楕円曲線の $\mathbf{F}_p$ 有理点の群構造

中島 匠一 (学習院大学)

有理数体上の楕円曲線 E を素数 p でリダクションすると, $\mathbf{F}_p$ 有理点の群 $E(\mathbf{F}_p)$ ができる ($\mathbf{F}_p$ は p 元体を表す). 筆者は学習院大学の大学院生だった萩原賢紀君 (現在は佼成学園に勤務) と共同で, E を固定して p を動かしたときの $E(\mathbf{F}_p)$ の群構造の分布を調べて, いくつかの知見を得た. 講演では数値実験の結果を紹介し, そこから得られた予測について述べた. 講演時に「現在研究が進展中」と言っていた事柄 (最後の節参照) については, まだ結論が出せていない. したがって, 残念ながら, この報告には講演の時以上の結果を盛り込むことはできなかったことをおことわりしておく.

1 問題の設定

有理数体 $\mathbf{Q}$ 上の楕円曲線 E を考えると, E は射影平面 (射影座標を $[X:Y:Z]$ とする) 内で

$$E:\ Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \quad (a,b,c \in \mathbf{Z})$$

と表せ, E は無限遠点 $\mathcal{O} = [0:1:0]$ を単位元とする群の構造をもつ. ここで E の判別式を Δ_E とすれば, Δ_E は 0 でない整数であり, 素数 p が Δ_E の約数でないときには, E を法 p でリダクションしたものが $\mathbf{F}_p$ 上の楕円曲線となることがわかっている. このような素数 p を E の good prime と呼ぶが, 以下, この報告では

$$p \text{ は奇素数で, } E \text{ の good prime である}$$

と仮定して話を進める. (もちろん, そのような p は無限個存在する.) 簡単にわかることだが, E の $\mathbf{F}_p$ 有理点の集合 $E(\mathbf{F}_p)$ は

$$E(\mathbf{F}_p) = \{(x,y) \in \mathbf{F}_p^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}$$

と表される.

楕円曲線に関する基礎理論によって, $E(\mathbf{F}_p)$ について次のことが知られている.

FACT. 有限アーベル群として

$$E(\mathbf{F}_p) \cong \mathbf{Z}/n_{1,p}\mathbf{Z} \oplus \mathbf{Z}/n_{2,p}\mathbf{Z}$$

が成り立つような自然数 $n_{1,p}, n_{2,p}$ で

$$n_{1,p} \text{ は } n_{2,p} \text{ の約数}$$

をみたすようなものが唯 1 組定まる. ここで, 自然数 n に対して, $\mathbf{Z}/n\mathbf{Z}$ は位数 n の巡回群を表す.

まず $n_{1,p}, n_{2,p}$ について簡単にわかることを挙げておく.

(1) $E(\mathbf{F}_p)$ の元の個数を $|E(\mathbf{F}_p)|$ で表せば, 明らかに

$$|E(\mathbf{F}_p)| = n_{1,p}n_{2,p}$$

が成り立つので, $n_{1,p}, n_{2,p}$ がわかれば $|E(\mathbf{F}_p)|$ がわかる. しかし, このことの逆は成り立たず, $|E(\mathbf{F}_p)|$ だけでは $n_{1,p}, n_{2,p}$ の各々は定まらない. したがって, E の $\mathbf{F}_p$ 上の合同ゼータ関数がわかっても, それだけでは $n_{1,p}, n_{2,p}$ は決定できない.

(2) $n_{2,p}$ はアーベル群 $E(\mathbf{F}_p)$ の exponent に等しく, また

$$n_{1,p} = 1 \quad \Longleftrightarrow \quad E(\mathbf{F}_p) \text{ は巡回群}$$

が成り立つ.

以上の記号のもとで, 我々の問題設定は次のようなものである:

楕円曲線 E を固定し素数 p を動かすときに, 自然数の組 $(n_{1,p}, n_{2,p})$ はどのように分布するか?

更に具体的にいうと, 次の 2 つの問題について考察した.

問題 1. p を動かすとき, $n_{1,p}$ はどんな分布をするか.

問題 2. p を動かすとき, $\dfrac{n_{2,p}}{n_{1,p}}$ はどんな分布をするか.

