楕円曲線の $\mathbf{mod}\, p$ での巡回性と計算機実験

竹内 良平 (都立大・理)

1. Introduction & Result

E : $\mathbb{Q}$ 上定義された楕円曲線,
p : 素数, $\mathbb{F}_p$: p 元体

Theorem (Hasse). p を E の good prime とするとき,
(1) $\sharp E(\mathbb{F}_p) = p + 1 - a_p, \quad |a_p| \leq 2\sqrt{p}.$
(2) $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ 但し, $n_1 | n_2,\ n_1 | p-1.$

☆ $n_1 = 1 \implies E(\mathbb{F}_p)$ は巡回群

そこで 1 つ楕円曲線 $E/\mathbb{Q}$ を固定し, 素数 p を動かすとき, どのくらいの頻度で $E(\mathbb{F}_p)$ は巡回群になるのか？という問題を考える. そして, この問題を次のように定式化する.

Main Problem. $N_E(x) := \{ p \leq x \mid E(\mathbb{F}_p)$ は巡回群 $\}$ とするとき, $\sharp N_E(x)$ の大きさを求めよ.

Theorem 1. $E : y^2 = x^3 - a \ \ (a \in \mathbb{Z}_{\neq 0}),\ |a| = \prod_{i=1}^{g} p_i$ (但し, p_i たちは相異なる素数で, $\forall i : p_i \equiv 1, 5, 11 \pmod{12}$) とする.

このとき,

$$\sharp N_E(x) \sim \delta_E(x/\log x)$$

であり, δ_E の値は次のようになる.

$$\delta_E = \begin{cases} \dfrac{1}{2} + \dfrac{1}{2}(1 - A_E) \times C_k & (\text{if } \ a \equiv \pm 1 \pmod 9) \\ \dfrac{1}{2} + \dfrac{1}{2}\left(1 + \dfrac{1}{5}A_E\right) \times C_k & (\text{if } \ a \not\equiv \pm 1 \pmod 9) \end{cases}.$$

ここで,

$$A_E := \prod_{\substack{p|a \\ p \equiv 1 \,(\mathrm{mod}\, 3)}} \frac{-1}{p(p-2)} \prod_{\substack{p|a \\ p \equiv -1 \,(\mathrm{mod}\, 3)}} \frac{-1}{p^2 - 2},$$

$$C_k := \frac{5}{6} \prod_{p \equiv 1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \equiv -1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{1}{p^2 - 1}\right)$$

$$= 0.5011126 \cdots .$$

2. Known results for Main Problem

この Main Problem に対して, 次の一般的な解答が知られている.

Lemma 1. $E[m]$ で E の m-等分点 全体 (m は自然数) の集合とする. このとき, E の good prime p に対して,

$E(\mathbb{F}_p)$ が巡回群 $\iff$ $\forall q$: 素数, p は $\mathbb{Q}(E[q])$ で完全分解しない.

Theorem (Serre, R. Murty). μ を Möbius 関数とする. このとき, 一般リーマン予想 (GRH) を仮定すると,

$$\sharp N_E(x) \sim \delta_E \frac{x}{\log x} \quad \text{ここで,} \quad \delta_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}$$

で, 更には $\delta_E = 0 \Leftrightarrow \lim_{x\to\infty} \sharp N_E(x) < \infty \Leftrightarrow \mathbb{Q}(E[2]) = \mathbb{Q}$ である.

Theorem (R. Murty). E が虚数乗法 (CM) を持つとき, 上の Theorem は無条件に (GRH なしで) 成り立つ.

Theorem (R. Gupta). $E : y^2 = x^3 - ax \ \ (a \in \mathbb{Z}_{\neq 0})$ とする.
このとき $\sharp N_E(x) \sim \delta_E(x/\log x)$ で, δ_E の値は次のようになる.

$$\delta_E = \begin{cases} 0 & (\text{if } \ a \text{が平方数}) \\ \dfrac{1}{2} & (\text{if } \ -a \text{が平方数}) \\ \dfrac{1}{4} + \dfrac{1}{2} \times C_k & (\text{if } \ a \text{の} \text{square-free part} \text{が偶数}) \\ \dfrac{1}{4} + \dfrac{1}{2}\,(1 - A_E) \times C_k & (\text{otherwise}) \end{cases}.$$

