Tate-Shafarevich groups, regulators of elliptic curves and L-functions

Christophe Delaunay

Notations

- Let E be an elliptic curve defined $\mathbb{Q}$ with conductor N:

$$E \ : \ y^2 = x^3 + Ax + B$$

- Let $L(E,s)$ be its L-function:

$$L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

- Let $\varepsilon(E)$ be the root number:

$$\Lambda(E,s) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma\left(\frac{s}{2}\right) L(E,s) = \varepsilon(E)\ \Lambda(E, 2-s)$$

Notations

- If d is a fundamental discriminant coprime with N, let E_d be the quadratic twist of E by d:

$$E_d \ : \ y^2 = x^3 + Ad^2x + Bd^3$$

- The L-function of E_d is given:

$$L(E_d, s) = \sum_{n\geq 1} \left(\frac{d}{n}\right) \frac{a_n}{n^s}$$

- The root number is $\varepsilon(E)\left(\frac{d}{-N}\right)$ and the conductor is Nd^2.

$\rightsquigarrow$ How do the invariants of E_d behave as d is varying over a natural set of discriminants?

- $\rightarrow$ The rank, r_d, of $E_d(\mathbb{Q})$.
- $\rightarrow$ The Tate-Shafarevich group, $Ш(E_d)$, of $E_d/\mathbb{Q}$.
- $\rightarrow$ The regulator, $R(E_d)$, of $E_d(\mathbb{Q})$.

- We separate the even ($\varepsilon(E_d) = 1$) and the odd ($\varepsilon(E_d) = -1$) case.

Notations

• If d is a fundamental discriminant coprime with N, let E_d be the quadratic twist of E by d:

$$E_d \ : \ y^2 = x^3 + Ad^2x + Bd^3$$

• The L-function of E_d is given:

$$L(E_d, s) = \sum_{n \geq 1} \left(\frac{d}{n}\right) \frac{a_n}{n^s}$$

• The root number is $\varepsilon(E)\left(\frac{d}{-N}\right)$ and the conductor is Nd^2.

$\rightsquigarrow$ How do the invariants of E_d behave as d is varying over a natural set of discriminants?

→ The rank, r_d, of $E_d(\mathbb{Q})$.

→ The Tate-Shafarevich group, $Ш(E_d)$, of $E_d/\mathbb{Q}$.

→ The regulator, $R(E_d)$, of $E_d(\mathbb{Q})$.

• We separate the even ($\varepsilon(E_d) = 1$) and the odd ($\varepsilon(E_d) = -1$) case.

Notations

- If d is a fundamental discriminant coprime with N, let E_d be the quadratic twist of E by d:

$$E_d \ : \ y^2 = x^3 + Ad^2x + Bd^3$$

- The L-function of E_d is given:

$$L(E_d, s) = \sum_{n \geq 1} \left(\frac{d}{n}\right) \frac{a_n}{n^s}$$

- The root number is $\varepsilon(E)\left(\frac{d}{-N}\right)$ and the conductor is Nd^2.

$\rightsquigarrow$ How do the invariants of E_d behave as d is varying over a natural set of discriminants?

$\rightarrow$ The rank, r_d, of $E_d(\mathbb{Q})$.

$\rightarrow$ The Tate-Shafarevich group, $Ш(E_d)$, of $E_d/\mathbb{Q}$.

$\rightarrow$ The regulator, $R(E_d)$, of $E_d(\mathbb{Q})$.

- We separate the even ($\varepsilon(E_d) = 1$) and the odd ($\varepsilon(E_d) = -1$) case.

Even case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = -\varepsilon(E)$.

- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0 \, , |d| \leq T \, , \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = +1$;

- Define $Ш_a(E_d)$ by:

$$L(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} Ш_a(E_d)$$

So $Ш_a(E_d) = 0$ if $L(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Even case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = -\varepsilon(E)$.

- Consider the family of elliptic curves $(E_d)_{d\in\mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0\ , |d| \leq T\ , \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = +1;$

- Define $Ш_a(E_d)$ by:

$$L(E_d, 1) = \frac{\Omega(E_d)\prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\mathrm{tors}}|^2} Ш_a(E_d)$$

So $Ш_a(E_d) = 0$ if $L(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Even case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = -\varepsilon(E)$.

- Consider the family of elliptic curves $(E_d)_{d\in\mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0\ , |d| \leq T\ , \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = +1$;

- Define $Ш_a(E_d)$ by:

$$L(E_d, 1) = \frac{\Omega(E_d)\prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} Ш_a(E_d)$$

So $Ш_a(E_d) = 0$ if $L(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Even case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = -\varepsilon(E)$.
- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0\ , |d| \leq T\ , \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = +1$;

- Define $Ш_a(E_d)$ by:

$$L(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} Ш_a(E_d)$$

So $Ш_a(E_d) = 0$ if $L(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Even case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = -\varepsilon(E)$.
- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0 \,, |d| \leq T \,, \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = +1$;

- Define $Ш_a(E_d)$ by:

$$L(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\mathrm{tors}}|^2} Ш_a(E_d)$$

So $Ш_a(E_d) = 0$ if $L(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Even case

Conjecture (Keating-Snaith)

We have, as $T \to \infty$:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} L(E_d, 1)^k \sim g_k(O^+) a_k(E) (\log T)^{k(k-1)/2}$$

- $g_k(O^+)$ is explicit and comes from RMT.
- $a_k(E)$ is an explicit arithmetic factor depending on the choice of ε_p.
- If $k \in \mathbb{N}$, other leading orders can be predicted (by the work of B. Conrey, D. Farmer, J. Keating, M. Rubinstein and N. Snaith).

What are the consequences on $Ш_a(E_d)$?

Even case

Conjecture (Keating-Snaith)

We have, as $T \to \infty$:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} L(E_d, 1)^k \sim g_k(O^+) a_k(E) (\log T)^{k(k-1)/2}$$

- $g_k(O^+)$ is explicit and comes from RMT.
- $a_k(E)$ is an explicit arithmetic factor depending on the choice of ε_p.

- If $k \in \mathbb{N}$, other leading orders can be predicted (by the work of B. Conrey, D. Farmer, J. Keating, M. Rubinstein and N. Snaith).

What are the consequences on $Ш_a(E_d)$?

Even case

Conjecture (Keating-Snaith)

We have, as $T \to \infty$:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} L(E_d, 1)^k \sim g_k(O^+) a_k(E) (\log T)^{k(k-1)/2}$$

- $g_k(O^+)$ is explicit and comes from RMT.
- $a_k(E)$ is an explicit arithmetic factor depending on the choice of ε_p.

- If $k \in \mathbb{N}$, other leading orders can be predicted (by the work of B. Conrey, D. Farmer, J. Keating, M. Rubinstein and N. Snaith).

What are the consequences on $Ш_a(E_d)$?

Even case

Proposition

For $|d|$ large enough, we have:

$$L(E_d,1) = 1^* \frac{\Omega}{\sqrt{|d|}} \left(\prod_{p|d} c_p(E_d) \right) Ш_a(E_d)$$

- Ω depends on the choice ε_p.
- $1^* = 2$ if $8 \mid d$ and c_4 is even and $1^* = 1$ otherwise (we will forget it).
- By partial summation on $\sum_{d\in\mathcal{F}(T)} L(E_d,1)^k$, we get:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d\in\mathcal{F}(T)} Ш_a(E_d)^k \prod_{p|d} c_p(E_d)^k \sim T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2}}$$

Even case

Proposition

For $|d|$ large enough, we have:

$$L(E_d, 1) = 1^* \frac{\Omega}{\sqrt{|d|}} \left(\prod_{p|d} c_p(E_d) \right) Ш_a(E_d)$$

- Ω depends on the choice ε_p.
- $1^* = 2$ if $8 \mid d$ and c_4 is even and $1^* = 1$ otherwise (we will forget it).
- By partial summation on $\sum_{d \in \mathcal{F}(T)} L(E_d, 1)^k$, we get:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} Ш_a(E_d)^k \prod_{p|d} c_p(E_d)^k \sim \frac{g_k(O^+) a_k(E)}{\Omega^k} \frac{2}{k+2} T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2}}$$

Even case

Proposition

For $|d|$ large enough, we have:

$$L(E_d,1) = 1^* \frac{\Omega}{\sqrt{|d|}} \left(\prod_{p|d} c_p(E_d) \right) Ш_a(E_d)$$

- Ω depends on the choice ε_p.
- $1^* = 2$ if $8 \mid d$ and c_4 is even and $1^* = 1$ otherwise (we will forget it).
- By partial summation on $\sum_{d \in \mathcal{F}(T)} L(E_d,1)^k$, we get:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} Ш_a(E_d)^k \prod_{p|d} c_p(E_d)^k \sim \underbrace{\frac{g_k(O^+)a_k(E)}{\Omega^k} \frac{2}{k+2}}_{B_k} T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2}}$$

Average of $\prod_{p|d} c_p(E_d)^k$

• For all $p \mid d$, Tate's algorithm implies:

$$c_p(E_d) = 1 + \text{ the number of roots of } F = x^3 + Ax + B \text{ in } \mathbb{F}_p$$

There are 3 cases:

• $F(x)$ has 3 roots in $\mathbb{Q}$ $\rightsquigarrow c_p(E_d) = 4$.

• $F(x)$ has 1 root in $\mathbb{Q}$ $\rightsquigarrow c_p(E_d) = 1$ or 4 depending on some congruences classes of p.

• $F(x)$ has no root in $\mathbb{Q}$ $\rightsquigarrow c_p(E_d) = 1,\ 2$ or 4 with some density for each possibilities.

Average of $\prod_{p|d} c_p(E_d)^k$

- For all $p \mid d$, Tate's algorithm implies:

$$c_p(E_d) = 1 + \text{ the number of roots of } F = x^3 + Ax + B \text{ in } \mathbb{F}_p$$

There are 3 cases:

- $F(x)$ has 3 roots in $\mathbb{Q}$ $\rightsquigarrow c_p(E_d) = 4$.

- $F(x)$ has 1 root in $\mathbb{Q}$ $\rightsquigarrow c_p(E_d) = 1$ or 4 depending on some congruences classes of p.

- $F(x)$ has no root in $\mathbb{Q}$ $\rightsquigarrow c_p(E_d) = 1,\ 2$ or 4 with some density for each possibilities.

Average of $\prod_{p|d} c_p(E_d)^k$

In the first cases, we are led to estimate sums of the form:

$$*(T) = \sum_{\substack{n<T \\ n \text{ squarefree} \\ n\equiv a \bmod N}} \left(\prod_{j\in(\mathbb{Z}/N\mathbb{Z})^\times} t_j^{|\{p|n\ ,\ p\equiv j \bmod N\}|} \right)$$

where the $(t_j)_j$ are non-negative numbers.