これらの問題について, 我々はまず数値実験をおこない, その結果を受けていくつかの予測をした. ただ, 問題 2 の数値実験からはまだ一般的な法則を予測するには至っていない. したがって, ここでは問題 1 についてだけ報告することにした.

我々の結果は第 3 節で述べることにして, 次節ではこれまでに知られていた結果をまとめる.

2 既知の結果

$(n_{1,p}, n_{2,p})$ の分布については, まず「いつ $n_{1,p} = 1$ となるか」という問題が注目された. 1975 年に Borosch-Moreno-Porta が計算機による数値実験を発表したが, その論文で「頻繁に $n_{1,p} = 1$ となる」ことを指摘した. この結果を受けて, 1976 年に Serre が代数体の GRH (= 一般リーマン仮説) を仮定すれば

$$c_E(1) = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbf{Q}(E[k]) : \mathbf{Q}]}$$

とおくとき, 漸近式

$$|\{p < x \mid n_{1,p} = 1\}| \sim C_E(1)\frac{x}{\log x} \quad (x \to \infty)$$

が成り立つことを示した. ただし, $\mu(k)$ はメビウス関数, $E[k]$ は E の k 等分点の集合, $\mathbf{Q}(E[k])$ は $E[k]$ の点の座標が $\mathbf{Q}$ 上生成する体を表している. さらに Serre は, $\mathbf{Q}(E[2]) = \mathbf{Q}$ となる場合を除けば $C_E(1) > 0$ であることを予測したが, これは 2004 年までには M.R.Murty, R.Gupta, A.C.Cojocaru により証明された. (Serre の結果を GRH なしで証明する試みも数多くなされているが, それについては省略する.)

このように $n_{1,p}=1$ についてある程度の結果がでたあと, 2003 年頃に R.Takeuchi (竹内良平氏) が一般の $n_{1,p}$ の値分布について数値実験をおこなった. その結果, 彼は, 任意の自然数 n について

$$c_E(n)=\sum_{k\geq 1}\frac{\mu(k)}{[\mathbf{Q}(E[nk]):\mathbf{Q}]}$$

とおくとき

$$|\{p<x\mid n_{1,p}=n\}|\sim C_E(n)\frac{x}{\log x}\quad(x\to\infty)$$

が成り立つだろうと予想した. この予想は, 2004 年に A.C.Cojocaru によって証明さた (一部 GRH を仮定; また, 誤差項の評価もなされている).

以上のように $(n_{1,p},n_{2,p})$ の分布については多くの結果があるが, $n\geq 2$ の場合には「いつ $C_E(n)>0$ であるか？」という問題についてはほとんど何もわかっていなかったようである. 我々の数値実験の結果として, この問題に対する部分的な結果と予測が得られたので, 次節以降でそれについて述べる.

3 Mapleによる数値実験と一般法則の予測

第 1 節で述べた問題について, 我々は数式処理ソフト Maple11 を使って数値実験をおこなった. 作成したプログラムは, 楕円曲線 E と素数 p を入力して $(n_{1,p},n_{2,p})$ を出力するものである. 実際のプログラム作成とデータの整理は萩原君に担当してもらって, その詳しい結果は萩原君の修士論文に述べられている. ここでは $n_{1,p}$ の取りうる値 (第 1 節の問題 1) に関係するデータを紹介する.

我々のプログラムは任意の楕円曲線に有効であるので, non-CM 型楕円曲線についてもデータは得られている. しかし, non-CM の場合には非常に高い割合の p について $n_{1,p}\leq 2$ となってしまっており, 一般的な分布について何かを予測するにはデータ不足であることは否定できない. これに対して, E が CM 型であるときは我々の実験した範囲の数値から一般的な予測ができそうであった. 我々は CM 型の中でも, ガウス整数環 $\mathbf{Z}[\sqrt{-1}]$ を準同型環にもつ曲線

$$y^2=x^3+bx\quad(b\in\mathbf{Z})$$

を特に詳しく調べることとして,

$$|b|\leq 20,\quad p<8\times 10^4$$

の範囲で計算を実行しデータを集積した. 以下, そのデータから作成したグラフを紹介する.

