暗号理論概説
＜第 3 回＞楕円曲線を用いた素因数分解

上野正樹

昨年度の紀要（第 15 号）では，現在主流な公開鍵暗号の 1 つである RSA 暗号の理論と運用，そして実装方法を考察し，公開鍵暗号特有の攻撃手法について紹介した．RSA 暗号の安全性は素因数分解の困難性によって保障されている．第 3 回では，その素因数分解法として有力な楕円曲線法について述べてみたい．この楕円曲線法は現代数学のエッセンスが多く含まれている，なかなか壮大かつ非常に美しい結果なのだが，この理解のために，その前身であるポラードの $p-1$ 法の記述をかなり細かく行った．楕円曲線法の 1 つの例のように感じてもらえるとありがたい．

1　素数と素因数分解アルゴリズム

素数というのは古今東西，多くの数学者や科学者にとって関心事となっている．これはいわゆるプロの数学者のような人たちだけでなく，アマチュアの方々にとっても魅力的なようだ．素数で検索をかけると，実にいろいろなウェブサイトが候補にあがる．

素数が無限に存在すると知っている人にとっては，素朴な興味として，現在見つかっている素数の中で最も大きい数はなにか？と思うだろう．このような問に答えてくれるものとしては，ウェブサイト『The Prime Pages』が詳しい[*1]．それによると 2018 年 7 月末日において，もっとも大きな素数は

$$2^{77232917}-1$$

であり，2300 万桁を超える巨大な素数となっている[*2]．このようなあまりに巨大な自然数に対して，現実的な時間内で素因数分解を行えるようなアルゴリズム，プログラムは存在していない（存在してしまったときは，RSA 暗号が使用できなくなる）．昨年度の紀要でも述べたように，p, q を素数として $n = p \times q$ の形をしているような合成数 n（RSA 型の合成数と呼ぶことにする）の素因数分解の記録は 768bit，232 桁である．先ほどの巨大素数と比較すると小さく感じるかもしれないが，232 桁というのは，宇宙に存在する原子の数よりも大きい（10^{150} 程度と推測されているようだ）．昨年度の紀要では，素因数分解の方法として，素朴な試し割を紹介したが，巨大な数に対して試し割はかなり厳しい．コン

[*1] http://primes.utm.edu/

[*2] 見つかっている最大の素数がこの数ということであって，この数までのすべての素数が発見されたわけではない．

ピュータの性能にもよるが，30bit（2^{30}）を超えると，試し割で因数を発見することはかなり困難になる．今現在，主流な素因数分解アルゴリズムは数体ふるい法と今回紹介する楕円曲線法で，RSA 型の合成数に対しては数体ふるい法が最も計算が速くできるアルゴリズムである．しかしながら，数体ふるい法というのは，かなり大きなプログラムであり，RSA 型ではないかもしれない合成数に対して遅い可能性も高い．そこで一般的には『まず楕円曲線法で素因数分解を試みて，うまくいかなかった場合に数体ふるい法』というアプローチが有効になる．その意味で，楕円曲線法による素因数分解は充分な意味があることを最初に述べておきたい．

2　楕円曲線の定義と楕円曲線における加法公式

2.1　楕円曲線とその有理点

楕円曲線というのは，『楕円曲線暗号』と呼ばれる暗号にもあるように，様々な数学シーンで利用されている．この紀要では，本当に必要最小限な楕円曲線の理解に留めるが，傍から見ると非常に奇妙なルールに見えるだろう．そしてその奇妙なルールが素因数分解に利用されるというのが，またまた不思議だ．自分自身の力不足なのだろうが，数学は自然科学ではあるものの，数学から得られる結果は不自然なことも多く感じる．

＜楕円曲線の定義（**mod** p 上）＞
p を素数とする．$a \pmod p$, $b \pmod p$ に対して，

$$E : y^2 \equiv x^3 + ax + b \pmod{\mathrm{p}}$$

と表され，$4a^3 + 27b^2 \not\equiv 0 \pmod p$ を満たすとき，E を p 上の楕円曲線（elliptic curve）という．

この楕円曲線の概形は次のセクションで示すことにしたい．また今後，
$y^2 \equiv x^3 + ax + b \pmod p$ などは $y^2 = x^3 + ax + b \pmod p$ と書き，$4a^3 + 27b^2 \not\equiv 0 \pmod{\mathrm{p}}$ も $4a^3 + 27b^2 \neq 0 \pmod p$ と書くことにする．このような楕円曲線上にあるような，整数座標 (x, y) はどのくらいあるだろうか？次の例をみてもらいたい．

例 1　$p = 7$ として，楕円曲線 $y^2 = x^3 + 3x + 4$ を考える．$a = 3, b = 4$ なので $4a^3 + 27b^2 = 108 + 432 = 540 \equiv 1 \neq 0 \pmod 7$ なので，楕円曲線である．この整数座標を調べてみると，

（1）$x = 0$ とすると，$y^2 = 4$ なので $y = 2$ と $y = -2 \equiv 5 \pmod 7$ なので，(0,2), (0,5) と 2 つ
（2）$x = 1$ とすると，$y^2 = 1$ なので $y = 1$ と $y = -1 \equiv 6 \pmod 7$ なので，(1,1), (1,6) と 2 つ
（3）$x = 2$ とすると，$y^2 = 18 \equiv 4$ なので，$y = 2$ と $y = -2 \equiv 5$ なので，(2,2), (2,5)
（4）$x = 3$ とすると，$y^2 = 40 \equiv 5$ なので，これを満たす整数 y は**存在しない**．$x = 4$ も同様である．
（5）$x = 5$ とすると，$y^2 = 144 \equiv 4$ なので，$y = 2$ と $y = -2 \equiv 5$ なので，(5,2), (5,5)