Theorem

$$*(T) \sim \mathrm{Cst}\ \ T\ \log(T)^{t-1}$$

where $t = \frac{1}{\varphi(N)} \sum_{j\in(\mathbb{Z}/N\mathbb{Z})^\times} t_j$ is the average of the t_j and:

$$\mathrm{Cst} = \frac{1}{\varphi(N)\Gamma(t)} \prod_{p|N}(1-1/p)^t \prod_j \prod_{p\equiv j \bmod N} (1+t_j/p)(1-1/p)^{t_j}$$

Average of $\prod_{p|d} c_p(E_d)^k$

In the first cases, we are led to estimate sums of the form:

$$*(T) = \sum_{\substack{n<T \\ n \text{ squarefree} \\ n \equiv a \bmod N}} \left(\prod_{j \in (\mathbb{Z}/N\mathbb{Z})^\times} t_j^{|\{p|n\ ,\ p \equiv j \bmod N\}|} \right)$$

where the $(t_j)_j$ are non-negative numbers.

Theorem

$$*(T) \sim \mathrm{Cst}\ \ T\ \log(T)^{t-1}$$

where $t = \frac{1}{\varphi(N)} \sum_{j \in (\mathbb{Z}/N\mathbb{Z})^\times} t_j$ is the average of the t_j and:

$$\mathrm{Cst} \ = \frac{1}{\varphi(N)\Gamma(t)} \prod_{p|N} (1 - 1/p)^t \prod_j \prod_{p \equiv j \bmod N} (1 + t_j/p)(1 - 1/p)^{t_j}$$

Even case

- Finally, we are led to make the following conjecture:

Conjecture

There exists $C_k > 0$ such that:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} \text{Ш}_a(E_d)^k \sim C_k \, T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2} + \mathrm{tam}_k}$$

Let L be the field of decomposition of $x^3 + Ax + B$ over $\mathbb{Q}$.

If $[L:\mathbb{Q}] = 1$ then $\mathrm{tam}_k = 4^{-k} - 1$.

If $[L:\mathbb{Q}] = 2$ then $\mathrm{tam}_k = \frac{1}{2}(2^{-k} + 4^{-k}) - 1$.

If $[L:\mathbb{Q}] = 3$ then $\mathrm{tam}_k = \frac{4^{-k}}{3} + \frac{2}{3} - 1$.

If $[L:\mathbb{Q}] = 6$ then $\mathrm{tam}_k = \frac{4^{-k}}{6} + \frac{2^{-k}}{2} + \frac{1}{3} - 1$.

Even case

- Finally, we are led to make the following conjecture:

Conjecture

There exists $C_k > 0$ such that:

$$\frac{1}{|\mathcal{F}(T)|}\sum_{d\in\mathcal{F}(T)} Ш_a(E_d)^k \sim C_k\, T^{\frac{k}{2}}(\log T)^{\frac{k(k-1)}{2}+\mathrm{tam}_k}$$

Let L be the field of decomposition of x^3+Ax+B over $\mathbb{Q}$.

If $[L:\mathbb{Q}]=1$ then $\mathrm{tam}_k = 4^{-k}-1$.

If $[L:\mathbb{Q}]=2$ then $\mathrm{tam}_k = \frac{1}{2}(2^{-k}+4^{-k})-1$.

If $[L:\mathbb{Q}]=3$ then $\mathrm{tam}_k = \frac{4^{-k}}{3}+\frac{2}{3}-1$.

If $[L:\mathbb{Q}]=6$ then $\mathrm{tam}_k = \frac{4^{-k}}{6}+\frac{2^{-k}}{2}+\frac{1}{3}-1$.

Numerical Check

- Need to compute $L(E_d, 1)$, then:

$$Ш_a(E_d) = \frac{L(E_d,1)}{\Omega\sqrt{|d|}} \prod_{p|d} \frac{1}{c_p(E_d)}$$

Theorem (Kohnen)

$L(E_d, 1) = (*)\, b(|d|)^2$, where

$$\sum b(|d|) q^{|d|} \text{ is a weight 3/2 modular form}$$

- Example:

$$E = 32a2 \;:\; y^2 = x^3 - x$$

The conjecture is:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} Ш_a(E_d)^k \sim C_k T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2} + 4^{-k} - 1}$$

Numerical Check

- Need to compute $L(E_d, 1)$, then:

$$Ш_a(E_d) = \frac{L(E_d, 1)}{\Omega\sqrt{|d|}} \prod_{p|d} \frac{1}{c_p(E_d)}$$

Theorem (Kohnen)

$L(E_d, 1) = (*)\ b(|d|)^2$, where

$$\sum b(|d|)q^{|d|} \text{ is a weight 3/2 modular form}$$

- Example:

$$E = 32a2\ :\ y^2 = x^3 - x$$

The conjecture is:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} Ш_a(E_d)^k \sim C_k T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2} + 4^{-k} - 1}$$

Numerical Check

- Need to compute $L(E_d, 1)$, then:

$$Ш_a(E_d) = \frac{L(E_d,1)}{\Omega\sqrt{|d|}} \prod_{p|d} \frac{1}{c_p(E_d)}$$

Theorem (Kohnen)

$L(E_d, 1) = (*)\ b(|d|)^2$, where

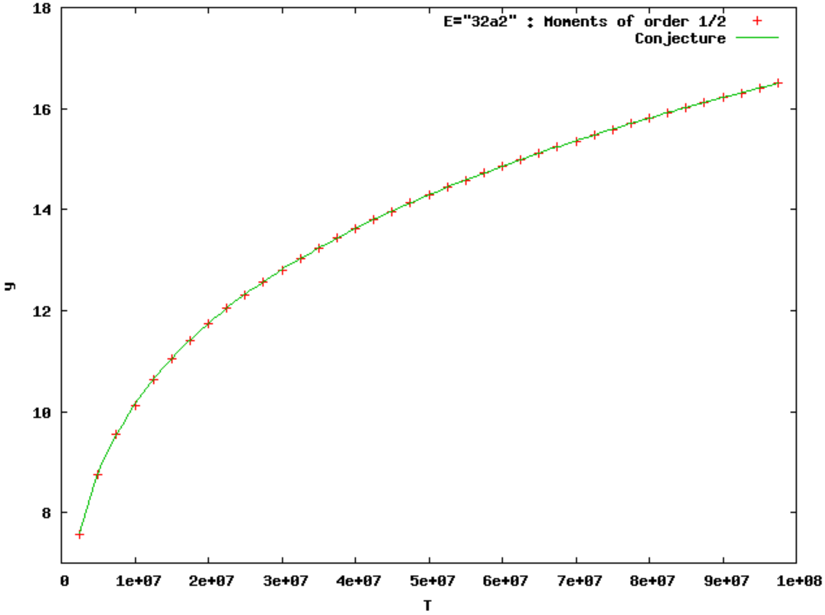
$$\sum b(|d|)q^{|d|} \text{ is a weight 3/2 modular form}$$

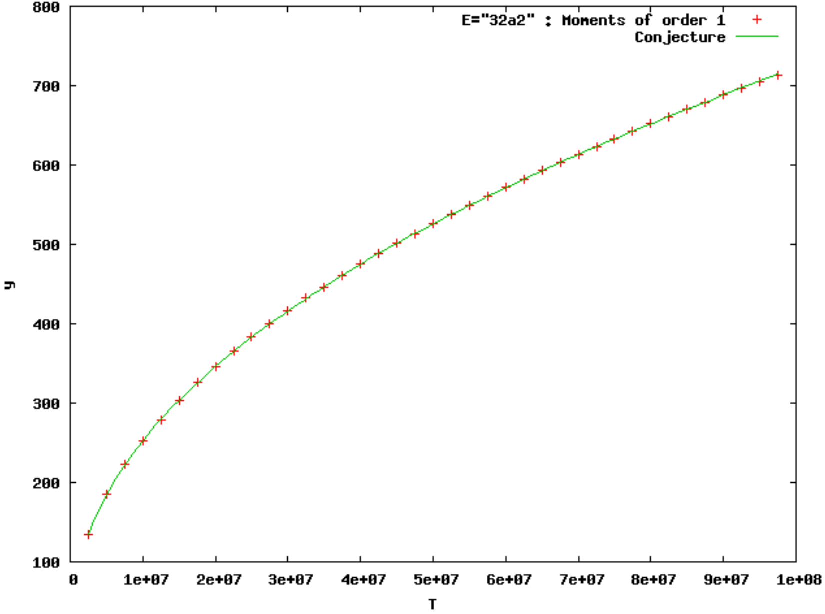
- Example:

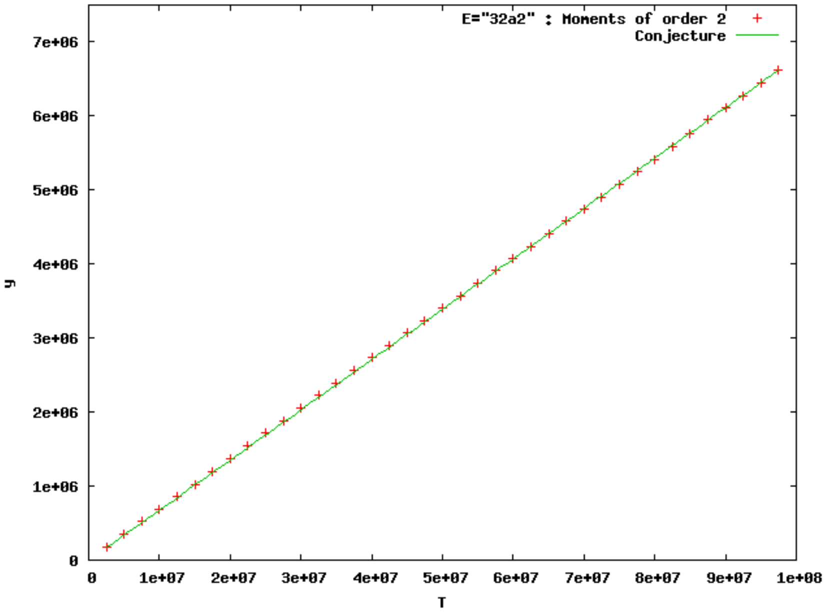
$$E = 32a2 \ : \ y^2 = x^3 - x$$

The conjecture is:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} Ш_a(E_d)^k \sim C_k T^{\frac{k}{2}} (\log T)^{\frac{k(k-1)}{2} + 4^{-k} - 1}$$


E="32a2" : Moments of order 1/2
Conjecture
y
T
18
16
14
12
10
8
0
1e+07
2e+07
3e+07
4e+07
5e+07
6e+07
7e+07
8e+07
9e+07
1e+08


E="32a2" : Moments of order 1
Conjecture
800
700
600
500
400
300
200
100
y
0
1e+07
2e+07
3e+07
4e+07
5e+07
6e+07
7e+07
8e+07
9e+07
1e+08
T


E="32a2" : Moments of order 2
Conjecture
7e+06
6e+06
5e+06
4e+06
3e+06
2e+06
1e+06
0
y
0
1e+07
2e+07
3e+07
4e+07
5e+07
6e+07
7e+07
8e+07
9e+07
1e+08
T

- An other application: the number of (no) extra-rank:

$$|\{d \in \mathcal{F}(T)\ ,\ r(E_d) = 0\}| \text{ or } |\{d \in \mathcal{F}(T)\ ,\ r(E_d) \geq 2\}|$$

No extra-rank

$\lvert\{d \in \mathcal{F}(T),\ \ L(E_d, 1) \neq 0\}\rvert$	$\gg$	$T^{1-\varepsilon}$	(Ono-Skinner)
	$\gg$	T	for some E (several authors)
	$\sim$	$\lvert\mathcal{F}(T)\rvert$	conjecturally (Goldfeld - BSD)

Extra-rank

$\lvert\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}\rvert$	$\gg$	$T^{1/2-\varepsilon}$	under BSD (Gouvêa-Mazur)
	$\gg$	$T^{3/4-\varepsilon}$	conjecturally (C.K.R.S.)