虚数乗法の環が $\mathbf{Z}[\sqrt{-1}]$ であることから, 素数 p を

- $p\equiv 1\pmod 4$
- $p\equiv 3\pmod 4$

の 2 組に分けることは自然である. この各々の場合に関して

> 横軸に b を取り, 縦軸に自然数 n を取って
> $n_{1,p}=n$ となる p が存在するときは $\circ$, 存在しないときは $+$ をつける.

として, グラフを作成した (b を定めることは E を定めるのと同じであることに注意). $p\equiv 3\pmod 4$ の場合のほうが結果は単純で, グラフは次のようになった.

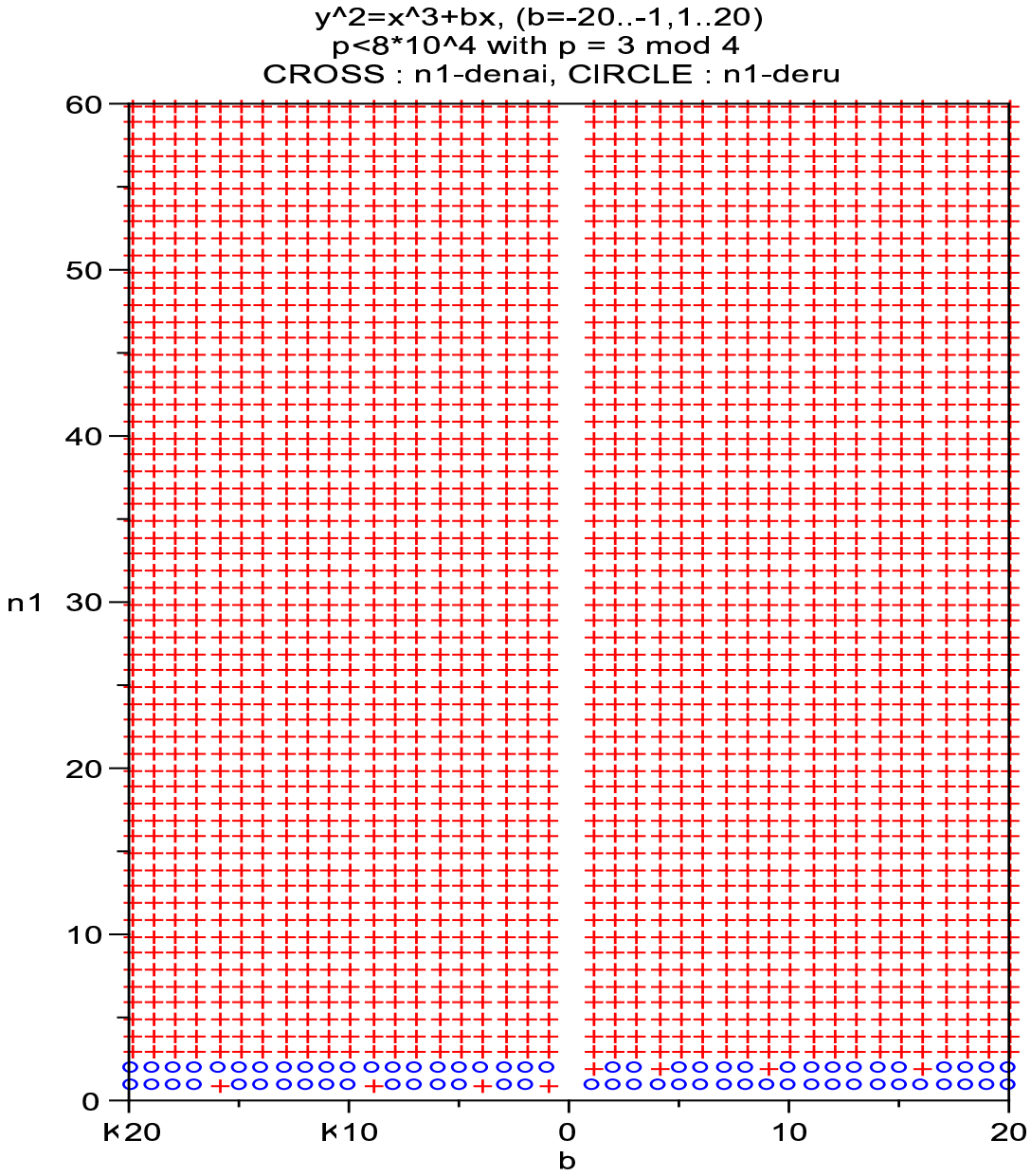

図 1: $p \equiv 3 \pmod 4$

これと比較して $p \equiv 1 \pmod 4$ のときのグラフはまったく違う様子をしていて, 次のようなものである.