ここで,

$$A_E := \prod_{\substack{p \mid a_2 \\ p \equiv 1 \,(\mathrm{mod}\, 4)}} \frac{-1}{p(p-2)} \prod_{\substack{p \mid a_2 \\ p \equiv -1 \,(\mathrm{mod}\, 4)}} \frac{-1}{p^2 - 2},$$

$$\begin{aligned} C_k &:= \frac{1}{2} \prod_{p \equiv 1 \,(\mathrm{mod}\, 4)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \equiv -1 \,(\mathrm{mod}\, 4)} \left(1 - \frac{1}{p^2 - 1}\right) \\ &= 0.388745 \cdots . \end{aligned}$$

3. Case of Mordell's curve (Outline of Proof)

Notation. $E : y^2 = x^3 - a$ $(a \in \mathbb{Z}_{\neq 0})$ として１つ固定する.
このとき, E は $k := \mathbb{Q}(\rho)$ (但し, $\rho^2 + \rho + 1 = 0$) で CM を持つ.

$\alpha \in \mathbb{Z}[\rho]$ に対し,

$k((\alpha))$: ray class field mod α,

$\varphi(\alpha) = \varphi_k(\alpha) := \sharp(\mathbb{Z}[\rho]/(\alpha))^\times$: k の Euler 関数,

$E[\alpha] := \{P \in E(\mathbb{C}) \,|\, \alpha P = \mathcal{O}\}$, $E^x[\alpha] := \{x \,|\, P = (x, y) \in E[\alpha]\}$,

$K_\alpha := k(E[\alpha])$, $K_\alpha^x := k(E^x[\alpha])$.

$a \in \mathbb{Z}_{\neq 0}$ に対し,

a_2, a_3 : それぞれ a の square-free part, cube-free part,

$\mathfrak{f}_2 = (f_2)$, $\mathfrak{f}_3 = (f_3)$: それぞれ $k(\sqrt{3a_2})/k$, $k(\sqrt[3]{a_3})/k$ の導手.

Fact 1. $K_{1-\rho} = k(\sqrt{3a_2}),\ K_2 = k(\sqrt[3]{a_3})$.

Fact 2. $\widehat{a_2} := \begin{cases} 3|a_2| & (\text{if } 3 \nmid a_2) \\ |a_2/3| & (\text{if } 3 \mid a_2) \end{cases},\ \widetilde{a_3} := \prod_{p|a_3} p$ とすると,

$$f_2 = \begin{cases} \widehat{a_2} & (\text{if } a_2 \equiv -1 \pmod 4) \\ 4\widehat{a_2} & (\text{if } a_2 \not\equiv -1 \pmod 4) \end{cases},\ f_3 = \begin{cases} \widetilde{a_3} & (\text{if } a_3 \equiv \pm 1 \pmod 9) \\ 3\widetilde{a_3} & (\text{if } a_3 \not\equiv \pm 1 \pmod 9) \end{cases}.$$

Fact 3. $(\alpha, \beta) = 1 \Rightarrow K_{\alpha\beta} = K_\alpha K_\beta$.

$K_\alpha, K_\alpha^x : \text{Galois}/k,\ [K_\alpha : K_\alpha^x] \leq 2$.