Conjecture (Conrey, Keating, Rubinstein and Snaith)

There exist $C_E > 0$ and $b_E \in \mathbb{R}$ such that :

$$\frac{|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|}{|\mathcal{F}(T)|} \sim C_E\, T^{-1/4}\, (\log T)^{b_E}$$

$\rightsquigarrow$ We will discuss about b_E.

- An other application: the number of (no) extra-rank:

$$|\{d \in \mathcal{F}(T)\ ,\ r(E_d) = 0\}| \text{ or } |\{d \in \mathcal{F}(T)\ ,\ r(E_d) \geq 2\}|$$

No extra-rank

$\|\{d \in \mathcal{F}(T),\ \ L(E_d, 1) \neq 0\}\|$	$\gg$	$T^{1-\varepsilon}$	(Ono-Skinner)
	$\gg$	T	for some E (several authors)
	$\sim$	$\|\mathcal{F}(T)\|$	conjecturally (Goldfeld - BSD)

Extra-rank

$\|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}\|$	$\gg$	$T^{1/2-\varepsilon}$	under BSD (Gouvêa-Mazur)
	$\gg$	$T^{3/4-\varepsilon}$	conjecturally (C.K.R.S.)

Conjecture (Conrey, Keating, Rubinstein and Snaith)

There exist $C_E > 0$ and $b_E \in \mathbb{R}$ such that :

$$\frac{|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|}{|\mathcal{F}(T)|} \sim C_E\, T^{-1/4}\, (\log T)^{b_E}$$

$\rightsquigarrow$ We will discuss about b_E.

- An other application: the number of (no) extra-rank:

$$|\{d \in \mathcal{F}(T)\ ,\ r(E_d) = 0\}| \text{ or } |\{d \in \mathcal{F}(T)\ ,\ r(E_d) \geq 2\}|$$

No extra-rank

$$\begin{aligned} |\{d \in \mathcal{F}(T),\ \ L(E_d, 1) \neq 0\}| &\gg T^{1-\varepsilon} && \text{(Ono-Skinner)} \\ &\gg T && \text{for some } E \text{ (several authors)} \\ &\sim |\mathcal{F}(T)| && \text{conjecturally (Goldfeld - BSD)} \end{aligned}$$

Extra-rank

$$\begin{aligned} |\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}| &\gg T^{1/2-\varepsilon} && \text{under BSD (Gouvêa-Mazur)} \\ &\gg T^{3/4-\varepsilon} && \text{conjecturally (C.K.R.S.)} \end{aligned}$$

Conjecture (Conrey, Keating, Rubinstein and Snaith)

There exist $C_E > 0$ and $b_E \in \mathbb{R}$ such that :

$$\frac{|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|}{|\mathcal{F}(T)|} \sim C_E\, T^{-1/4}\, (\log T)^{b_E}$$

$\rightsquigarrow$ We will discuss about b_E.

- An other application: the number of (no) extra-rank:

$$|\{d \in \mathcal{F}(T)\ ,\ r(E_d) = 0\}| \text{ or } |\{d \in \mathcal{F}(T)\ ,\ r(E_d) \geq 2\}|$$

No extra-rank

$|\{d \in \mathcal{F}(T),\ \ L(E_d, 1) \neq 0\}|$	$\gg$	$T^{1-\varepsilon}$	(Ono-Skinner)
	$\gg$	T	for some E (several authors)
	$\sim$	$|\mathcal{F}(T)|$	conjecturally (Goldfeld - BSD)

Extra-rank

$|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|$	$\gg$	$T^{1/2-\varepsilon}$	under BSD (Gouvêa-Mazur)
	$\gg$	$T^{3/4-\varepsilon}$	conjecturally (C.K.R.S.)

Conjecture (Conrey, Keating, Rubinstein and Snaith)

There exist $C_E > 0$ and $b_E \in \mathbb{R}$ such that :

$$\frac{|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|}{|\mathcal{F}(T)|} \sim C_E\, T^{-1/4}\, (\log T)^{b_E}$$

$\rightsquigarrow$ We will discuss about b_E.

• An other application: the number of (no) extra-rank:

$$|\{d \in \mathcal{F}(T)\ ,\ r(E_d) = 0\}| \text{ or } |\{d \in \mathcal{F}(T)\ ,\ r(E_d) \geq 2\}|$$

No extra-rank

$|\{d \in \mathcal{F}(T),\ \ L(E_d,1) \neq 0\}|$	$\gg$	$T^{1-\varepsilon}$	(Ono-Skinner)
	$\gg$	T	for some E (several authors)
	$\sim$	$|\mathcal{F}(T)|$	conjecturally (Goldfeld - BSD)

Extra-rank

$|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|$	$\gg$	$T^{1/2-\varepsilon}$	under BSD (Gouvêa-Mazur)
	$\gg$	$T^{3/4-\varepsilon}$	conjecturally (C.K.R.S.)

Conjecture (Conrey, Keating, Rubinstein and Snaith)

There exist $C_E > 0$ and $b_E \in \mathbb{R}$ such that :

$$\frac{|\{d \in \mathcal{F}(T),\ \ r_d \geq 2\}|}{|\mathcal{F}(T)|} \sim C_E\, T^{-1/4}\, (\log T)^{b_E}$$

$\rightsquigarrow$ We will discuss about b_E.

- RMT model: $\mathrm{prob}\,(L(E_d,1) < x) \approx \sqrt{x}\,(\log|d|)^{3/8}$ (as $x \to 0$).

- The discretisation model: $\text{Ш}_a(E_d) < 1 \Leftrightarrow L(E_d,1) = 0$.

We predict:

$$\mathrm{prob}\,(L(E_d,1) = 0) \quad = \quad \mathrm{prob}\left(L(E_d,1) < \frac{\Omega}{\sqrt{|d|}} \prod_{p|d} c_p(E_d) \right)$$

- RMT model: $\mathrm{prob}\,(L(E_d,1) < x) \approx \sqrt{x}\,(\log|d|)^{3/8}$ (as $x \to 0$).
- The discretisation model: $\text{Ш}_a(E_d) < 1 \Leftrightarrow L(E_d,1) = 0$.

We predict:

$$\mathrm{prob}\,(L(E_d,1)=0) \quad = \quad \mathrm{prob}\left(L(E_d,1) < \frac{\Omega}{\sqrt{|d|}} \prod_{p|d} c_p(E_d) \right)$$

- RMT model: $\text{prob}\,(L(E_d,1) < x) \approx \sqrt{x}\,(\log|d|)^{3/8}$ (as $x \to 0$).
- The discretisation model: $Ш_a(E_d) < 1 \Leftrightarrow L(E_d,1) = 0$.

We predict:

$$\text{prob}\,(L(E_d,1) = 0) = \text{prob}\left(L(E_d,1) < \frac{\Omega}{\sqrt{|d|}} \prod_{p|d} c_p(E_d) \right)$$

$$\approx \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \sqrt{\prod_{p|d} c_p(E_d)}$$

We get:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1) = 0\}|}{|\mathcal{F}(T)|} \approx \frac{1}{T} \sum_{d \in \mathcal{F}(T)} \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \prod_{p|d} \sqrt{c_p(E_d)}$$

So, by partial summation:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1) = 0\}|}{|\mathcal{F}(T)|} \approx \frac{(\log T)^{3/8}}{T^{1/4}} \left(\frac{1}{T} \sum_{d \in \mathcal{F}(T)} \prod_{p|d} \sqrt{c_p(E_d)} \right)$$

- RMT model: $\text{prob}\,(L(E_d,1) < x) \approx \sqrt{x}\,(\log|d|)^{3/8}$ (as $x \to 0$).
- The discretisation model: $Ш_a(E_d) < 1 \Leftrightarrow L(E_d,1) = 0$.

We predict:

$$\begin{aligned}\text{prob}\,(L(E_d,1)=0) &= \text{prob}\left(L(E_d,1) < \frac{\Omega}{\sqrt{|d|}} \prod_{p|d} c_p(E_d)\right)\\ &\approx \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \sqrt{\prod_{p|d} c_p(E_d)}\end{aligned}$$

We get:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1)=0\}|}{|\mathcal{F}(T)|} \approx \frac{1}{T} \sum_{d\in\mathcal{F}(T)} \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \prod_{p|d} \sqrt{c_p(E_d)}$$

So, by partial summation:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1)=0\}|}{|\mathcal{F}(T)|} \approx \frac{(\log T)^{3/8}}{T^{1/4}} \left(\frac{1}{T} \sum_{d\in\mathcal{F}(T)} \prod_{p|d} \sqrt{c_p(E_d)}\right)$$

- RMT model: $\text{prob}\,(L(E_d,1) < x) \approx \sqrt{x}\,(\log|d|)^{3/8}$ (as $x \to 0$).
- The discretisation model: $Ш_a(E_d) < 1 \Leftrightarrow L(E_d,1) = 0$.

We predict:

$$\begin{aligned} \text{prob}\,(L(E_d,1) = 0) &= \text{prob}\left(L(E_d,1) < \frac{\Omega}{\sqrt{|d|}} \prod_{p|d} c_p(E_d) \right) \\ &\approx \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \sqrt{\prod_{p|d} c_p(E_d)} \end{aligned}$$

We get:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1) = 0\}|}{|\mathcal{F}(T)|} \approx \frac{1}{T} \sum_{d \in \mathcal{F}(T)} \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \prod_{p|d} \sqrt{c_p(E_d)}$$

So, by partial summation:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1) = 0\}|}{|\mathcal{F}(T)|} \approx \frac{(\log T)^{3/8}}{T^{1/4}} \left(\frac{1}{T} \sum_{d \in \mathcal{F}(T)} \prod_{p|d} \sqrt{c_p(E_d)} \right)$$

- RMT model: $\text{prob}\,(L(E_d,1) < x) \approx \sqrt{x}\,(\log|d|)^{3/8}$ (as $x \to 0$).
- The discretisation model: $Ш_a(E_d) < 1 \Leftrightarrow L(E_d,1) = 0$.