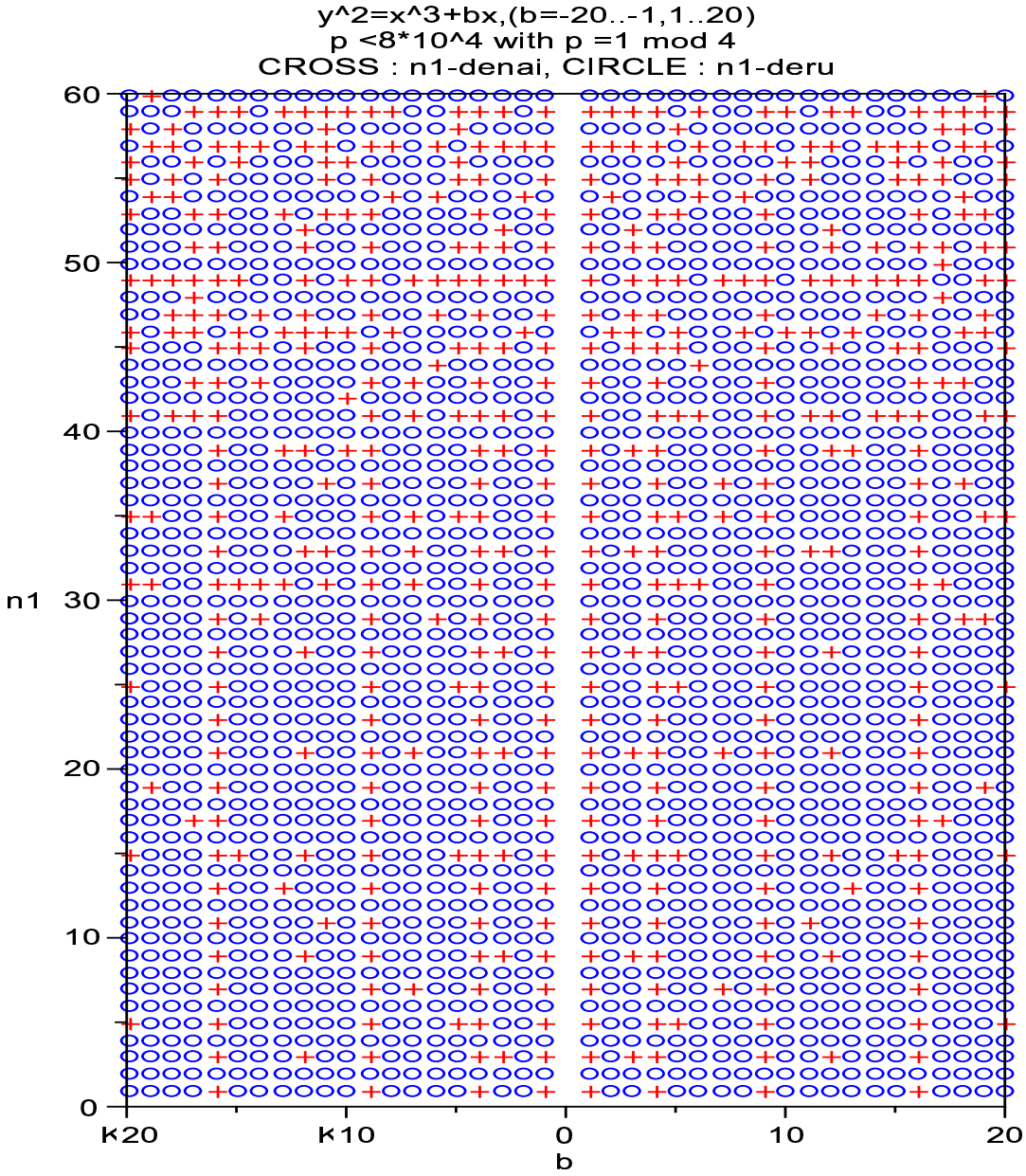

図 2: $p \equiv 1 \pmod 4$

実は, 虚数乗法を持つ楕円曲線の一般論を知っていれば $p \equiv 3 \pmod 4$ の場合の結果はすぐに証明ができる (特に, $n_{1,p} \leq 2$ であることがわかる). これに対して $p \equiv 1 \pmod 4$ の場合の分布はどのような法則があるかがはっきりしない. そこで, 更に分析を続けた結果, 曲線の係数の b を

$$b = b_0^2 \cdot b_1 \quad (b_0 \in \mathbf{N}, b_1 \text{ は square free})$$

と分解し, b_1 が偶数・奇数で場合分けするといいことに気付いた.

まず, b_1 が偶数の場合のグラフは下の通りである.