（6）$x=6$ とすると，$y^2=238\equiv 0$ なので，$y=0$ のみ．よって (6,0) の 1 点だけある．
以上から，$p=7$ における $y^2=x^3+3x+4$ の整数点は
(0,2), (0,5), (1,1), (1,6), (2,2), (2,5), (5,2), (5,5), (6,0) の 9 点ある． □

上の例 1 において，mod 7 で考えているので，$x=8$ 以上を代入する必要はない．また，以上のような整数点に加えて，仮想的な点 $\mathcal{O}$ を加えたものを，$E: y^2=x^3+3x+4$ の**有理点**と呼ぶ[*3]．この $\mathcal{O}$ は後述する楕円曲線上の加法における 0 のような役割を果たす．

2.2　楕円曲線上の有理点における加法

数学 B において，座標平面上のベクトルに対し，(1,2) + (−3,5) = (1 − 3, 2 + 5) のような足し算を考えたが，このような単純な定義では楕円曲線上の加法を考えることはできない．例 1 においても，(1,1) + (2,2) = (3,3) としたいが，(3,3) という点は先ほどの楕円曲線では存在していないからだ．これをきちんと楕円曲線の有理点の中で収めることができる加法（足し算）の方法として，次のような方法が考えられる．

＜楕円曲線の代数的加法公式（有理点のなす群構造）＞
p を素数，$P_1=(x_1,y_1), P_2=(x_2,y_2)$ とし，この 2 点が楕円曲線 $y^2=x^3+ax+b \pmod p$ 上の有理点とする．
（1）$-\mathcal{O}=\mathcal{O}$ と定める．
（2）$-P_1=(x_1,-y_1)$ と定める．
（3）$P_1+\mathcal{O}=P_1$，$\mathcal{O}+P_2=P_2$ と定める．
（4）P_1，$P_2\neq\mathcal{O}$ とし，$P_2=-P_1$ のときは，$P_1+P_2=P_1-P_1=\mathcal{O}$ と定める．
（5）P_1，$P_2\neq\mathcal{O}$ とし，$P_2\neq -P_1$ であるならば，

$$x_3=m^2-x_1-x_2,\ y_3=m(x_1-x_3)-y_1$$

に対して，$P_1+P_2=(x_3,y_3)$ と定める．ただし上の m は 2 点 P_1, P_2 を通る直線の傾きかまたは接線の傾きである．すなわち，

$$m=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & (x_1\neq x_2)\\[2ex] \dfrac{3x_1^2+a}{2y_1} & (x_1=x_2)\end{cases}$$

である．

注意 上の定義において，傾き m の中に分数が残っているが，これはもちろん mod p の中で考えているので，整数（自然数）に変換する必要がある．すなわち例えば

$$\frac{1}{x_1-x_2}\equiv s \pmod p$$

[*3] 正確に書くと，E の $\mathbb{F}_7$ 上の有理点．

となるような s が必要だが，これは見かけは分数だが，$1 \equiv s(x_1 - x_2) \pmod{p}$ という意味で考えている，仮の分数表記だということは注意しておきたい．これは前回の紀要で示した通り，

$$s(x_1 - x_2) - pk = 1$$

という 1 次不定方程式の解 s, k を探すことに他ならないが，拡張ユークリッドの互除法によって（この場合は）解が求まることになる．あとの例 2 の計算を参照にしてもらいたい．

上の方法で，きちんと $P_3 = (x_3, y_3)$ が楕円曲線上の点になっているか？を証明することは代入してもわかることだが，この一見滅茶苦茶な加法の定義，計算方法には当然意味がある．その幾何的な意味を説明することと，上の定義が一致することを示せば自然と P_3 が楕円曲線上の点になっていることも確かめられるので，そこで証明することにする[*4]．

＜楕円曲線の幾何的加法公式＞

P_1, P_2 を楕円曲線 $y_2 = x_3 + ax + b \pmod{p}$ 上の有理点とする．ただし $\mathcal{O}$ ではないとする．このとき，$P_1 + P_2 = P_3$ を次のように定める．

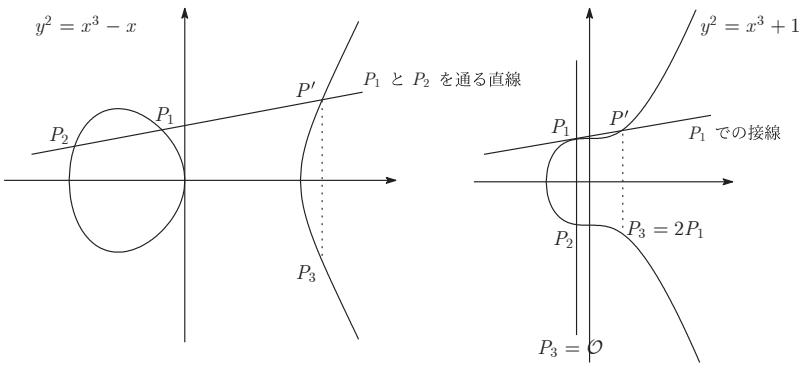
(1) P_1 と P_2 が x 軸対称な点ならば，$P_3 = \mathcal{O}$ とする．x 軸対称でないときは，以下の(2)～(4)のように定める．

