\left(\frac{19}{25}, \frac{103}{125}\right)$, so $h(2p)=\log 25 = 2\log p$.

$4p=\left(\frac{-350701}{265225}, \frac{-1391407}{136590875}\right)$, $h(4p)=\log(350701) = 3.97 \cdot h(2p)$

$8p = \ldots$, $h(8p) = 4.03 \cdot h(4p)$

In general, $h(2p)\approx 4h(p)$.

Thm [Tate]: Let E an EC. Then $\exists$ a constant C_E & a quadratic form $\hat{h}: E(\mathbb{Q}) \to \mathbb{R}$ such that $\forall p \in E(\mathbb{Q})$, have

$$|h(p)-\hat{h}(p)| \le C_E.$$

This $\hat{h}$, the NTht, is
- crucial in proving MW
- essential to formulation of BSD
- non-degenerate on $E(\mathbb{Q})\otimes_{\mathbb{Z}}\mathbb{Q}$?

Families of varieties

Eg. $y^2 = x^3 - t^2x + t^2$. For fixed value of $t \in \mathbb{Q}\setminus\{0\}$, get an EC.
($t=\pm 1$: get $y^2 = x^3 - x + 1$ again).

That E_t has $\hat{h}_{E_t}$: how does it vary as we vary t?
(Fix $t \rightsquigarrow E_t$, $\hat{h}_t : E_t(\mathbb{Q}) \to \mathbb{R}$)

[Sample question: how does constant in last thm vary with t?
· Not v. interesting, some answers, not useful.
· pt is that h is not interesting]

To ask better Question, need notion of:

Locally decomposable height.

Def: let X be the set of rat sol^ns of a collection of polynomials.
- eg. ~~E~~ $E(\mathbb{Q})$, or $\mathbb{Q}$ itself, or ...

A height fctn on X is just a fctn $X \to \mathbb{R}$.

eg. $X = E(\mathbb{Q})$, heights h, $\hat{h}$, constant fctns to $\mathbb{R}$, ...
- too many!

Special class of ht functions: locally decomposable hts

~~Def~~ Eg $h : \mathbb{Q}^* \to \mathbb{R}$.
$\frac{a}{b} \longmapsto \log\max(|a|, |b|)$.

Will write down a local decomposition.
· First, given a prime p & $x \in \mathbb{Q}$, define

$|x|_p = p^{-n}$ where n maximal integer s.t. $x \cdot p^{-n}$ has no p in denominator

eg. $|12|_2 = \frac{1}{4}$, $|12|_3 = \frac{1}{3}$, $|12|_5 = 1$,

$|\frac{1}{12}|_2 = 4$ $|\frac{1}{12}|_3 = 3$, $|\frac{1}{12}|_5 = 1$, ...

Set $|x|_\infty$ = 'usual abs. value'.

__Exercise__: $h(x) = \sum_{p \in \{\text{primes}\} \cup \{\infty\}} \log \max(|x|, 1)$. (from $\mathbb{Q}^* \to \mathbb{R}$).

'local' = 'prime-by-prime'. We say __h is an LD height.__

[__Formal defn__: After replacing X by alteration, ht given by ctsly metrised hermitian line bundle on a proper flat $\mathbb{Z}$-model.]

__Thm__ [Néron, '65]: $\hat{h}: E(\mathbb{Q}) \to \mathbb{R}$ is an LD height.

With this notion of LD hts, let's go back to families:

__Families II__, ~~Better~~

$y^2 = x^3 - t^2 x + t^2$. • Fix $t \to$ ell-curve E_t

• Notice that (t,t) is always a rational pt on E_t.
('section of the family').

Use this to define a fctn

$$H: \mathbb{Q}^* \longrightarrow \mathbb{R}$$
$$t \longmapsto \hat{h}_{E_t}((t,t)).$$

Eg. $1 \longmapsto \hat{h}_E((1,1))$, $E: y^2 = x^3 - x + 1$, $p = (1,1)$

This is a ht by defn. Is it an LD ht? No.

__Thm__ [Silverman, Tate]: There is an LD height $\hat{H}: \mathbb{Q}^* \to \mathbb{R}$

such that $H - \hat{H}$ is bounded.

(for any family, & any section).

[we gave a new pf w. R de Jong & O Biesel using study of resistance in electrical networks]

__Cor__: $\{t \in \mathbb{Q} \mid (t,t)$ is __torsion__ in $E_t(\mathbb{Q})\}$ is finite.

Families with more parameters.

Eg: $y^2 = x^3 - t^2 x + s^2$. Fix $s, t \in \mathbb{Q}$ (s.t. $27s^4 - 4t^6 \neq 0$.)
$\rightsquigarrow$ elliptic curve $E_{s,t}$.

· "section" (t, s).

In same way, get

$$H : \mathbb{Q} \times \mathbb{Q} \setminus \{27s^4 - 4t^6 = 0\} \longrightarrow \mathbb{R}$$

$$(s,t) \longmapsto \hat{h}_{E_{s,t}}((t,s)).$$

Again, $H(1,1) = \hat{h}_E(P)$, $E: y^2 = x^3 - x + 1$, $P = (1,1)$.

Noticed: If for all families "like this" (a Ab-sch / varieties/$\mathbb{Q}$) there is an LD ht $\hat{H}$ s.t. $H - \hat{H}$ bounded, then STC follows immediately.

Thm [H]: the fctn H as above does NOT have bounded difference from any LD ht.

(actually a complete classification of when this is possible. ~~Bl~~ Don't know an easy proof.)

Q: Is there an LD height $\hat{H}$ such that $H - \hat{H}$ is "small"?
Dream: prove some cases of STC ~~as~~ in this way.