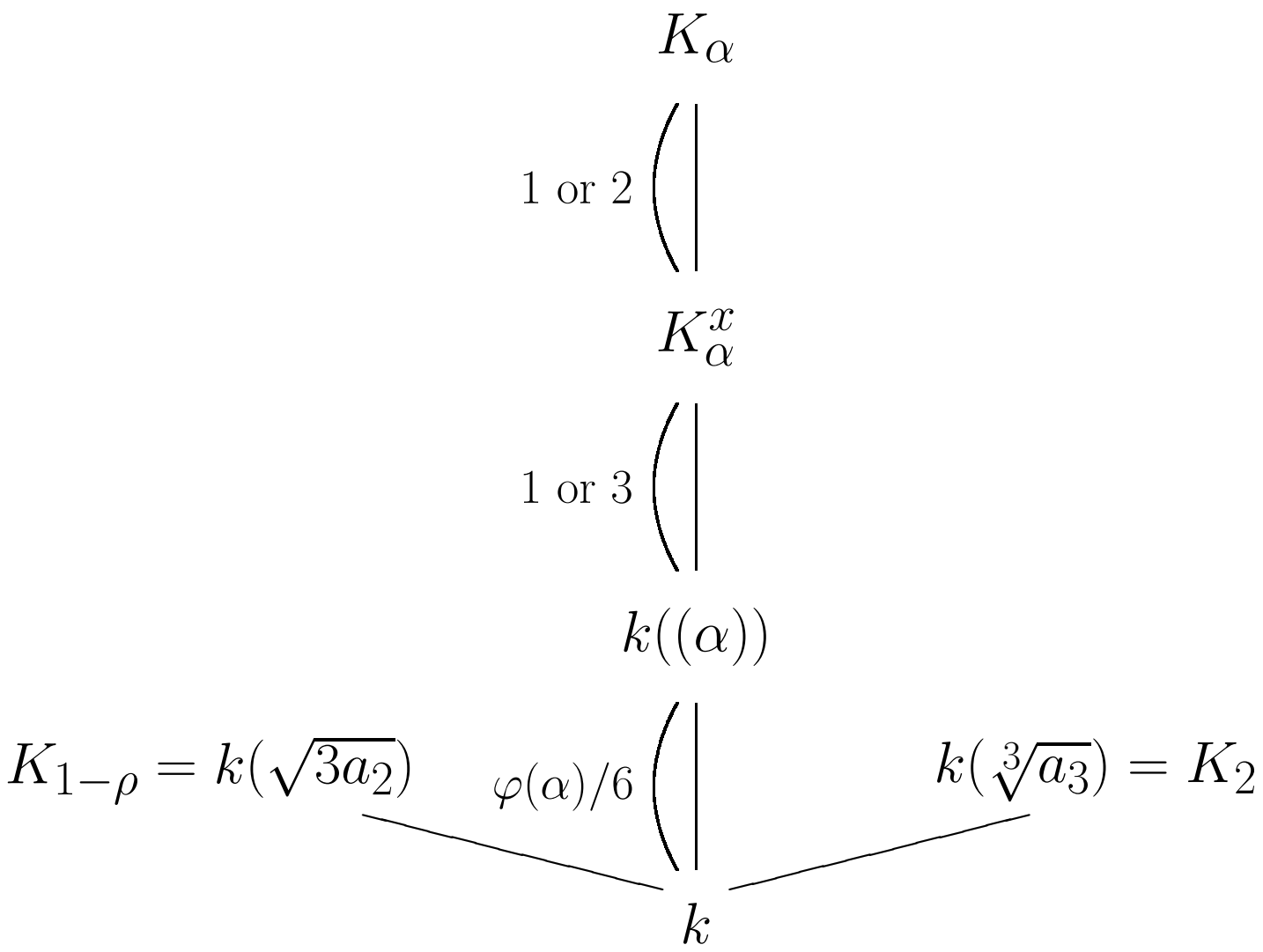
$\text{Gal}(K_\alpha/k) \hookrightarrow (\mathbb{Z}[\rho]/(\alpha))^\times,\ \text{Gal}(K_\alpha^x/k) \hookrightarrow (\mathbb{Z}[\rho]/(\alpha))^\times/\{\pm 1\}$.

CM-theory から,

$$k((\alpha)) = k((E^x[\alpha])^3) \quad \text{where } (E^x[\alpha])^3 := \{x^3 \mid x \in E^x[\alpha]\}.$$

$$\therefore\ K_\alpha^x \supset k((\alpha)).\ \text{更に}, [k((\alpha)) : k] = \begin{cases} \varphi(\alpha)/3 = 1 & (\text{if } (\alpha) = (2)) \\ \varphi(\alpha)/6 & (\text{if } (\alpha) \neq (2)) \end{cases}$$

であるので, 結局 $\varphi(\alpha)/6 \leq [K_\alpha : k] \leq \varphi(\alpha)$ を得る.