(2) 2 点 P_1, P_2 を通る直線 ℓ を引く．ただし $P_1 = P_2$ のときは P_1 を通る接線 ℓ を引く．

(3) その ℓ と楕円曲線 $y_2 = x_3 + ax + b$ との交点（P_1 と P_2 とは異なる点）を P' とする．

(4) P' と x 軸対称な点を P_3 とする．

上の定義（加法公式）における P' が先ほどの代数的な加法公式の $-P_3$ に対応している．図でこの加法公式を表すと，以下のようになる．楕円曲線の概形とともに確認してみたい．



上図のように，楕円曲線は $y^2 = \cdots$ の形なので，x 軸対称である．ただし，上図は整数点だけでなく，実数点を描写している．ここで，幾何的な加法公式から代数的な加法公式が示されることを説明したい．

[*4] 今回は P_1, P_2 を通る傾きが上の加法公式のようになる導出は省略したい．数学Ⅲの微分等を用いる．

証明. 代数的加法公式における m を用いると，幾何的加法公式の直線 ℓ は $y = mx + n$ のように書ける．この直線と楕円曲線 $y^2 = x^3 + ax + b$ との交点は

$$(mx + n)^2 = x^3 + ax + b$$

を満たす．これを整理すると $x^3 - m^2x^2 + (a - 2mn)x + b - n^2 = 0$ となる．ここで $P_1 = (x_1, y_1)$ は直線 ℓ 上にあることから，$y_1 = mx_1 + n$ を満たしているから $n = y_1 - mx_1$ として良いので，代入すると上式は

$$x^3 - m^2x^2 + (a - 2m(y_1 - mx_1))x + b - (y_1 - mx_1)^2 = 0$$

となる．一方，P_1, P_2, P_3 の x 座標は全て ℓ と楕円曲線の交点になっている（P' と P_3 の x 座標は一致している）ので，$(mx + n)^2 = x^3 + ax + b \Longleftrightarrow (x - x_1)(x - x_2)(x - x_3) = 0$ とも書くことができる．よって

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x + x_1x_2x_3 = 0$$

とも書ける．係数を比較すると $m^2 = x_1 + x_2 + x_3$ なので，$x_3 = m^2 - x_1 - x_2$ であることがわかった．y_3 は x 軸対称させていることを考慮にいれて，

$$y_3 = -(mx_3 + n) = -mx_3 - (y_1 - mx_1) = m(x_1 - x_3) - y_1$$

となり，確かめられたことになる． □

例 2 例 1 と同様にして $p = 7$ のときの $y^2 = x^3 + 3x + 4$ を考える．例 1 から (1,1), (5,2) は有理点であった．そこで (1,1) + (5,2) を計算してみる．まず傾き m は $x_1 \neq x_2$ であるから $m = \dfrac{1-2}{1-5} = -(-4)^{-1} \equiv -1 \cdot 3^{-1} \pmod 7$ となる．ここで加法での 注意 のように 3^{-1} は mod 7 における乗法の逆元計算であることから $m = -1 \cdot 3^{-1} = -1 \cdot 5 \equiv 2$ である．3^{-1} が $3 \cdot 5 = 15 \equiv 1 \pmod 7$ であることから 5 であることは $p = 7$ くらいであれば全ての元に対して掛け算してみても良いし，前回の紀要で触れた拡張ユークリッドの互除法を用いてもよい（前回の $ed \equiv 1 \pmod p$ の計算と同じ）．ともあれ，$m = 2$ とわかった．よって

$$\begin{cases} x_3 = m^2 - x_1 - x_2 = 2^2 - 1 - 5 = -2 = 5 \pmod 7 \\ y_3 = m(x_1 - x_3) - y_1 = 2(1-5) - 1 = -9 = 5 \pmod 7 \end{cases}$$

より，(1,1) + (5,2) = (5,5) となることがわかった．

次に得られた (5,5) の 2 倍点 $P_3 + P_3 = 2P_3$ を計算してみる[*5] と，今度は傾き M の計算が $M = \dfrac{3 \cdot 5^2 + a}{2 \cdot 5} = \dfrac{3 \cdot 5^2 + 3}{10} = 10^{-1}$ となる．$10^{-1} = 3^{-1}$ となるから，上から $M = 3^{-1} = 5$ となる．よって $x = M^2 - x_3 - x_3 = 1 \pmod 7$, $y = M(x_3 - x) - x_3 = 1 \pmod 7$ となるから, (5,5) + (5,5) = (1,1) である． □

[*5] のちにこれは $2P_3 = [2]P_3$ のように記述される．

3　種々の素因数分解アルゴリズム

ここまでで理論的なところでは楕円曲線を用いた素因数分解を説明することはできる．しかし公開鍵暗号の前夜にデフィー・ヘルマンの鍵交換があったように，楕円曲線を用いた素因数分解の方法もいきなりこのアイデアができたわけではない．ここでは前回の方法も踏まえて，素因数分解の方法をいくつか紹介してみたい．その中の 1 つであるポラードの $p-1$ 法というものが，楕円曲線法前夜のアルゴリズムになる．

3.1　試し割

まずは一番素朴な方法から．前回の紀要においては，与えられた自然数が素数か否か？を判定するための方法として紹介？したが，この方法はもちろん素因数分解にそのまま流用できる．