We predict:

$$\begin{aligned} \text{prob}\,(L(E_d,1)=0) &= \text{prob}\left(L(E_d,1) < \frac{\Omega}{\sqrt{|d|}} \prod_{p|d} c_p(E_d)\right) \\ &\approx \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \sqrt{\prod_{p|d} c_p(E_d)} \end{aligned}$$

We get:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1)=0\}|}{|\mathcal{F}(T)|} \approx \frac{1}{T} \sum_{d\in\mathcal{F}(T)} \frac{\log(|d|)^{3/8}}{|d|^{1/4}} \prod_{p|d} \sqrt{c_p(E_d)}$$

So, by partial summation:

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d,1)=0\}|}{|\mathcal{F}(T)|} \approx \frac{(\log T)^{3/8}}{T^{1/4}} \left(\frac{1}{T} \sum_{d\in\mathcal{F}(T)} \prod_{p|d} \sqrt{c_p(E_d)}\right)$$

CKRS Conjecture

$$E \;:\; y^2 = F(x)$$

Assume that E is a curve having maximal rational 2 torsion sub-group in its isogeny class.

Heuristics (joint work with M. Watkins)

$$\frac{|\{d \in \mathcal{F}(T),\ \ L(E_d, 1) = 0\}|}{|\mathcal{F}(T)|} \sim C_E\, T^{-1/4}\, (\log T)^{b_E}$$

where:

- $b_E = 3/8 + 1$ if $F(x)$ has 3 roots in $\mathbb{Q}$.
- $b_E = 3/8 + \sqrt{2}/2$ if $F(x)$ has 1 root in $\mathbb{Q}$.
- $b_E = 3/8 + 1/3$ or $3/8 + \sqrt{2}/2 - 1/3$ otherwise.

CKRS Conjecture

$$E \; : \; y^2 = F(x)$$

Assume that E is a curve having maximal rational 2 torsion sub-group in its isogeny class.

Heuristics (joint work with M. Watkins)

$$\frac{|\{d \in \mathcal{F}(T), \;\; L(E_d, 1) = 0\}|}{|\mathcal{F}(T)|} \sim C_E \, T^{-1/4} \, (\log T)^{b_E}$$

where:

- $b_E = 3/8 + 1$ if $F(x)$ has 3 roots in $\mathbb{Q}$.
- $b_E = 3/8 + \sqrt{2}/2$ if $F(x)$ has 1 root in $\mathbb{Q}$.
- $b_E = 3/8 + 1/3$ or $3/8 + \sqrt{2}/2 - 1/3$ otherwise.

Example

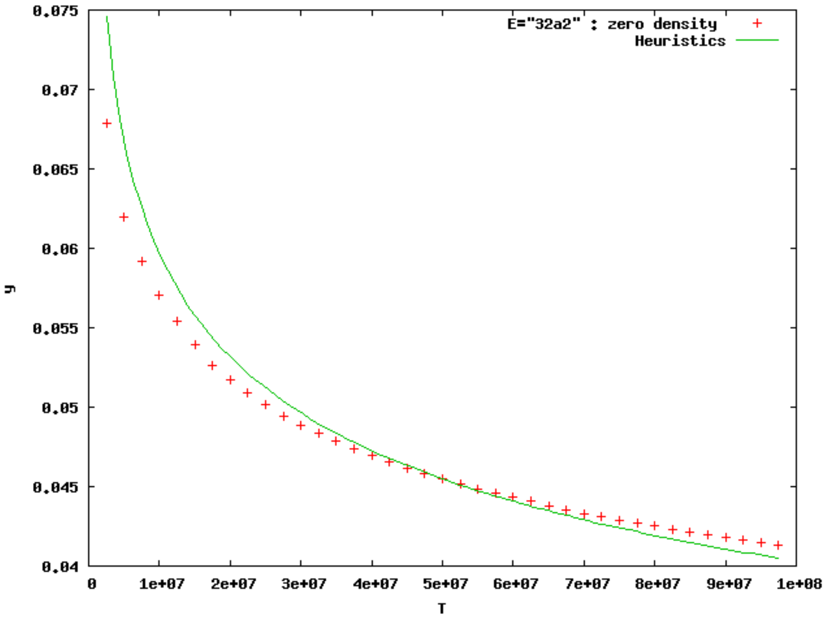
$$E = 32a2 \ : \ y = x^3 - x$$

The heuristic predicts that:

$$\frac{|\{d \in \mathcal{F}(T), \ \ L(E_d, 1) = 0\}|}{|\mathcal{F}(T)|} \sim C_E \, T^{-1/4} \, (\log T)^{3/8+1}$$

- Compare the numerical data ($T = 10^8$) and the heuristic.
- Problem: we are not able to predict the constant C_E.

We adjust the constant C_E such that the numerical data and the heuristic agree for $T = 5 \times 10^7$.


E="32a2" : zero density
Heuristics
0.075
0.07
0.065
0.06
0.055
0.05
0.045
0.04
y
0
1e+07
2e+07
3e+07
4e+07
5e+07
6e+07
7e+07
8e+07
9e+07
1e+08
T

Discussion

- In the discretisation process, it is implicitly assumed that the arithmetic of $\text{Ш}(E_d)$ does not give any contribution to the powers of $\log$.

But it could! As it is the case if we do not consider the good curve it its isogeny class.

- In fact, $\text{Ш}(E_d)$ is believed to have no influence on the powers of $\log$ but it takes a long time for the 2-part of $\text{Ш}(E_d)$ before it behaves as expected.

Discussion

- In the discretisation process, it is implicitly assumed that the arithmetic of $Ш(E_d)$ does not give any contribution to the powers of $\log$.

But it could! As it is the case if we do not consider the good curve it its isogeny class.

- In fact, $Ш(E_d)$ is believed to have no influence on the powers of $\log$ but it takes a long time for the 2-part of $Ш(E_d)$ before it behaves as expected.

Discussion

• In the discretisation process, it is implicitly assumed that the arithmetic of $\text{Ш}(E_d)$ does not give any contribution to the powers of $\log$.

But it could! As it is the case if we do not consider the good curve it its isogeny class.

• In fact, $\text{Ш}(E_d)$ is believed to have no influence on the powers of $\log$ but it takes a long time for the 2-part of $\text{Ш}(E_d)$ before it behaves as expected.

For our example, the Cohen-Lenstra heuristics for $Ш(E_d)$ assert that the probability that $p \mid Ш_a(E_d)$ is :

$$f(p) = 1 - \prod_{j \geq 1} (1 - p^{1-2j}) = \frac{1}{p} + \frac{1}{p^3} + \cdots$$

p	32a2	predictions
2	0.4357	0.5805
3	0.3579	0.3609
5	0.2076	0.2066
7	0.1483	0.1454

Numerical values for $T = 10^8$

A theorem of Heath-Brown (and the BSD and Goldfeld conjecture) implies that the correct red value for $T = \infty$ is given by the predictions.

But, the d's need to have a lot of prime factor for this to happen. Hence, the discriminants must be very large!!

Example: We only consider d such that $\omega(d) \geq 5$ for $32A2$.

For our example, the Cohen-Lenstra heuristics for $\text{Ш}(E_d)$ assert that the probability that $p \mid \text{Ш}_a(E_d)$ is :

$$f(p) = 1 - \prod_{j \geq 1} (1 - p^{1-2j}) = \frac{1}{p} + \frac{1}{p^3} + \cdots$$

p	32a2	predictions
2	0.4357	0.5805
3	0.3579	0.3609
5	0.2076	0.2066
7	0.1483	0.1454

Numerical values for $T = 10^8$

A theorem of Heath-Brown (and the BSD and Goldfeld conjecture) implies that the correct red value for $T = \infty$ is given by the predictions.

But, the d's need to have a lot of prime factor for this to happen. Hence, the discriminants must be very large!!

Example: We only consider d such that $\omega(d) \geq 5$ for $32A2$.

For our example, the Cohen-Lenstra heuristics for $\text{Ш}(E_d)$ assert that the probability that $p \mid \text{Ш}_a(E_d)$ is :

$$f(p) = 1 - \prod_{j \geq 1} (1 - p^{1-2j}) = \frac{1}{p} + \frac{1}{p^3} + \cdots$$

p	32a2	predictions
2	0.4357	0.5805
3	0.3579	0.3609
5	0.2076	0.2066
7	0.1483	0.1454

Numerical values for $T = 10^8$

A theorem of Heath-Brown (and the BSD and Goldfeld conjecture) implies that the correct red value for $T = \infty$ is given by the predictions.

But, the d's need to have a lot of prime factor for this to happen. Hence, the discriminants must be very large!!

Example: We only consider d such that $\omega(d) \geq 5$ for $32A2$.

For our example, the Cohen-Lenstra heuristics for $Ш(E_d)$ assert that the probability that $p \mid Ш_a(E_d)$ is :

$$f(p) = 1 - \prod_{j \geq 1} (1 - p^{1-2j}) = \frac{1}{p} + \frac{1}{p^3} + \cdots$$

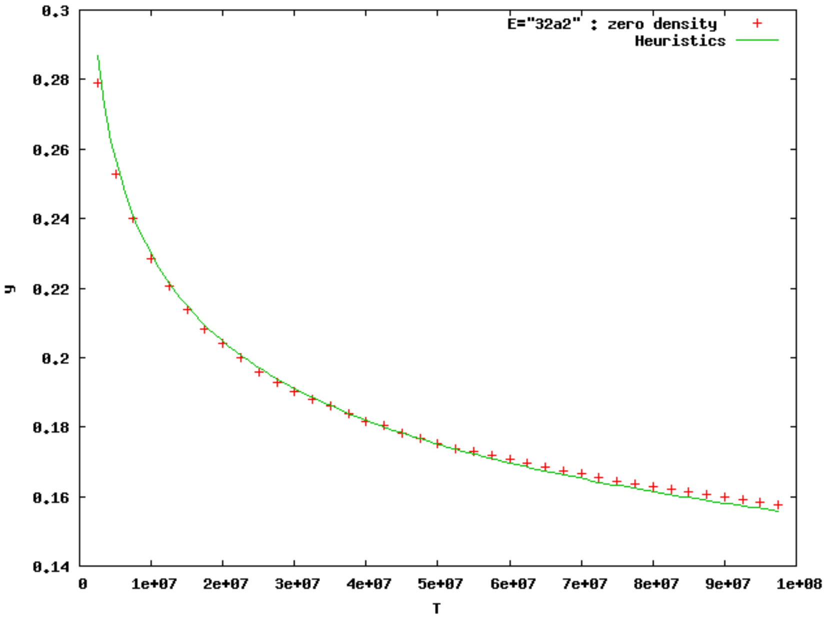
p	32a2	predictions
2	0.4357	0.5805
3	0.3579	0.3609
5	0.2076	0.2066
7	0.1483	0.1454

Numerical values for $T = 10^8$

A theorem of Heath-Brown (and the BSD and Goldfeld conjecture) implies that the correct red value for $T = \infty$ is given by the predictions.