K_α
1 or 2
K_α^x
1 or 3
$k((\alpha))$
$K_{1-\rho} = k(\sqrt{3a_2})$
$\varphi(\alpha)/6$
$k(\sqrt[3]{a_3}) = K_2$
k

Theorem 2. $E : y^2 = x^3 - a \ \ (a \in \mathbb{Z}_{\neq 0}),\ \ |a| = \prod_{i=1}^{g} p_i$ (但し, p_i たちは相異なる素数で, $\forall i : p_i \equiv 1, 5, 11 \pmod{12}$) とする.
このとき, $\alpha \in \mathbb{Z}[\rho]$ に対して,

$$[K_\alpha : k] = \begin{cases} \varphi(\alpha) & (\text{if } \ (1-\rho)f_2 \nmid \alpha \ \text{ and } \ 2f_3 \nmid \alpha) \\ \varphi(\alpha)/2 & (\text{if } \ (1-\rho)f_2 \mid \alpha \ \text{ and } \ 2f_3 \nmid \alpha) \\ \varphi(\alpha)/3 & (\text{if } \ (1-\rho)f_2 \nmid \alpha \ \text{ and } \ 2f_3 \mid \alpha) \\ \varphi(\alpha)/6 & (\text{if } \ (1-\rho)f_2 \mid \alpha \ \text{ and } \ 2f_3 \mid \alpha) \end{cases}.$$

Proposition 1. $a = \pi_1 \cdots \pi_g \ \text{in} \ \mathbb{Z}[\rho]$, 但し $\forall i,\ \mathcal{N}(\pi_i) \equiv 1 \pmod 4$.

(1) $(1-\rho) \nmid \alpha$ であれば, $\sqrt{3a_2} \in K_\alpha \ \Leftrightarrow \ f_2 \mid \alpha$.

(2) $(1-\rho)f_2 \nmid \alpha$ であれば, $[K_\alpha : k] = \varphi(\alpha) \ \text{or} \ \varphi(\alpha)/3$.

Proposition 2. $2 \nmid a,\ 3 \nmid a$ のとき,

(1) $2 \nmid \alpha$ であれば, $\sqrt[3]{a_3} \in K_\alpha \ \Leftrightarrow \ f_3 \mid \alpha$.

(2) $2f_3 \nmid \alpha$ であれば, $[K_\alpha : k] = \varphi(\alpha) \ \text{or} \ \varphi(\alpha)/2$.

Lemma 2 (R. Murty). k : 類数 1 の虚二次体, $E/\mathbb{Q}$: k の order で CM を持つ楕円曲線, とする. このとき $m > 2$ ならば, $\mathbb{Q}(E[m])$ は k を含む. すなわち, $\mathbb{Q}(E[m]) = K_m$ である.

Lemma 3 (Euler 積展開).

$$
\begin{aligned}
C_k &:= \sum_{m=1}^{\infty} \frac{\mu(m)}{\varphi(m)} \\
&= \prod_{p=3} \left(1 - \frac{1}{p(p-1)}\right) \prod_{p \equiv 1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \equiv -1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{1}{p^2-1}\right) \\
&= \frac{5}{6} \prod_{p \equiv 1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \equiv -1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{1}{p^2-1}\right) .
\end{aligned}
$$

4. 計算機実験

Millerのアルゴリズム$\cdots E(\mathbb{F}_p)$の群構造を決定する.

$$\left.\begin{array}{c} \sharp E(\mathbb{F}_p)\text{の計算} \\ \mathrm{GCD}(\sharp E(\mathbb{F}_p), p-1)\text{の素因数分解} \end{array}\right\} \text{以外は実用的多項式時間.}$$

これを**PARI-GP**に実装 $\Longrightarrow \sharp E(\mathbb{F}_p)$を計算してくれる$p$なら$\mathrm{OK}$.

☆ $\boldsymbol{\delta_E(x) = \sharp N_E(x)/\pi(x)}$ の値 (xまでの**density**) を表示.

$(N_E(x) = \{\, p \le x \mid E(\mathbb{F}_p)\text{は巡回群}\,\},\ \pi(x) : x\text{以下の素数の個数})$