＜アルゴリズム 1．原始的な試し割＞

0．与えられた数 **A** の素因数分解をしたい．つまり，因数が知りたい．
1．**2** から **A−1** までの数で割ってみて，割り切れたらその因数で割り算する．
2．**1** で与えられた因数ではない方の数に対して，**1** の操作を繰り返す．
3．これ以上割り算することができなくなったら操作を終了して，素因数分解が完成する．
4．一度も因数が見つからないときは，与えられた数は素数ということになる．

このような方法なのだが，上のアルゴリズムにおける，2 ～ 4 の操作は当たり前なことなので，今後このセクションでは省略する．

上の試し割は説明が不要なくらい誰にでもその方法を伝えることができるので，汎用性は高そうだが，前回にも述べたように，あまりにも因数が与えられるまでに時間がかかる（もちろん上のアルゴリズムには多少改善の余地があるのだが）．これは人間の手計算で時間がかかるのは当然としても，コンピュータを用いても時間がかかることも前回述べた．次に紹介する方法も古典的な方法ではあるものの，改良を加えた試し割と比較しても相当速い．

3.2　エラトステネスのふるい

正確に言えば，エラトステネスのふるいも，素因数分解の方法というよりは，素数判定の色が濃いが，試し割とこのエラトステネスのふるいは，ほとんど区別することなく素因数分解の方法に流用できる．小学校や中学校においては，エラトステネスのふるいというと正方形の中に数字を書き込み，斜線を引いていくという方法で教わることが多いかもしれないが，巨大な数に対してその作業を行うのは返って面倒になる．一般的には次のように行うことが多いだろう．

＜アルゴリズム **2**．エラトステネスのふるい＞

0．与えられた **A** の素因数分解を得たい．
1．**2** から **A** までの数を並べておく．
2．まず **2** は素数である．この素数 **2** を用いて，**2** の倍数を消していく．
3．**2** の作業を終えて，残っている数の最小のものである **3** は素数である．
4．今度は素数 **3** の倍数を消していく．
5．**4** の作業を終えて，残っている数の最小のものである **5** は素数である．
6．もし倍数を消す作業の中で **A** が消せたら **A** の約数が得られたことになる．
7．以上の作業を繰り返して，一度も消すことができなければ **A** は素数．

エラトステネスのふるいの場合，自然とそのようになるが，試し割にしてもこの方法にしても，$\sqrt{A}$ まで作業をしたらそこでアルゴリズムを停止して構わない．A の約数のどちらかは必ず $\sqrt{A}$ 以下だからだ．

例 3　5359 の素因数分解を考える．まず 2 から 5359 までの数を並べておく（必ずしも実際に書く必要はないのだが）．

（1）まず 2, 4, 6, 8, …, 5358 を消す．
（2）3 が残っているので，3, 9, 15, …, 5355 を消す．
（3）4 は既に消えていて，5 が残っているので，5, 25, 35, …, 5345 を消す．
（4）6 は既に消えていて，7 が残っているので，7 の倍数を消す．
（5）8, 9, 10 が既に作業 1, 2 で消えているので，残っている 11 の倍数を消す．
（6）12 は既に消えているので 13 の倍数を消す．
（7）14, 15, 16 は既に消えているので，17 の倍数を消す．
（8）18 は既に消えているので，19 の倍数を消す．
（9）20, 21, 22 は既に消えているので，23 の倍数を消す．すると 23 で 5359 は割り切れる．よって $5359 = 23 \times 233$ がわかる（233 は上の作業を繰り返すと素数とわかる）．

□

上の作業は因数が得られたので終了したが，この作業を $\sqrt{5359} < 74$ なので 73 の倍数を消す作業まで行えば，**5359 以下の全ての素数が得られる**ことになる．さて，一見このエラトステネスの作業は手間が多く，時間がかかるように見えるかもしれないが，実装してテストを行うと，明らかに試し割よりも速く結果を得ることができる．その一番大きな理由は，

エラトステネスのふるいは，実際には割り算を行っていない

ことにある．2 の倍数を消す作業をするときには，$2, 2+2=4, 4+2=6$ のように 2 ずつ足していき消してしまえば良い．つまり 2 個飛びで数字を消していけば良い．例えば 11 の倍数を消す作業をするときも，単に 11 個飛びで数字を消していけば良いような単純作業で消えていくのである．試し割の場合，莫大な回数の割り算をしてみないといけないこ

とが時間のかかる要因になっている．コンピュータにおいても，割り算は足し算と比べるとそれなりに計算コストが高いことは留意する必要がある．

なお，上の例の 5359 は 23 と 233 と，2 つの素数の大小に差がある．試し割にしてもエラトステネスのふるいにしても，$\sqrt{A}$ に近い因数 2 つで構成されているときが，もっとも効率が悪い例になる（素数そのものである場合はもっと効率が悪いが）．つまりここまでの 2 種類の素因数分解法は，実際の数の大小と計算コストには大きな相関関係がないことを意味している．例えば $1147 = 31 \times 37$ のほうが作業としてはあとに約数が見つかることになり，5359 の素因数分解よりも時間がかかる．楕円曲線法もこのように，実際にもっている因数の大小によって計算コストが変わる方法になっているが，数体ふるい法は最初に与えられている数の大小によって計算コストが決まるアルゴリズムになっている点で大きく異なっている．