But, the d's need to have a lot of prime factor for this to happen. Hence, the discriminants must be very large!!

Example: We only consider d such that $\omega(d) \geq 5$ for $32A2$.


E="32a2" : zero density
Heuristics
0.3
0.28
0.26
0.24
0.22
0.2
0.18
0.16
0.14
y
0
1e+07
2e+07
3e+07
4e+07
5e+07
6e+07
7e+07
8e+07
9e+07
1e+08
T

Discussion

- We can also compare the heuristic with the odd part of $\text{Ш}_a(E_d)$.

- Indeed, the same arguments works if we count:

$$\frac{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd and } \ \text{Ш}(E_d)_a \leq 1\}|}{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd}\}|}$$

Question: Have we

$$\frac{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) = 1\}|}{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd}\}|} \approx T^{-1/4}\,(\log T)^{3/8+1}\ ?$$

Example: $E = 32a2$

Discussion

- We can also compare the heuristic with the odd part of $\text{Ш}_a(E_d)$.
- Indeed, the same arguments works if we count:

$$\frac{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd and } \text{Ш}(E_d)_a \leq 1\}|}{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd}\}|}$$

Question: Have we

$$\frac{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) = 1\}|}{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd}\}|} \approx T^{-1/4}\,(\log T)^{3/8+1} \ ?$$

Example: $E = 32a2$

Discussion

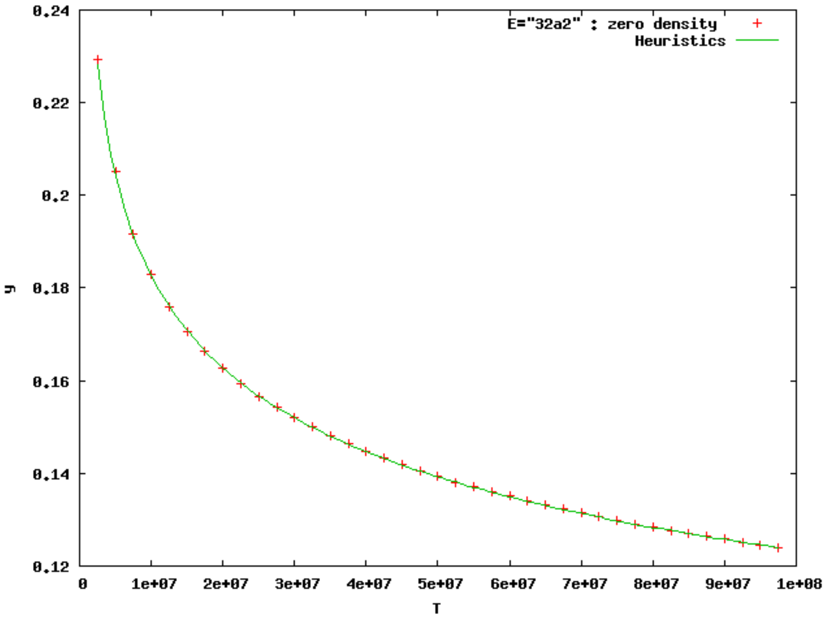
- We can also compare the heuristic with the odd part of $\text{Ш}_a(E_d)$.
- Indeed, the same arguments works if we count:

$$\frac{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd and } \text{Ш}(E_d)_a \leq 1\}|}{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd}\}|}$$

Question: Have we

$$\frac{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) = 1\}|}{|\{d \in \mathcal{F}(T),\ \ \text{Ш}_a(E_d) \text{ is odd}\}|} \approx T^{-1/4} \, (\log T)^{3/8+1} \ ?$$

Example: $E = 32a2$


E="32a2" : zero density
Heuristics
0.24
0.22
0.2
0.18
0.16
0.14
0.12
y
0
1e+07
2e+07
3e+07
4e+07
5e+07
6e+07
7e+07
8e+07
9e+07
1e+08
T

Odd case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = \varepsilon(E)$.

- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0\ ,|d| \leq T\ ,\text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = -1$;

- Define $Ш_a(E_d)$ by:

$$L'(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} R(E_d) Ш_a(E_d)$$

where $R(E_d)$ is the regulator of E_d.

So $Ш_a(E_d) = 0$ if $L'(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Odd case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\displaystyle\prod_{p|N} \varepsilon_p = \varepsilon(E)$.

- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0 \, , |d| \leq T \, , \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = -1;$

- Define $Ш_a(E_d)$ by:

$$L'(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} R(E_d) Ш_a(E_d)$$

where $R(E_d)$ is the regulator of E_d.

So $Ш_a(E_d) = 0$ if $L'(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Odd case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = \varepsilon(E)$.
- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0\,, |d| \leq T\,, \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = -1$;

- Define $Ш_a(E_d)$ by:

$$L'(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\mathrm{tors}}|^2} R(E_d) Ш_a(E_d)$$

where $R(E_d)$ is the regulator of E_d.

So $Ш_a(E_d) = 0$ if $L'(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Odd case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = \varepsilon(E)$.

- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0 \,, |d| \leq T \,, \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = -1$;

- Define $Ш_a(E_d)$ by:

$$L'(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\mathrm{tors}}|^2} R(E_d) Ш_a(E_d)$$

where $R(E_d)$ is the regulator of E_d.

So $Ш_a(E_d) = 0$ if $L'(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Odd case

- For all $p \mid N$, fix a sign $\varepsilon_p = \pm 1$ such that: $\prod_{p|N} \varepsilon_p = \varepsilon(E)$.
- Consider the family of elliptic curves $(E_d)_{d \in \mathcal{F}(\infty)}$ where:

$$\mathcal{F}(T) = \{d < 0 \,, |d| \leq T \,, \text{fund. discr. such that } \left(\frac{d}{p}\right) = \varepsilon_p\}$$

$\rightarrow \varepsilon(E_d) = -1$;

- Define $Ш_a(E_d)$ by:

$$L'(E_d, 1) = \frac{\Omega(E_d) \prod_{p|Nd^2} c_p(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} R(E_d) Ш_a(E_d)$$

where $R(E_d)$ is the regulator of E_d.

So $Ш_a(E_d) = 0$ if $L'(E_d, 1) = 0$ and $Ш_a(E_d) = |Ш(E_d)|$ otherwise (by the Birch and Swinnerton-Dyer conjecture).

Odd case

Conjecture (N. Snaith)

We have, as $T \to \infty$:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} L'(E_d, 1)^k \sim A_k (\log T)^{k(k+1)/2}$$

- A_k comes from RMT and an arithmetic factor.

What are the consequences on $R(E_d)$?

Odd case

Proposition

For $|d|$ large enough, we have:

$$L'(E_d,1) = 1^* \, \frac{\Omega}{\sqrt{|d|}} \left(\prod_{p|d} c_p(E_d) \right) Ш_a(E_d) R(E_d)$$

- Ω depends on the choice ε_p.
- $1^* = 2$ if $8 \mid d$ and c_4 is even and $1^* = 1$ otherwise.
- By partial summation on $\sum_{d \in \mathcal{F}(T)} L'(E_d,1)^k$, we get:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} R(E_d)^k Ш_a(E_d)^k \prod_{p|d} c_p(E_d)^k \sim B_k \, T^{k/2} (\log T)^{\frac{k(k+1)}{2}}$$

for some B_k.

Odd case

Proposition

For $|d|$ large enough, we have:

$$L'(E_d,1) = 1^* \frac{\Omega}{\sqrt{|d|}} \left(\prod_{p|d} c_p(E_d) \right) Ш_a(E_d) R(E_d)$$

- Ω depends on the choice ε_p.
- $1^* = 2$ if $8 \mid d$ and c_4 is even and $1^* = 1$ otherwise.
- By partial summation on $\sum_{d \in \mathcal{F}(T)} L'(E_d,1)^k$, we get:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{d \in \mathcal{F}(T)} R(E_d)^k Ш_a(E_d)^k \prod_{p|d} c_p(E_d)^k \sim B_k \, T^{k/2} (\log T)^{\frac{k(k+1)}{2}}$$

for some B_k.

Average of $Ш_a(E_d)^k$

- Heuristics on $Ш$ $\rightsquigarrow$ If $0 < k < 1$ then:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} |Ш_a(E_d)|^k \to \mathrm{Cst}(k)$$

Hence:

Heuristics (joint work with X.-F. Roblot)

For $0 < k < 1$:

$$M_k(T) = \frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d)^k \sim A_k \, T^{\frac{k}{2}} \, (\log T)^{\frac{k(k+1)}{2} + \mathrm{tam}_k}$$

Let $F(x) = x^3 + Ax + B$.

- $\mathrm{tam}_k = 4^{-k} - 1$ if $F(x)$ has 3 roots in $\mathbb{Q}$.
- $\mathrm{tam}_k = \frac{1}{2}(2^{-k} + 4^{-k}) - 1$ if $F(x)$ has 1 root in $\mathbb{Q}$.
- $\mathrm{tam}_k = \frac{4^{-k}}{3} + \frac{2}{3} - 1$ or $\mathrm{tam}_k = \frac{4^{-k}}{6} + \frac{2^{-k}}{2} + \frac{1}{3} - 1$ otherwise.

Average of $Ш_a(E_d)^k$

- Heuristics on $Ш$ $\rightsquigarrow$ If $0 < k < 1$ then:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} |Ш_a(E_d)|^k \to \mathrm{Cst}(k)$$

Hence:

Heuristics (joint work with X.-F. Roblot)

For $0 < k < 1$:

$$M_k(T) = \frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d)^k \sim A_k \, T^{\frac{k}{2}} \, (\log T)^{\frac{k(k+1)}{2} + \mathrm{tam_k}}$$

Let $F(x) = x^3 + Ax + B$.

- $\mathrm{tam_k} = 4^{-k} - 1$ if $F(x)$ has 3 roots in $\mathbb{Q}$.
- $\mathrm{tam_k} = \frac{1}{2}(2^{-k} + 4^{-k}) - 1$ if $F(x)$ has 1 root in $\mathbb{Q}$.
- $\mathrm{tam_k} = \frac{4^{-k}}{3} + \frac{2}{3} - 1$ or $\mathrm{tam_k} = \frac{4^{-k}}{6} + \frac{2^{-k}}{2} + \frac{1}{3} - 1$ otherwise.

Average of $Ш_a(E_d)^k$

- Heuristics on $Ш$ $\rightsquigarrow$ If $0 < k < 1$ then:

$$\frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} |Ш_a(E_d)|^k \to \mathrm{Cst}(k)$$

Hence:

Heuristics (joint work with X.-F. Roblot)

For $0 < k < 1$:

$$M_k(T) = \frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d)^k \sim A_k \, T^{\frac{k}{2}} \, (\log T)^{\frac{k(k+1)}{2} + \mathrm{tam_k}}$$

Let $F(x) = x^3 + Ax + B$.