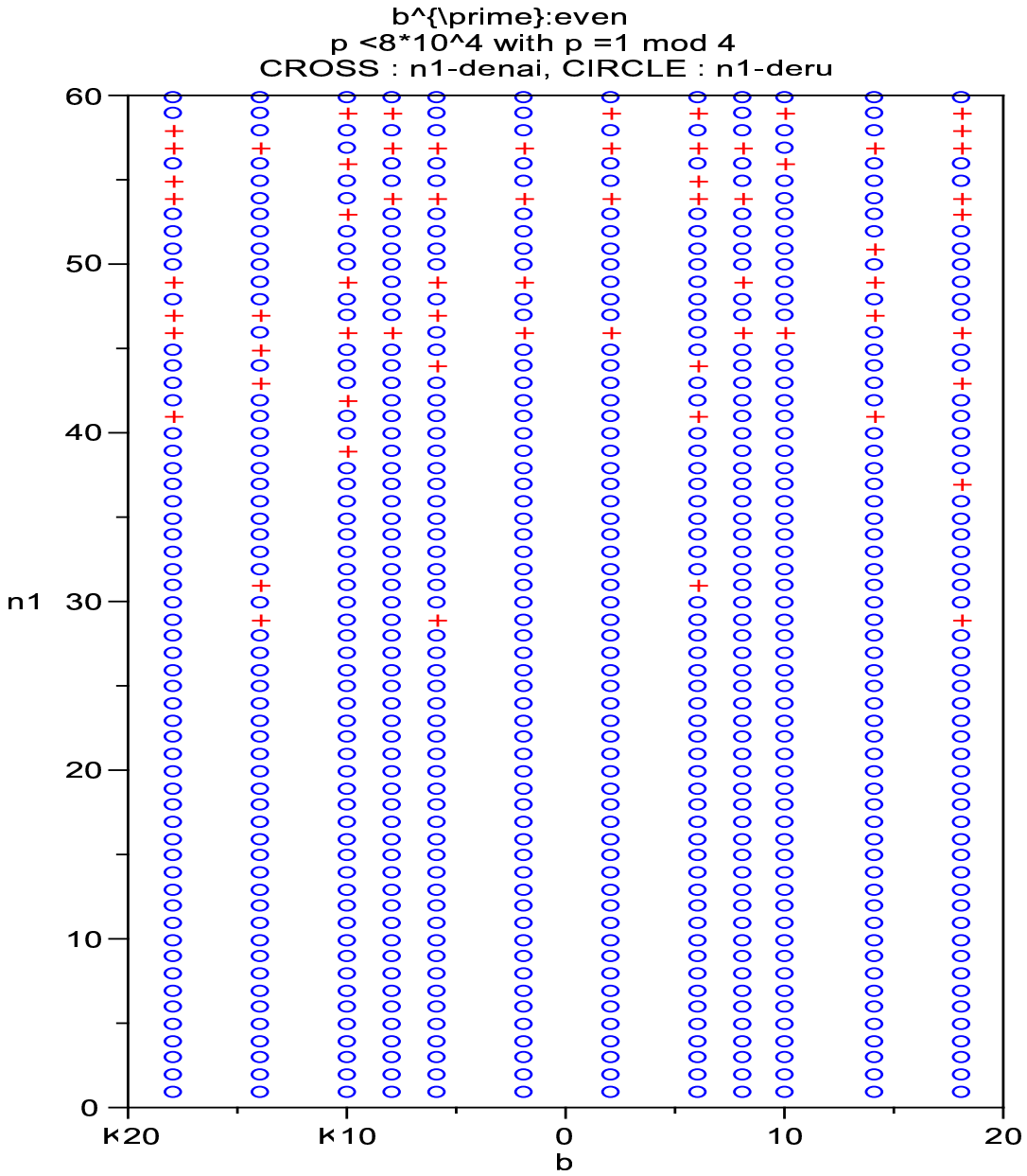

図 3: b_1 が偶数, $p \equiv 1 \pmod 4$ のとき

そして, b_1 が奇数の場合はこうなっている.