3.3 ポラードの $p-1$ 法

試し割，エラトステネスのふるいの 2 種類をここまで紹介したが，どちらにしても，小さい数（実際には小さい素数で良いが）から割ったり消したりしていくということ自体には大きな違いはないし，実際素因数分解なのだから，それ以外の方法は無いであろうというのが大方の考えだろう．しかし，計算機の発達に合わせて驚くべき計算法による素因数分解法が考えられた．それがこの $p-1$ 法である．まずは具体的な計算例を紹介してみたい．

例 4　$A = 540143$ の素因数分解を考える．

（1）$B = 8$ としてみる．この最初の設定は重要ではあるが，通常好き勝手な数字を選ぶ．B が大きくなるほど成功率はあがるが，大きすぎてもいけない（後述する）．

（2）B 以下の数，すなわち 1,2,3,4,5,6,7,8 の最小公倍数 ℓ を計算する．$2^3 \times 3 \times 5 \times 7 = 840$ が最小公倍数．

（3）小さな数 a を選ぶ．$a = 2$ とここではしてみる．

（4）a^{ℓ} (mod A) を計算する．すなわち $2^{840} \equiv 53047 \pmod{540143}$

（5）(4)で得られた数に対して，1 を引く．$53047 - 1 = 53046$．この 53046 と $A = 540143$ との最大公約数を，ユークリッドの互除法で計算する．この場合最大公約数は $gcd(53046,540143) = 421$ となり，なんとこれは $A = 540143$ の約数になっている．$540143 = 421 \times 1283$ が得られ，終了する．□

全く不思議だ．一見しただけでは意味がわからないまま，因数が発見できたことになる．この $p-1$ 法の根幹にある理論は何か．それがまたフェルマの小定理になっている．RSA 暗号を作るうえで最も重要な定理（第 14 号）であり，これを用いると弱点があるものの確率的素数判定を行うことができ（第 15 号），手品のような素因数分解法をも支えている．全くもってこの定理は恐ろしい．フェルマ自身の予想も超えて広く利用される．これが本物の『良い定理』だ．

まずはこのアルゴリズムをまとめておく．

＜アルゴリズム 3．$p-1$ 法＞

0. 与えられた整数 n の素因数分解を得たい．
1. 適当な自然数 B を選び，$1, 2, \ldots, B$ の最小公倍数 ℓ を求める．
2. 適当な小さな自然数 a を選び，$a^{\ell} \equiv C \pmod{n}$ を計算する．
3. $C-1$ と n の最大公約数 $G = gcd(C-1, n)$ を計算する．
4. $1 < G < n$ ならば，G が n の因数になる．
5. $G = n$ のときは，B を小さくすれば良い．$G = 1$ のときは，B を大きくしたり a の値を変更して 1 に戻る．

3.3.1 ポラードの $p-1$ 法の理論

まずフェルマの小定理を改めて見直してみよう．p を素数とする．このとき，a が p の倍数でないならば

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．よって，$C' = a^{m(p-1)}$ とするとこのフェルマの小定理から $1 = 1^m \equiv (a^{p-1})^m = a^{m(p-1)} \pmod{p}$ なので，$C' - 1 = a^{m(p-1)} - 1$ は p の倍数であることがわかる．**つまり**

$m(p-1)$ のように $p-1$ の倍数であれば，$C'-1$ は p の倍数

だとフェルマの小定理から主張できる．

一方で素因数分解したい合成数 n が素数 p, q に対して $n = p \times q$ という形だとすると，n は p の倍数になっている．よって **$C'-1$ と n はともに p の倍数なのだから，共通因数として p をもっていることになる．よってユークリッドの互除法において最大公約数を計算すれば p があぶりだせるかもしれない**（下の例 5 の(3)のようにうまくいかないときある）．しかし，実際には $n = p \times q$ の分解は与えられていないので，上記の計算における $a^{m(p-1)} \pmod{p}$ の計算をすることはできない．そこで，$a^{m(p-1)} \pmod{n}$ のように，n で代用してみようというのが，うまいアイデアだ．あらためて $p-1$ 法のアルゴリズムを具体例とともに追っていこう．

例 5 例 4 より $n = 540143 = 421 \times 1283$ であった．

(1) $B = 8$ としたことによって，$\ell = 840$ になっていた．アルゴリズム 1 の手順 1 が完了した．

(2) このとき，$n = 421 \times 1283$ の小さいほうの素数 421 に注目すると $421 - 1 = 420$ である．ℓ はこの 420 の倍数になっている．すなわち，$\ell = 2(p-1)$ となっている．よってフェルマの小定理から，

$$a^{\ell} \equiv 1 \pmod{p}$$

を満たすはずだ．よって $C - 1 \equiv a^{\ell} - 1$ は p の倍数になっている．

(3) よって $C-1$ と n は互いに共通因数 p をもっていることがわかった．さらに $\ell = 840$ はもう一つの素因数 1283 については，$1283 - 1 = 1282$ なので倍数になって

いない．なぜこのようなことを書くのかというと，もし ℓ が 1282 の倍数にもなってしまうと，先ほどと同じ理屈で $C-1$ は $q=1283$ の倍数にもなってしまう．すると $C-1$ は p, q 両方を因数にもってしまい，$gcd(C-1, n)=n$ となってしまい，p, q があぶりだせないことになり失敗する．つまり $n=pq$ のうち，**$p-1$ の倍数にはなっているが，$q-1$ の倍数にはなっていないような ℓ（つまり B）の設定が重要**になる．すなわち

$$a^{\ell} \equiv 1 \pmod{p} \quad \text{だが} \quad a^{\ell} \not\equiv 1 \pmod{q}$$