- $\mathrm{tam_k} = 4^{-k} - 1$ if $F(x)$ has 3 roots in $\mathbb{Q}$.
- $\mathrm{tam_k} = \frac{1}{2}(2^{-k} + 4^{-k}) - 1$ if $F(x)$ has 1 root in $\mathbb{Q}$.
- $\mathrm{tam_k} = \frac{4^{-k}}{3} + \frac{2}{3} - 1$ or $\mathrm{tam_k} = \frac{4^{-k}}{6} + \frac{2^{-k}}{2} + \frac{1}{3} - 1$ otherwise.

Upper bounds

- Lindelöf $\Rightarrow$

$$R(E_d) \ll |d|^{1/2+\varepsilon}$$

Proposition

N square-free, $\varepsilon_p = +1,\ \forall p|N$, $L(E,1) \neq 0$ then

$$\frac{1}{T^*} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d) \ll T^{1/2} \log T$$

Lower bounds

Proposition

We have

$$R(E_d) > \frac{1}{3} \log |d| + O(1)$$

If $j(E) \neq 0, 1728$ and $w_p = +1, \ \forall p \mid N$:

$$R(E_d) > \frac{1}{1296 c(E)^2} \log |d|$$

Optimal: $E \ : \ y^2 = x^3 + Ax + B = F(x)$.

The point $(r, 1) \in E_{F(r)}$ and $h \approx \log(F(r))$.

Example: $E = 11a1$.

Lower bounds

Proposition

We have

$$R(E_d) > \frac{1}{3}\log|d| + O(1)$$

If $j(E) \neq 0, 1728$ and $w_p = +1,\ \forall p \mid N$:

$$R(E_d) > \frac{1}{1296c(E)^2}\log|d|$$

Optimal: $E\ :\ y^2 = x^3 + Ax + B = F(x)$.

The point $(r,1) \in E_{F(r)}$ and $h \approx \log(F(r))$.

Example: $E = 11a1$.

Lower bounds

Proposition

We have

$$R(E_d) > \frac{1}{3}\log|d| + O(1)$$

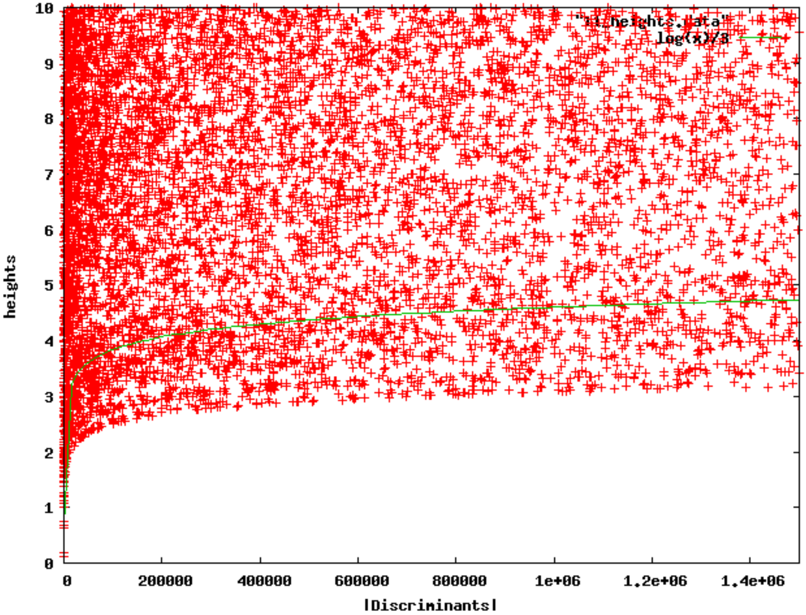
If $j(E) \neq 0, 1728$ and $w_p = +1,\ \forall p \mid N$:

$$R(E_d) > \frac{1}{1296c(E)^2}\log|d|$$

Optimal: $E\ :\ y^2 = x^3 + Ax + B = F(x)$.

The point $(r, 1) \in E_{F(r)}$ and $h \approx \log(F(r))$.

Example: $E = 11a1$.


log(x)/3
heights
|Discriminants|
0
1
2
3
4
5
6
7
8
9
10
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06

Numerical check

$$L'(E_d, 1) = \frac{\Omega}{\sqrt{|d|}} c(E_d)\ R(E_d)\ \text{Ш}_a(E_d)$$

→ If $L'(E_d, 1) \neq 0$ then:

$$E_d(\mathbb{Q}) = < G_d > \oplus \text{Torsion}$$

$$R(E_d) = 2h(G_d) \rightsquigarrow \text{find } G_d \in E_d(\mathbb{Q}).$$

• Efficient algorithm for computing G_d and $\text{Ш}_a(E_d)$ at "the same time".

Numerical check

$$L'(E_d,1) = \frac{\Omega}{\sqrt{|d|}} c(E_d)\ R(E_d)\ \text{Ш}_a(E_d)$$

$\rightarrow$ If $L'(E_d,1) \neq 0$ then:

$$E_d(\mathbb{Q}) = < G_d > \oplus \text{Torsion}$$

$$R(E_d) = 2h(G_d) \rightsquigarrow \text{find } G_d \in E_d(\mathbb{Q}).$$

• Efficient algorithm for computing G_d and $\text{Ш}_a(E_d)$ at “the same time”.

Example

- Finding G_d might be complicated:

$E = 11a1$ and $d = -1482139$ then (on the minimal model of E_d), the abscissa of G_d is a rational number such that the numerator and the denominator have ≈ 4320 digits.

And we have : $h(E_d) \approx 9945$.

The numerator of the abscissa of G_d is:

2626914163715788373011505693935892465023966285938661623601264958911869710379354821953092228638535709852293922347110
6420693712053799494480957073655050549865973802093302989718994909926085639138521038658387204788969769251829399796376
4230777576140746007001964179159051838221723260217040933423895649679116537266751298303983204220906012167999049681943
2108991850150658469745715485018157989425059588099902104506237536755932925212260557543980051042248814313543553611755
5672877245151326681176620288243743524056666985243046716469271070623979945599500346476075858500767502038588420404741
9615371391071481209937700164975500656691341301117104970941950706763906686415519511398962660874547910208479223761929
7761749441604129930611161529596386056770885057395910471323268713422324228498945306825193761031392864659083178145638
3774034353843313425839451564297663444413589794397666733867803807991851676979482798464903862779903272771125226295396
0709689740806143073222814107041284537473799552472764839194453658808773832989893688133541522076612422285990507198063
9510183749886296789770894175715647798283423515665420127733040056233824808518143038370234558383538634382301040369902
3384802026992740136979769212794545558294822953071468751299836164017907574577661932659762200617526126153077658585554
6506848426645947354728074428162850406554997749157979760331199284302706221388160329039473907019625204959272452574621
8565155659936296955635869761121428551882586654287174878845261760534253181742705464839421275785352400703757690821627
8729908445749796095058136683283297990823308660881695705693600506151097743450867210750226106934157947251454339324643
1896365575013300472586584088202371076890770213739490399091491035034421458336966017108095663635120522776551890717176
6324013327755325819598972996555371068716551397929945109583076385853055605483613471909490886804373891207635242935486
3562692429868333526981388733828283090720213679042919762988507511291676927852877078409469500378725533620588950046510
4539077376239399832524948429671217408367486407765029101408636433205913375104630646129499231160387406474276549966455
7146932030099694430181933164433607927908520505959965338952219957224400854805416114558287197204880545163181227070759
2291971199767322171293729717201194556921005439582013351208129165164869952015234653384880391020482126016211616158829
0525324015939990133108219487354120601177277210167053043521508566198488469274252797538933315924130306794617092796978
2214754047924299473188264050939657419190144275499605206771491607561986665865446762819097190730153789415929434242751
1161897986015746995414991912002116682060842953350351358746265884661776962865691110732960200995585372328157986921482
4719960632571110184671545544726356557924129018443729810065391978502824027745319795173285076102000129252997887065814
8524230661940882793375948201245422737230827618305971638652956620085299679663239209642651113642955951391398230101203
2989050096212602092859688863494997027249550204185803656206656437111399084814788373832313294456657156941686731623322
8248670554466475423467659409128012712077245480899021213905233386864797834788876769927462606380486703546640046629280
3776710374762911549582788008601648701036127577455676693903491106075703378556103344060316663197368770494076563561504
7306981954278922506892815316324486705269952776839705746316794522675847606228109369608162847599501680588151435914265
4180110613422257226637950363225313969002836163239902628408564276997318997078027927418322490270189548644677308357492
9912511549691379149687464162780237142683963750252696660342758869083702649684482358846234344722332741393085759800608
5644022660014457290370173670762559115239593800900725738986249333193105522023360140990051347321614435850671512753176
3295436771738486310505677924931633140121575598952505349068669498680453445072001471864457954529223066758283674614435
6631252476359856334626086714945439031204045142932868406026326950066262489966073930355969958625432977008966902630647
6436225091423987050724457858068127731256011891884596417259739911365870961345765213172391374837585094642732811401268
4486272433157144064127958544081465734907879675192397684715695935004573362169655253163121796284297291028115020174376
0764250644544308635332608897691702824683304398292965971149674453665597467860662180837903081427108202797099114452001
3302480275087559359344739432483804353059317517459045362960801012949009

The method

- We must have $L(E, 1) \neq 0$.

- We take $\varepsilon_p = +1$ for all $p \mid N$.

Step 1

- Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the "Heegner point".

$\rightsquigarrow$ Compute $\quad P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

where

$$\varphi \,:\, X_0(N) = \Gamma_0(N)\backslash\overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$

is the modular parametrization of E.

- The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)|h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow O(|d|^{1/2+\varepsilon})$ steps.)

Step 1

- Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the “Heegner point”.

$\rightsquigarrow$ Compute $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

where

$$\varphi \ : \ X_0(N) = \Gamma_0(N)\backslash\overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$

is the modular parametrization of E.

- The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)|h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow O(|d|^{1/2+\varepsilon})$ steps.)

Step 1

- Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the "Heegner point".

$\rightsquigarrow$ Compute $\quad P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

where

$$\varphi \ : \ X_0(N) = \Gamma_0(N) \backslash \overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$

is the modular parametrization of E.

- The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)| h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow O(|d|^{1/2+\varepsilon})$ steps.)

Step 1

- Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the "Heegner point".

$\rightsquigarrow$ Compute $\quad P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

where

$$\varphi \; : \; X_0(N) = \Gamma_0(N) \backslash \overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$

is the modular parametrization of E.

- The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)| h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow O(|d|^{1/2+\varepsilon})$ steps.)

Step 1

- Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the "Heegner point".

$\rightsquigarrow$ Compute $$P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C}).$$

where
$$\varphi : X_0(N) = \Gamma_0(N) \backslash \overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$
is the modular parametrization of E.

- The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)|h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow$ $O(|d|^{1/2+\varepsilon})$ steps.)

Step 1

• Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the "Heegner point".