《例》

164840/220000=0.749272727272727272727272727272727272

172275/230000=0.749021739130434782608695652173913043 47

179726/240000=0.748858333333333333333333333333333333

$\sharp N_E(x)$　$\pi(x)$　　$x \fallingdotseq (240000\text{-th prime}) = 3346601$

Example 1. $a = 5 \not\equiv \pm 1 \pmod 9$, $E : y^2 = x^3 - 5$,

$$\delta_E = \frac{1}{2} + \frac{57}{115}\, C_k = 0.74837754956521739 13 \cdots$$

```
2X,3X,5X,OK!
7509/10000=0.75090000000000000000000000000000000001
15004/20000=0.75020000000000000000000000000000000000
22530/30000=0.75100000000000000000000000000000000000
29947/40000=0.74867500000000000000000000000000000000
37492/50000=0.74984000000000000000000000000000000000
44984/60000=0.74973333333333333333333333333333333333
52462/70000=0.74945714285714285714285714285714285714
59944/80000=0.74930000000000000000000000000000000000
67417/90000=0.74907777777777777777777777777777777777
74911/100000=0.74911000000000000000000000000000000000
82420/110000=0.74927272727272727272727272727272727272
89884/120000=0.74903333333333333333333333333333333333
97347/130000=0.74882307692307692307692307692307692307
104841/140000=0.74886428571428571428571428571428571428
112407/150000=0.74938000000000000000000000000000000000
119878/160000=0.74923750000000000000000000000000000000
127391/170000=0.74935882352941176470588235294117647058
134883/180000=0.74935000000000000000000000000000000000
142372/190000=0.74932631578947368421052631578947368421
149848/200000=0.74924000000000000000000000000000000000
157389/210000=0.74947142857142857142857142857142857142
164840/220000=0.74927272727272727272727272727272727272
172275/230000=0.74902173913043478260869565217391304347
179726/240000=0.74885833333333333333333333333333333333
                    ⋮
374413/500000=0.74882599999999999999999999999999999999
381862/510000=0.74874901960784313725490196078431372548
389273/520000=0.74860192307692307692307692307692307692
396687/530000=0.74846603773584905660377358490566037735

prime(530003)=7844801
```

Example 2. $a = -17 \equiv 1 \pmod 9$, $E : y^2 = x^3 + 17$,

$$\delta_E = \frac{1}{2} + \frac{144}{287}\, C_k = 0.75142931846689895 47\cdots$$

```
2X,3X,17X,OK!
7518/10000=0.751800000000000000000000000000000000000000000
15036/20000=0.7518000000000000000000000000000000000000000000
22575/30000=0.7525000000000000000000000000000000000000000000
30095/40000=0.7523750000000000000000000000000000000000000000
37591/50000=0.7518200000000000000000000000000000000000000000
45078/60000=0.7513000000000000000000000000000000000000000000
52675/70000=0.7525000000000000000000000000000000000000000000
60178/80000=0.7522250000000000000000000000000000000000000000
67712/90000=0.7523555555555555555555555555555555555555555555
75210/100000=0.7521000000000000000000000000000000000000000000
82745/110000=0.7522272727272727272727272727272727272727272272
90192/120000=0.7516000000000000000000000000000000000000000000
93936/125000=0.7514880000000000000000000000000000000000000000
97727/130000=0.7517461538461538461538
```

Example 3. $a = 56877643 = 23 \cdot 197 \cdot 12553 \equiv 1 \pmod 9$,

$[\ 23 \equiv 11 \pmod{12},\ 197 \equiv 5 \pmod{12},\ 12553 \equiv 1 \pmod{12}\ ]$

$E : y^2 = x^3 - 56877643, \quad \mathrm{rank}_{\mathbb{Q}} E = 7$ (Womack(2000))

$$\delta_E = \frac{1}{2} + \frac{1611077930892084}{3222155861784167}\, C_k = 0.7505563\cdots$$

```
2X,3X,23X,197X,12553X,OK!
7561/10000=0.75610000000000000000000000000000000000000000
15067/20000=0.75335000000000000000000000000000000000000000
22602/30000=0.75340000000000000000000000000000000000000000
30090/40000=0.75225000000000000000000000000000000000000000
37640/50000=0.75280000000000000000000000000000000000000000
75065/100000=0.75065000000000000000000000000000000000000000
150199/200000=0.75099500000000000000000000000000000000000000
187797/250000=0.75118800000000000000000000000000000000000000
225387/300000=0.75129000000000000000000000000000000000000000
262833/350000=0.75095142857142857142857142857142857142857142
300493/400000=0.75123250000000000000000000000000000000000000
338065/450000=0.75125555555555555555555555555555555555555555
375673/500000=0.75134600000000000000000000000000000000000000
413167/550000=0.75121272727272727272727272727272727272727272
450675/600000=0.75112500000000000000000000000000000000000000
488109/650000=0.75093692307692307692307692307692307692307692
525592/700000=0.75084571428571428571428571428571428571428571
563281/750000=0.75104133333333333333333333333333333333333333
600735/800000=0.75091875000000000000000000000000000000000000
638229/850000=0.75085764705882352941176470588235294117647058
675752/900000=0.75083555555555555555555555555555555555555555
713255/950000=0.75079473684210526315789473684210526315789473
720772/960000=0.75080416666666666666666666666666666666666666
728283/970000=0.75080721649484536082474226804123711340206185
735769/980000=0.75078469387755102040816326530612244897959183
743271/990000=0.75077878787878787878787878787878787878787878
750764/1000000=0.75076400000000000000000000000000000000000000

?prime(1000005)=15485941
```