を満たすようにしたい．この場合 $1283-1=1282=2\times 641$ なので，$B=641$ 以上にすると失敗することになる．もっと言えば，$421-1=420=2^2\times 3\times 5\times 7$ と 7 までの素数でしか構成されていないことが $B=8$ でうまくいく理由になる．この例においては，$8 \leqq B \leqq 640$ までなら $n=421\times 1283$ と $C-1$ がともに 421 を共通因数にもち，1283 は因数に持たないので，

$$gcd(C-1, 540143)=421$$

となり，素因数 421 を得ることができる．

(4) 最後に極端に小さく $B=3$ としたとしよう．すると $\ell=6$ になる．この場合，$a^{\ell}=2^6=64$ なので，$G=gcd(63, n)=1$ となり，因数は得られない．以上のことがアルゴリズム 3 の手順 4，5 の説明になる．

(5) 以上のことは 421,1283 というペアがわからなくても計算には支障がない．単に $p-1$ の倍数になっているが $q-1$ の倍数にはなっていない，などのことが途中では確かめられないだけだ．$p-1$ 法がうまくいかないほとんどのケースは(4)のように $gcd(C-1, n)=1$ となって，B を大きくしていき，$p-1$ の倍数になるように調整していく． □

しかし，次のような厄介な例もある．

例 6 $n=2047=23\times 89$ の素因数分解を考える．この程度の桁数であれば試し割でもあっという間に計算が終了してしまうのだが，$p-1$ 法だとなかなか厄介な存在になる．上の例でも書いたように，この場合の B の設定は $23-1=22$ の倍数にはなるが，$89-1=88$ の倍数にはならないような B にしなくてはならない．しかし 22 は 11 の倍数なので $B=11$ 以上が最低ラインになるが，この時点で必ず $\ell>88$ であるようになってしまい（もちろん 88 の倍数になっている），そのような B の設定は不可能になる．このようなときにはアルゴリズム 3 の手順 5 にあるように，a の値を変更して計算することになるが，この例の場合その a もなかなか発見が難しい（$a=12$ で成功する）． □

3.3.2 $n=540143=421\times 1283$ の再考

上の例に限らず，$p-1$ 法は完璧ではない（そもそも完璧な素因数分解法は見つかっていないが）．しかしそもそも試し割で完了するような数であるならば，試し割やエラトステネスのふるいで計算すれば良いので，基本的には『それなりに』大きな数における素因

数分解を考えるときには，この $p-1$ 法は有効だ．具体的にどんなときに，$p-1$ 法はうまくいくのだろうか？

(1) $n=p\times q$ の p,q を求めたい．

(2) うまく B を設定して，B 以下までの自然数の最小公倍数 ℓ が $p-1$ の倍数にはなるが，$q-1$ の倍数にはならないようにしたい．このことを言葉ではなく数式で判定しないといけないが，それは

$$a^{\ell}\equiv 1 \pmod{p} \quad \text{だが} \quad a^{\ell}\not\equiv 1 \pmod{q}$$

で確かめられる．

(3) 片方の，例えば $p-1$ を素因数分解したときに，**小さな素因数だけで構成されていると $p-1$ 法はかなり高い確率で成功する**．

(4) つまり，540143 はそれなりに大きい数で，2 つの素数 421,1283 もそれなりに大きな素数ではあるが，$421-1=420$ については，$420=2^2\times 3\times 5\times 7$ と小さい素数でのみ構成されるので，$B=8$ で済んでいたことになる．もう片方の $1283-1=1282=2\times 641$ が 641 を含んでいるおかげで，元々の 540143 という数字のサイズに対して，$8\leqq B\leqq 640$ とかなりの候補を選出できるのはありがたい．

(5) よって困るのは，$p-1, q-1$ ともに（元々の数字と比較して）大きな素数をもっているときになる．元々の数が大きくなれば自然と $p-1$ などが大きな素数を因数にもつ確率はあがり，計算コストも上がるので，できるだけ B を小さくし，B の候補がたくさんあると良い．

このような感じになる．しかし $p-1$ 法の場合，最初の n が与えられたら $p-1, q-1$ ともに（当たり前だが）1 通りの値しかない．よって $p-1$ ができるだけ小さな素数でのみ構成されるように，といってもそのようなことを人の手で操作することは不可能だ．それを必ずしも $p-1$ ではなく人の手で調整できるようにした方法が楕円曲線法ということになる．

4　楕円曲線法

$p-1$ 法の場合，ℓ というある決めた B 以下までの値の最小公倍数が，$p-1$ の倍数になっていれば良いことになっていた．さらに $q-1$ の倍数にはならないようにするということももちろんあるのだが，まずは $p-1$ の倍数を作りたい．$p-1$ の倍数を作るためには $p-1$ の素因数が小さい素数で構成されているとなお良いが，それは元々の n が決まっていると，人の手では調整することができない．しかし例えば $p-2$ ならば小さな素因数で構成されていて，$p-2$ の倍数を作ることができるかもしれない．$p-2$ が駄目でも $p-10$ なら？のようにここを変更できないだろうか，としたのが楕円曲線法なのである．

そもそもなぜ $p-1$ の倍数を作りたいのかというと，フェルマの小定理が $a^{p-1}\equiv 1 \pmod{p}$ のように，$p-1$ 乗であったからだ[*6]．したがってフェルマの小定理のような結果が成り