$\rightsquigarrow$ Compute $\quad P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

where

$$\varphi \ : \ X_0(N) = \Gamma_0(N)\backslash\overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$

is the modular parametrization of E.

• The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)|h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow O(|d|^{1/2+\varepsilon})$ steps.)

Step 1

- Compute the class group $Cl(d)$ of $\mathbb{Q}(\sqrt{d})$.

$\rightsquigarrow$ For each $[\mathfrak{a}] \in Cl(d)$, let $\tau_{[\mathfrak{a}]} \in X_0(N)$ the "Heegner point".

$\rightsquigarrow$ Compute $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

where

$$\varphi \ : \ X_0(N) = \Gamma_0(N) \backslash \overline{\mathbb{H}} \longrightarrow E(\mathbb{C})$$

is the modular parametrization of E.

- The point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ but it appears as a complex point.

In order to recognize it, for each $[\mathfrak{a}] \in Cl(d)$ we have to evaluate a polynomial with $O(h(P_d))$ coefficients.

$\rightsquigarrow$ This requires $O(|Cl(d)|h(P_d)) = O(|d|^{1+\varepsilon})$ steps.

(in fact a simultaneous evaluation $\rightsquigarrow$ $O(|d|^{1/2+\varepsilon})$ steps.)

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.

- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592c(E)^2 L(E, 1)} \log |d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.
- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.
- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592 c(E)^2 L(E, 1)} \log |d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.
- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.
- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592c(E)^2 L(E,1)} \log|d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.

- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592 c(E)^2 L(E,1)} \log|d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.
- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.
- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592c(E)^2 L(E, 1)} \log |d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.

- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592c(E)^2 L(E,1)} \log|d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.

- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.

- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592c(E)^2 L(E, 1)} \log|d| \Rightarrow L'(E_d, 1) = 0$$

Step 2

- We have $P_d = \sum_{[\mathfrak{a}]} \varphi(\tau_{[\mathfrak{a}]}) \in E(\mathbb{C})$.
- And $P_d = (a + b\sqrt{d}, y) \in E(\mathbb{Q}(\sqrt{d}))$ $\rightsquigarrow$ recognize a and b in $\mathbb{Q}$.

This step can fail

- If $h(P_d)$ is large $\rightsquigarrow$ increase the precision.
- If P_d is a torsion point $\Leftrightarrow L'(E_d, 1) = 0$.

Proposition

$$L'(E_d, 1) \leq \frac{\mathrm{vol}(E)|d|^{-1/2}}{2592c(E)^2 L(E,1)} \log|d| \Rightarrow L'(E_d, 1) = 0$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

Let $\psi : E \xrightarrow{\sim} E_d$ defined over $\mathbb{Q}(\sqrt{d})$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}.$
2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow Q_d = \ell_d G_d \mod \text{Torsion}.$
3. $\ell_d \neq 0.$

- "Divide" Q_d by $1, 2, \ldots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log|d|}}$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

$$\text{Let } \psi \quad : E \xrightarrow{\sim} E_d \text{ defined over } \mathbb{Q}(\sqrt{d})$$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}.$
2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow Q_d = \ell_d G_d \mod \text{Torsion}.$
3. $\ell_d \neq 0.$

- "Divide" Q_d by $1, 2, \ldots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log|d|}}$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

$$\text{Let } \psi \; : E \xrightarrow{\sim} E_d \text{ defined over } \mathbb{Q}(\sqrt{d})$$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}$.

2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow Q_d = \ell_d G_d \mod \text{Torsion}$.

3. $\ell_d \neq 0$.

- "Divide" Q_d by $1, 2, \ldots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log |d|}}$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

$$\text{Let } \psi \ : E \xrightarrow{\sim} E_d \text{ defined over } \mathbb{Q}(\sqrt{d})$$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}$.

2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow Q_d = \ell_d G_d \mod \text{Torsion}$.

3. $\ell_d \neq 0$.

- "Divide" Q_d by $1, 2, \ldots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log |d|}}$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

$$\text{Let } \psi \;: E \xrightarrow{\sim} E_d \text{ defined over } \mathbb{Q}(\sqrt{d})$$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow$ $E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}$.

2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow$ $Q_d = \ell_d G_d \mod \text{Torsion}$.

3. $\ell_d \neq 0$.

- “Divide” Q_d by $1, 2, \ldots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log|d|}}$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

$$\text{Let } \psi \; : E \xrightarrow{\sim} E_d \text{ defined over } \mathbb{Q}(\sqrt{d})$$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}$.
2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow Q_d = \ell_d G_d \mod \text{Torsion}$.
3. $\ell_d \neq 0$.

- "Divide" Q_d by $1, 2, \ldots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log|d|}}$$

Step 3

At this step, P_d is a point of infinite order in $E(\mathbb{Q}(\sqrt{d}))$.

$$\text{Let } \psi \quad : E \xrightarrow{\sim} E_d \text{ defined over } \mathbb{Q}(\sqrt{d})$$

Facts

1. $L'(E_d, 1) \neq 0$ $\rightsquigarrow E_d(\mathbb{Q}) = \langle G_d \rangle \oplus \text{Torsion}.$
2. $Q_d = \psi(P_d - \overline{P_d}) \in E_d(\mathbb{Q})$ $\rightsquigarrow Q_d = \ell_d G_d \mod \text{Torsion}.$
3. $\ell_d \neq 0.$

- "Divide" Q_d by $1, 2, \dots \ell_d$ (when possible) until G_d is found.

Proposition

$$|\ell_d| < 36c(E)\sqrt{\frac{2h(Q_d)}{\log |d|}}$$

Step 4

At this step, G_d, $R(E_d) = h(G_d)$ and ℓ_d have been computed.

- Calculate $|\text{Ш}(E_d)|$.

$$\text{(BSD)} \rightsquigarrow L'(E_d, 1) = \frac{\Omega c(E_d)}{\sqrt{|d|}} R(E_d) \ |\text{Ш}(E_d)|.$$

Proposition

$$|\text{Ш}(E_d)| = \frac{(|E(\mathbb{Q})_{\text{tors}}| \ |E_d(\mathbb{Q})_{\text{tors}}| \ \ell_d)^2}{|\text{Ш}(E)| c(E)^2} \ \frac{1}{* \ c(E_d)}$$

where $* = 2, 4$ or 8 is explicit.

Step 4

At this step, G_d, $R(E_d) = h(G_d)$ and ℓ_d have been computed.

- Calculate $|\text{Ш}(E_d)|$.

$$\text{(BSD)} \rightsquigarrow L'(E_d, 1) = \frac{\Omega c(E_d)}{\sqrt{|d|}} R(E_d) \quad |\text{Ш}(E_d)|.$$

Proposition

$$|\text{Ш}(E_d)| = \frac{(|E(\mathbb{Q})_{\text{tors}}| \; |E_d(\mathbb{Q})_{\text{tors}}| \; \ell_d)^2}{|\text{Ш}(E)| c(E)^2} \; \frac{1}{* \; c(E_d)}$$

where $* = 2, 4$ or 8 is explicit.

Step 4

At this step, G_d, $R(E_d) = h(G_d)$ and ℓ_d have been computed.

- Calculate $|Ш(E_d)|$.

$$\text{(BSD)} \rightsquigarrow L'(E_d, 1) = \frac{\Omega c(E_d)}{\sqrt{|d|}} R(E_d) \quad |Ш(E_d)|.$$

Proposition

$$|Ш(E_d)| = \frac{(|E(\mathbb{Q})_{\text{tors}}| \ \ |E_d(\mathbb{Q})_{\text{tors}}| \ \ \ell_d)^2}{|Ш(E)| c(E)^2} \quad \frac{1}{* \ \ c(E_d)}$$

where $* = 2, 4$ or 8 is explicit.

Summary

- We computed G_d, $R(E_d)$, $|\text{Ш}(E_d)|$ and $L'(E_d, 1)$.

This costs: $O(|d|^{1/2+\varepsilon})$ steps.

Remark: Computing $L'(E_d, 1)$ by:

$$L'(E_d, 1) = 2 \sum_{n \geq 1} \frac{a(n)}{n} \left(\frac{d}{n}\right) \int_{2\pi n/|d|\sqrt{N}}^{\infty} e^{-t} dt/t$$

needs $O(|d|)$ coefficients, the constant depending on the precision.

Summary

- We computed G_d, $R(E_d)$, $|Ш(E_d)|$ and $L'(E_d,1)$.

This costs: $O(|d|^{1/2+\varepsilon})$ steps.

Remark: Computing $L'(E_d,1)$ by:

$$L'(E_d,1) = 2\sum_{n\geq 1} \frac{a(n)}{n}\left(\frac{d}{n}\right)\int_{2\pi n/|d|\sqrt{N}}^{\infty} e^{-t}dt/t$$

needs $O(|d|)$ coefficients, the constant depending on the precision.

Example : $E = 11a1$

- $E = 11a1 \quad : \quad y^2 = x^3 - 4x^2 - 160x - 1264$.
- $\varepsilon_{11} = +1 \qquad \rightsquigarrow d = 1, 3, 4, 5, 9 \pmod{11}$.

  $\rightsquigarrow$ Number of discriminants $222900 \quad (|d| \leq 1600000)$.

Prediction

$$\frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d)^k \sim A_k T^{\frac{k}{2}} (\log T)^{\frac{k(k+1)}{2} + \mathrm{tam}_k}$$

- $M_{1/4} \sim 0.50\, T^{1/8} \log(T)^{0.027\cdots}$.
- $M_{1/2} \sim 0.23\, T^{1/4} \log(T)^{0.145\cdots}$.
- $M_{3/4} \sim 0.09\, T^{3/8} \log(T)^{0.350\cdots}$.

Example : $E = 11a1$

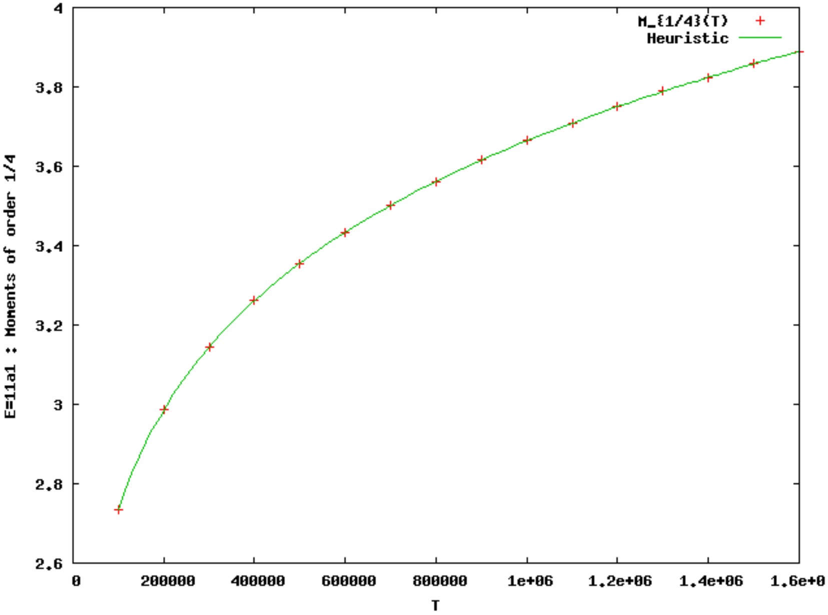
- $E = 11a1 \quad : \quad y^2 = x^3 - 4x^2 - 160x - 1264$.
- $\varepsilon_{11} = +1 \qquad \rightsquigarrow d = 1, 3, 4, 5, 9 \pmod{11}$.