☆ **non-CM case**

Fact. $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$

Theorem (Serre). 楕円曲線 E は CM を持たないものとする. このとき, 高々有限個の素数 p を除いて,

$$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_p).$$

即ち, 有限個の素数 p を除いて, $[\mathbb{Q}(E[p]) : \mathbb{Q}] = (p^2-1)(p^2-p)$.

ここで, 例外となる有限個の p を E の exceptional prime という.

- 任意の square-free な m に対して, $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$

という条件を E に仮定すると, density δ_E の値は次の様になる.

$$C_{\mathrm{non-CM}} := \sum_{m=1}^{\infty} \frac{\mu(m)}{\sharp \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})} = \prod_p \left(1 - \frac{1}{(p^2-1)(p^2-p)}\right)$$
$$= 0.8137519061\cdots.$$

Example 4. $E : y^2 + y = x^3 - x$, conductor $N = 37$
Exceptional prime : Nothing, $C_{\mathrm{non-CM}} = 0.8137519061\cdots$.

```
37X,OK!
40729/50000=0.81458000000000000000000000000000000000000000
81425/100000=0.81425000000000000000000000000000000000000000
122096/150000=0.81397333333333333333333333333333333333333333
162776/200000=0.81388000000000000000000000000000000000000000
203489/250000=0.81395600000000000000000000000000000000000000
244164/300000=0.81388000000000000000000000000000000000000000
284863/350000=0.81389428571428571428571428571428571428571428
325571/400000=0.81392750000000000000000000000000000000000000
366190/450000=0.81375555555555555555555555555555555555555555
406903/500000=0.81380600000000000000000000000000000000000000
447577/550000=0.81377636363636363636363636363636363636363636
488254/600000=0.81375666666666666666666666666666666666666666
528948/650000=0.81376615384615384615384615384615384615384615
569645/700000=0.81377857142857142857142857142857142857142857
610315/750000=0.81375333333333333333333333333333333333333333
650974/800000=0.81371750000000000000000000000000000000000000
691667/850000=0.81372588235294117647058823529411764705882352
732475/900000=0.81386111111111111111111111111111111111111111
773251/950000=0.81394842105263157894736842105263157894736842
814005/1000000=0.81400500000000000000000000000000000000000000
854610/1050000=0.81391428571428571428571428571428571428571428
895269/1100000=0.81388090909090909090909090909090909090909090
935982/1150000=0.81389739130434782608695652173913043478260869
976764/1200000=0.81397000000000000000000000000000000000000000
1017396/1250000=0.81391680000000000000000000000000000000000000
1058169/1300000=0.81397615384615384615384615384615384615384615
1098778/1350000=0.81390962962962962962962962962962962962962962
1139396/1400000=0.81385428571428571428571428571428571428571428

?prime(1400001)=22182379
```

Example 5. $E : y^2 + y = x^3 + x^2$, conductor $N = 43$
Exceptional prime : Nothing, $C_{\mathrm{non-CM}} = 0.8137519061\cdots$.

```
43X,OK!
81541/100000=0.81541000000000000000000000000000000000000000
162936/200000=0.81468000000000000000000000000000000000000000
244266/300000=0.81422000000000000000000000000000000000000000
325789/400000=0.81447250000000000000000000000000000000000000
407130/500000=0.81426000000000000000000000000000000000000000
488483/600000=0.81413833333333333333333333333333333333333333
569798/700000=0.81399714285714285714285714285714285714285142
651273/800000=0.81409125000000000000000000000000000000000000
732776/900000=0.81419555555555555555555555555555555555555555
814233/1000000=0.81423300000000000000000000000000000000000000
903544/1110000=0.81400360360360360360360360360360360360360360
976897/1200000=0.81408083333333333333333333333333333333333333
1017691/1250000=0.81415280000000000000000000000000000000000000
1058281/1300000=0.81406230769230769230769230769230769230769230
1098916/1350000=0.81401185185185185185185185185185185185185185
1139658/1400000=0.81404142857142857142857142857142857142857142
1180269/1450000=0.81397862068965517241379310344827586206896551
1220852/1500000=0.81390133333333333333333333333333333333333333
1261409/1550000=0.81381225806451612903225806451612903225806451
1302082/1600000=0.81380125000000000000000000000000000000000000
1342650/1650000=0.81372727272727272727272727272727272727272727
1383467/1700000=0.81380411764705882352941176470588235294117647
1424087/1750000=0.81376400000000000000000000000000000000000000
1464805/1800000=0.81378055555555555555555555555555555555555555
1505401/1850000=0.81373027027027027027027027027027027027027027
1546044/1900000=0.81370736842105263157894736842105263157894736
1586753/1950000=0.81371948717948717948717948717948717948717948
1627425/2000000=0.81371250000000000000000000000000000000000000

?prime(2000000)=32452843
```