立つものを用意できれば，必ずしも $p-1$ の倍数を作らなくても良いはずだ．そこで前のセクションで用意した，楕円曲線の加法公式を利用しようというアイデアが生まれた．その利用方法を順を追って説明していくために，いくつかのことを確認・準備する．

＜素数上の楕円曲線の有理点＞
(x_1, y_1) が $y^2 \equiv x^3 + ax + b \pmod{p}$ を満たすとき，(x_1, y_1) のことを素数 p 上の $y^2 = x^3 + ax + b$ の有理点と呼ぶ（例 1 参照）．

このことを，整数 n に拡張する．

＜整数 n 上の（擬）楕円曲線の有理点＞
(x_1, y_1) が $y^2 \equiv x^3 + ax + b \pmod{n}$ を満たすとき，(x_1, y_1) のことを整数 n 上の $y^2 = x^3 + ax + b$ の有理点と呼ぶ．

整数 n のときは，本質的には楕円曲線とは呼べないのだが（群構造をもたない），ここではひとまとめに楕円曲線と呼んでしまうことにする．また，この紀要では今後しばらく整数 n は 2 つの異なる素数に対して RSA 型の $n = p \times q$ の形の合成数のみを考えることにしよう．このような $n = pq$ の形の合成数上の楕円曲線 $y^2 = x^3 + ax + b \pmod{n}$ からは自然と素数 p 上の有理点と素数 q 上の有理点が派生する．次の例を見てみたい．

例 7 $n = 77 = 7 \times 11$ 上の楕円曲線 $y^2 = x^3 + 3x + 2 \pmod{77}$ を考えると，$(26, 32)$ は有理点になっている．この点に対して，x, y 座標をそれぞれ $p = 7$ で割ると $26 = 5 \pmod 7$, $32 = 4 \pmod 7$ なので $(5, 4)$ は $y^2 = x^3 + 3x + 2 \pmod 7$ 上の有理点になっている．

実際 $y^2 = 4^2 = 2 \pmod 7$，$x^3 + 3x + 2 = 125 + 15 + 2 = 142 = 2 \pmod 7$ なので $y^2 = x^3 + 3x + 2 \pmod 7$ を満たす．

同時に，$q = 11$ についても同様にして，$26 = 4 \pmod{11}$，$32 = 10 \pmod{11}$ なので $(4, 10)$ という $y^2 = x^3 + 3x + 2 \pmod{11}$ 上の有理点をうむ．このようにすると

$$y^2 = x^3 + 3x + 2 \pmod{77} \text{の有理点} (26, 32) \Longleftrightarrow \begin{cases} y^2 = x^3 + 3x + 2 \pmod 7 \text{ の有理点 } (5, 4) \\ y^2 = x^3 + 3x + 2 \pmod{11} \text{ の有理点 } (4, 10) \end{cases}$$

という対応がつく．右の $(5, 4) \pmod 7$，$(4, 10) \pmod{11}$ という有理点のペアから左の $n = 77$ の有理点 $(26, 32)$ の作り方は，例えば x 座標だけを言葉で考えてみると，

7 で割ると 5 余り，11 で割ると 4 余るような整数を 77 で割った余りはいくつか？ $(\rightarrow 26)$

という問題になるので，26 を求めるのは少しコツ（？）がいるが，それはまさしく前回少し紹介した中国の剰余定理の問題になっている．中国の剰余定理によればこの問題は余りとしては 1 通りしか組み合わせがない．その対応によって，$n = pq$ 上の有理点は p 上の有理点と q 上の有理点をペアで考えることで，同一視することができる．注意が必要なのは，

[6*] 大学数学の言葉でいうと，$(\mathbb{Z}_p)^*$ という群の位数が $p-1$ ということになる．

（1）ペアで考えていること．

（2）（1）はつまり，$(26,32)$ という $y^2=x^3+3x+2 \pmod{77}$ での有理点を $p=7$ 上の有理点として考えるときには $(26,32)=(5,4) \pmod 7$ とそのまま 7 で割った余りにすれば良いが，$(5,4)$ という $y^2=x^3+3x+2 \pmod 7$ での有理点を $n=77$ 上で考えるとき，そのまま $(5,4)$ を 77 で割った余りにはしてはいけない，ということだ（そもそも $n=77$ 上では $(5,4)$ は有理点にならないから，本来おかしな議論なのだが）．$(5,4) \pmod 7$ と相方の $(4,10) \pmod{11}$ という有理点があって初めて $(26,32)$ を得ることができる．しかし今後の楕円曲線法の議論は mod n 上の点から p または q への有理点を考えることがほとんどなので，特別な意味はもたないかもしれない． □

以上から，$n=pq$ に対する $y^2=x^3+ax+b$ の有理点 $(x,y) \pmod n$ に対して

$$\text{有理点 } (x,y) \pmod n \Longleftrightarrow \begin{cases} \text{有理点 } (x,y) \pmod p \\ \text{有理点 } (x,y) \pmod q \end{cases}$$

という対応がついた[*7]（$\mathcal{O} \pmod n$ は $\mathcal{O} \pmod p$, $\mathcal{O} \pmod q$ が対応）．上のように，n 上でも p 上でも q 上でも同じ記号 (x, y) と書き $\pmod n$ をつけて区別したり，$(x^{(n)}, y^{(n)})$ のように書くこともある．この紀要は $\pmod n$ のように，mod をつけて区別することにする．