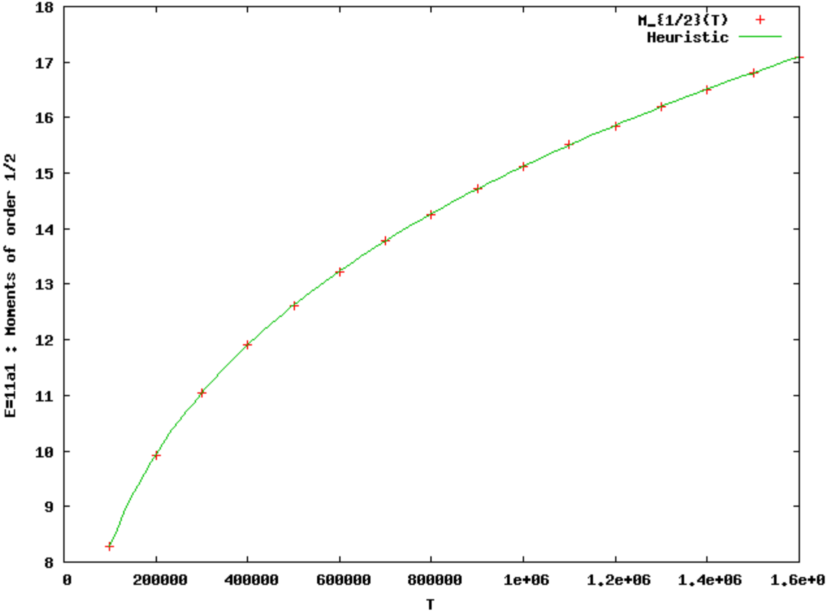
  $\rightsquigarrow$ Number of discriminants $222900 \quad (|d| \leq 1600000)$.

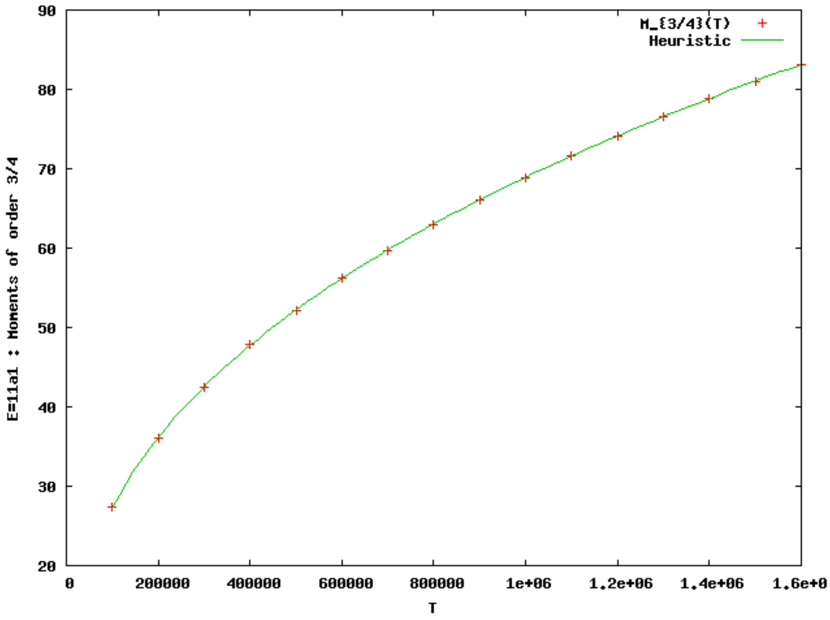
Prediction

$$\frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d)^k \sim A_k T^{\frac{k}{2}} (\log T)^{\frac{k(k+1)}{2} + \mathrm{tam}_k}$$

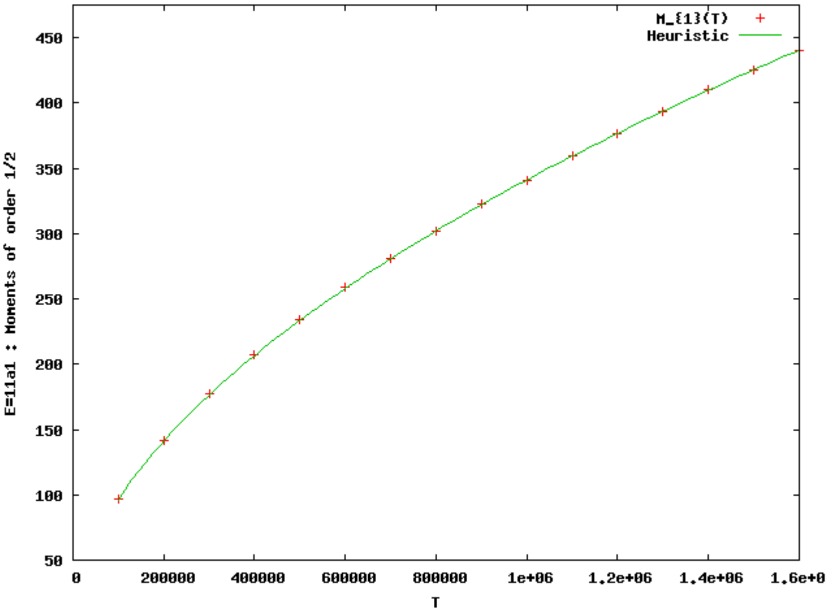
- $M_{1/4} \sim 0.50\, T^{1/8} \log(T)^{0.027\cdots}$.
- $M_{1/2} \sim 0.23\, T^{1/4} \log(T)^{0.145\cdots}$.
- $M_{3/4} \sim 0.09\, T^{3/8} \log(T)^{0.350\cdots}$.


M_{1/4}(T)
Heuristic
E=11a1 : Moments of order 1/4
T
4
3.8
3.6
3.4
3.2
3
2.8
2.6
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06
1.6e+0


M_{1/2}(T)
Heuristic
E=11a1 : Moments of order 1/2
T
18
17
16
15
14
13
12
11
10
9
8
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06
1.6e+0



M_{3/4}(T)
Heuristic
E=11a1 : Moments of order 3/4
T
90
80
70
60
50
40
30
20
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06
1.6e+0


M_{1}(T)
Heuristic
E=11a1 : Moments of order 1/2
T
450
400
350
300
250
200
150
100
50
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06
1.6e+0

What about $\text{Ш}_a(E_d)$?

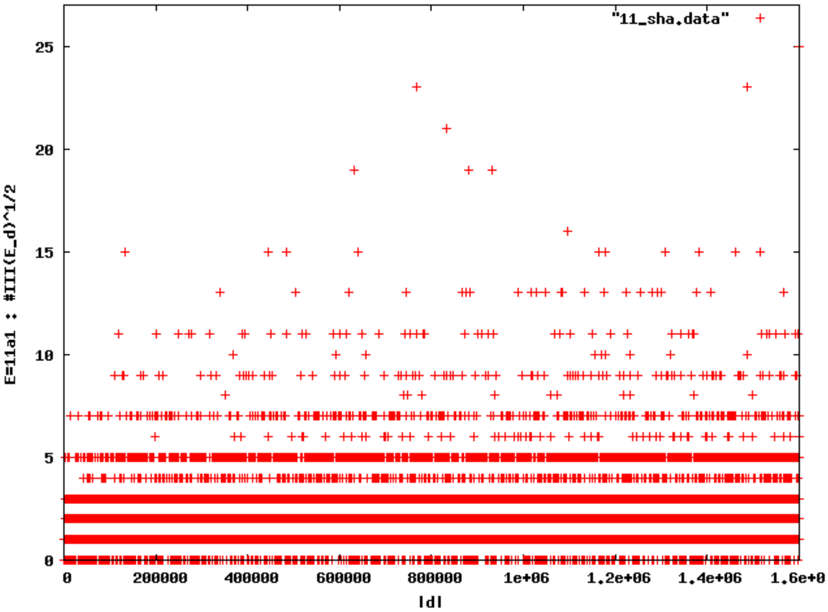
- $E = 11a1 \quad : \quad y^2 = x^3 - 4x^2 - 160x - 1264$.

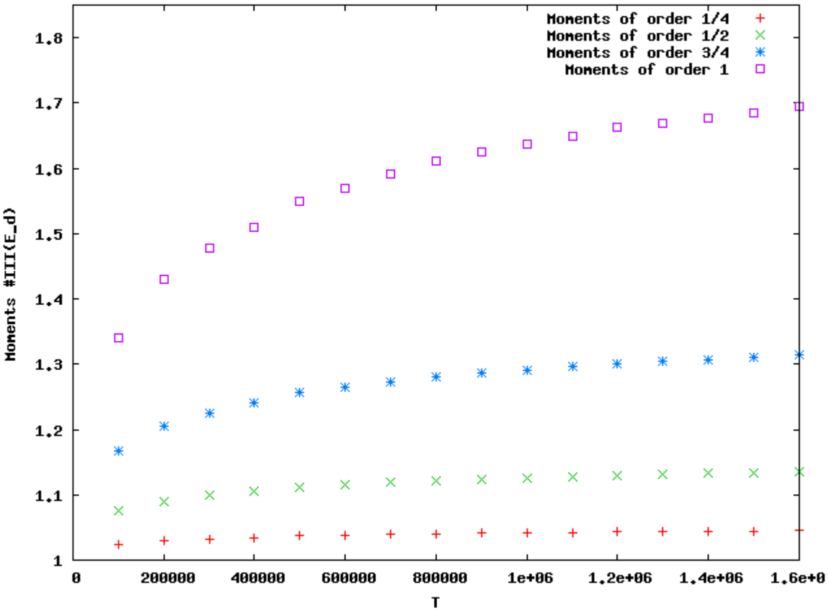
- Among the 222900 discriminants:

$\rightsquigarrow$ 671 are such that $\text{Ш}_a(E_d) = 0$.

$\rightsquigarrow$ 207277 are such that $\text{Ш}_a(E_d) = 1$.

$\rightsquigarrow$ 5551 are such that $\text{Ш}_a(E_d) = 4$.


"11_sha.data"
25
20
15
10
5
0
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06
1.6e+0
|d|
E=11a1 : #III(E_d)^1/2



Moments of order 1/4
Moments of order 1/2
Moments of order 3/4
Moments of order 1
Moments #III(E_d)
T
1
1.1
1.2
1.3
1.4
1.5
1.6
1.7
1.8
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06
1.6e+0