Example 6. $E : y^2 + y = x^3 - x^2$, conductor $N = 11$

Exceptional prime : 5, $[\mathbb{Q}(E[5]) : \mathbb{Q}] = 20$, $(\sharp \mathrm{GL}_2(\mathbb{F}_5) = 480)$

$$\frac{456}{479}\, C_{\mathrm{non-CM}} = \left(1 - \frac{1}{20}\right) \prod_{p \neq 5} \left(1 - \frac{1}{(p^2-1)(p^2-p)}\right)$$
$$= 0.7746782237611691 \cdots .$$

```
11X,OK!
19438/25000=0.777520000000000000000000000000000000000000000
38804/50000=0.776080000000000000000000000000000000000000000
58160/75000=0.775466666666666666666666666666666666666666666
77570/100000=0.775700000000000000000000000000000000000000000
97009/125000=0.776072000000000000000000000000000000000000000
116405/150000=0.776033333333333333333333333333333333333333333
135661/175000=0.775205714285714285714285714285714285714285714
155040/200000=0.775200000000000000000000000000000000000000000
174448/225000=0.775324444444444444444444444444444444444444444
193831/250000=0.775324000000000000000000000000000000000000000
213186/275000=0.775221818181818181818181818181818181818181818
232476/300000=0.774920000000000000000000000000000000000000000
251768/325000=0.774670769230769230769230769230769230769230769
271146/350000=0.774702857142857142857142857142857142857142857
290557/375000=0.774818666666666666666666666666666666666666666
309824/400000=0.774560000000000000000000000000000000000000000
329167/425000=0.774510588235294117647058823529411764705882352
348525/450000=0.774500000000000000000000000000000000000000000
367913/475000=0.774553684210526315789473684210526315789473684
387320/500000=0.774640000000000000000000000000000000000000000

?prime(500000)=7368787
```

Example 7. $E : y^2+y = x^3-x^2-10x-20$, conductor $N = 11$

Exceptional prime : 5, $\quad \mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$, $\quad ([\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4)$

$$\frac{360}{479}\, C_{\mathrm{non-CM}} = \left(1-\frac{1}{4}\right)\prod_{p\neq 5}\left(1-\frac{1}{(p^2-1)(p^2-p)}\right)$$
$$= 0.61158807139039665 97\cdots .$$

```
11X,OK!
6143/10000=0.614300000000000000000000000000000000000000000000000
12256/20000=0.612800000000000000000000000000000000000000000000000
18381/30000=0.612700000000000000000000000000000000000000000000000
24510/40000=0.612750000000000000000000000000000000000000000000000
30605/50000=0.612100000000000000000000000000000000000000000000000
36729/60000=0.612150000000000000000000000000000000000000000000000
42860/70000=0.612285714285714285714285714285714285714285714285714
48951/80000=0.611887500000000000000000000000000000000000000000000
55071/90000=0.611900000000000000000000000000000000000000000000000
61207/100000=0.612070000000000000000000000000000000000000000000000
67369/110000=0.612445454545454545454545454545454545454545454545454
73479/120000=0.612325000000000000000000000000000000000000000000000
79630/130000=0.612538461538461538461538461538461538461538461538461
85732/140000=0.612371428571428571428571428571428571428571428571428
91899/150000=0.612660000000000000000000000000000000000000000000000

?prime(150000)=2015177
```