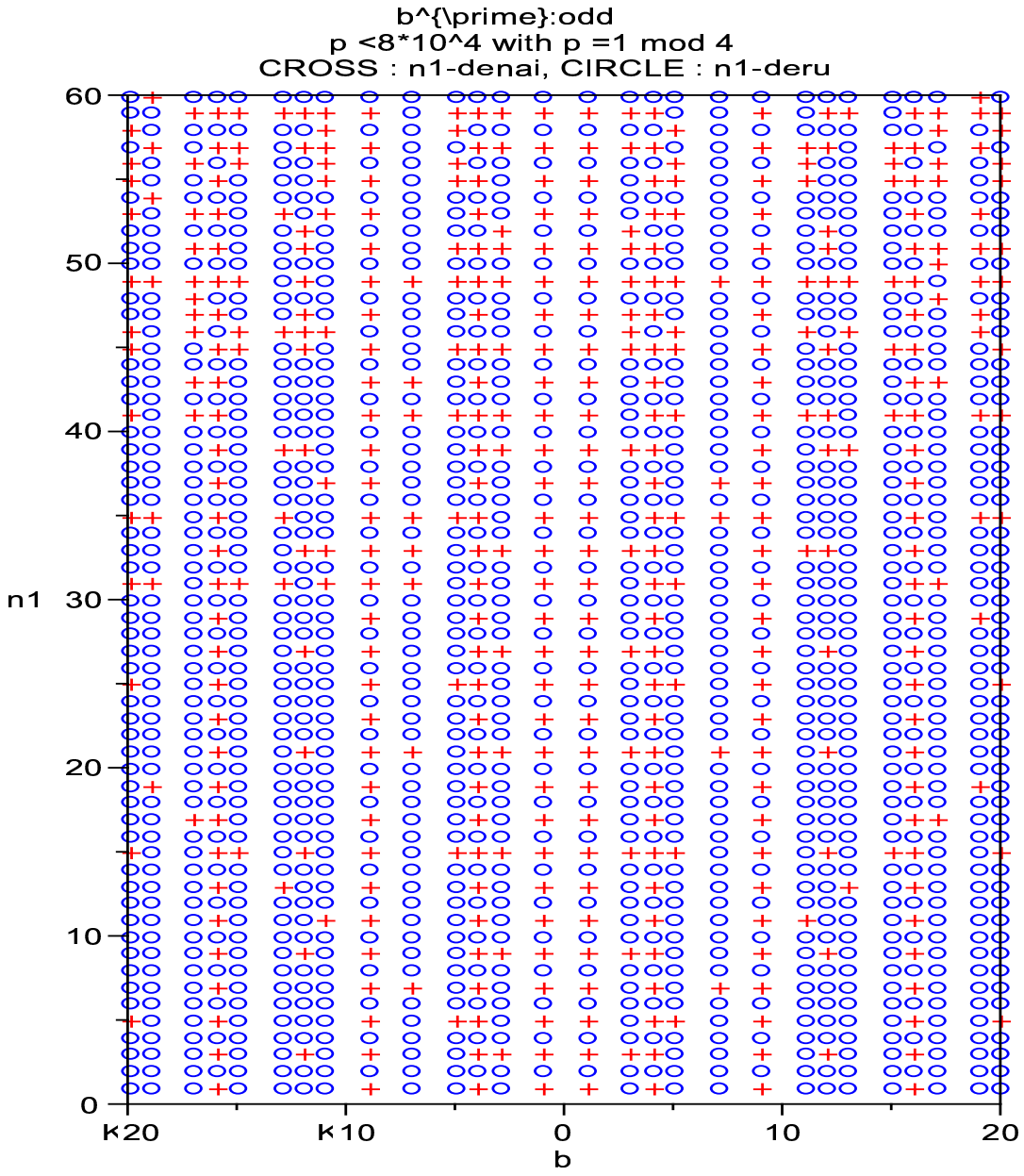

図 4: b_1 が奇数, $p \equiv 1 \pmod 4$ のとき

これらのグラフを調べた結果, 我々は次の予測を得た. (注: (A)(B) は b_1 が奇数の場合, (C) は b_1 が偶数の場合である. また, 素数は $p \equiv 1 \pmod 4$ をみたすもののみ考察の対象としている.)

予測. 記号は上の通りで, $p \equiv 1 \pmod 4$ とする.

(A) (b_1:奇数) $n \equiv b_1 \pmod{2b_1}$ ならば $n_{1,p} = n$ となる p は存在しない.

(B) (b_1:奇数) $n \not\equiv b_1 \pmod{2b_1}$ ならば $n_{1,p} = n$ となる p が存在する.

(C) (b_1:偶数) 任意の n について $n_{1,p} = n$ となる p が存在する.

上に与えたグラフを眺めると, グラフの下のほう (つまり, n の値が小さいところ) ではこの予測が当てはまっていることが確かめられる. グラフの上のほうでは予測にあわない箇所がある ($\circ$ になるべきところが $+$ になっている) が, それは計算した p の範囲が限定されてしまっているせいだと解釈できる. そのような「データ不足」の範囲を除いて考えると, 上の (A)(B)(C) の 3 つの法則でグラフの様子がすべて説明できることが確かめられる.

最後に, 予測が正しいかどうかについて, わかっていることを述べたい. まず, 現在我々が証明できていることは

予測 (A) は正しい

ということだけである. 楕円曲線の等分点に関する基本的事実を使えば, (A) の証明は困難ではないが, ここでは述べるのを省略させていただく.

予測 (B)(C) については, 更に強い主張が成り立つ可能性が高い. つまり, (B)(C) の状況で $C_E(n) > 0$ が証明できるのではないかと思われる ($C_E(n) > 0$ ならば $n_{1,p} = n$ となる p が無限個存在する). そして, 1990 年の論文で R.Gupta が $E : y^2 = x^3 + bx$ について $[\mathbf{Q}(E[k]) : \mathbf{Q}]$ を計算しているので, その結果を使えば $C_E(n) > 0$ が証明できると思えた. しかし, その論文の公式には一部誤りがあることが判明した. 講演で公式の修正を試みていることをお話したが, 残念ながら, いまだ成功していない. したがって, 大変申し訳ないことではあるが, 中途半端な形でこの報告を終わらせていただくほかはない.

参考文献

[1] I. Borosh, C.J. Moreno, H. Porta, *Elliptic curves over finite fields. II*, Math. Computation 29 (1975), 951–964.

[2] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number Theory, CRM Proc. Lec. Notes 36 (2004), 61–79.

[3] R. Gupta, *Division fields of* $Y^2 = X^3 - aX$, J. Number Theory 34 (1990), 335–345.

[4] M.R. Murty, *On Artin's conjecture*, J. Number Theory 16 (1983), 147–168.

[5] J-P. Serre, *Résumé des cours de 1977–1978*, Ann. Collège de France (1978), 67–70.

[6] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, IHES Publ. Math. 54 (1981), 123–201.

[7] R. Takeuchi, *On the distribution of the group of rational points of reductions of an elliptic curve*, Mathematical software (Beijing, 2002), World Sci. Publ., 271–280.

[8] 萩原 賢紀, 楕円曲線の $\mathbf{F}_p$ 有理点の群構造の分布, 学習院大学大学院自然科学研究科 (数学専攻) 2007 年度修士論文.