そして，素数上の楕円曲線では有理点における加法公式が成立していた．

＜素数上の楕円曲線の代数的加法公式（有理点のなす群構造）＞

p を素数，$P_1=(x_1, y_1), P_2=(x_2, y_2)$ とし，この 2 点が楕円曲線 $y^2=x^3+ax+b \pmod p$ 上の有理点とする．

（1）$-\mathcal{O}=\mathcal{O}$ と定める．

（2）$-P_1=(x_1, -y_1)$ と定める．

（3）$P_1+\mathcal{O}=P_1$，$\mathcal{O}+P_2=P_2$ と定める．

（4）P_1，$P_2 \neq \mathcal{O}$ とし，$P_2=-P_1$ のときは，$P_1+P_2=P_1-P_1=\mathcal{O}$ と定める．

（5）P_1，$P_2 \neq \mathcal{O}$ とし，$P_2 \neq -P_1$ であるならば，

$$x_3=m^2-x_1-x_2,\ y_3=m(x_1-x_3)-y_1$$

に対して，$P_1+P_2=(x_3, y_3)$ と定める．ただし上の m は 2 点 P_1, P_2 を通る直線の傾きかまたは接線の傾きである．すなわち，

$$m=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & (x_1 \neq x_2) \\ \dfrac{3x_1^2+a}{2y_1} & (x_1=x_2) \end{cases}$$

[*7] しかし後の記述からわかるように，同型ではない．そもそも mod n では有理点の集合は群になっていない．

4.1 楕円曲線法の原理

ここでは，上の加法公式を用いて，いかにしてポラードの $p-1$ 法のような状態にもっていくのかということについて，記述してみたい．まず次の補題を証明する．実質的にこれが楕円曲線法の主結果となる．

＜**補題 1**＞

p, q を異なる素数とし，$n = pq$ とする．$\mathcal{O}$ ではない 2 点 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ を n 上の（擬）楕円曲線 $y^2 = x^3 + ax + b$ の有理点とする．すなわち，今は先に $n = pq$ における有理点をとっているので，同じ x_1, y_1, x_2, y_2 に対して

$$(*)\begin{cases}(y_1)^2 \equiv (x_1)^3 + ax_1 + b \pmod{p}\\ (y_1)^2 \equiv (x_1)^3 + ax_1 + b \pmod{q}\\ (y_2)^2 \equiv (x_2)^3 + ax_2 + b \pmod{p}\\ (y_2)^2 \equiv (x_2)^3 + ax_2 + b \pmod{q}\end{cases}$$

を満たしている．このとき楕円曲線の加法公式において，

$$\begin{cases}P_1 + P_2 = \mathcal{O} \pmod{p}\\ P_1 + P_2 \neq \mathcal{O} \pmod{q}\end{cases}$$

が成立していれば，

$$\begin{cases}x_1 \neq x_2 \pmod{n} \text{ であり } x_1 - x_2 \text{ は } p \text{ の倍数かつ } q \text{ の倍数ではない}\\ x_1 = x_2 \pmod{n} \text{ であり } 2y_1 \text{ は } p \text{ の倍数かつ } q \text{ の倍数ではない}\end{cases}$$

のいずれかが成立する．

証明．加法公式（定義）から $P_1 + P_2 = \mathcal{O} \pmod{p}$ は $P_2 = -P_1$ と同値なので，$(x_2, y_2) = (x_1, -y_1)$ である．よって $x_1 \equiv x_2 \pmod{p}$ かつ $y_1 \equiv -y_2 \pmod{p}$ が成立する．さらに $P_1 + P_2 \neq \mathcal{O} \pmod{q}$ であるから $x_1 \not\equiv x_2 \pmod{q}$ または $y_1 \not\equiv -y_2 \pmod{q}$ が成立する．よって考えられる組み合わせは次の 2 通りしかない．

（1）$x_1 = x_2 \pmod{p}$ かつ $y_1 = -y_2 \pmod{p}$ かつ $x_1 \neq x_2 \pmod{q}$

（2）$x_1 = x_2 \pmod{p}$ かつ $y_1 = -y_2 \pmod{p}$ かつ $y_1 \neq -y_2 \pmod{q}$

(1)の場合，$x_1 = x_2 \pmod{p}$ かつ $x_1 \neq x_2 \pmod{q}$ より $x_1 - x_2$ は p の倍数だが q の倍数でないことを意味し，さらに $x_1 \neq x_2 \pmod{n}$ である（$x_1 = x_2 \pmod{n}$ だと $x_1 - x_2$ が n の倍数なので，q の倍数となり $x_1 = x_2 \pmod{q}$ となってしまう）．これで補題 1 の一つ目の主張は示された．

(2)のときは同様な理由で，$y_1 + y_2$ が p の倍数だが，q の倍数ではないことになる．このこと自体も面白い結果だが，とりあえず補題 1 の結果である $2y_1$ の性質に話を近づけていくことにする．ここで(2)の条件に $x_1 = x_2 \pmod{q}$ を付け加えても良いはずだ．なぜならば $x_1 \neq x_2 \pmod{q}$ なら，それは(1)の状況と同じなので，補題 1 の結果を満たしているからである．すると今加えた $x_1 = x_2 \pmod{q}$ と補題 1 の仮定 $(*)$ から

$$(y_1)^2 \equiv (x_1)^3 + ax_1 + b \equiv (x_2)^3 + ax_2 + b \equiv (y_2)^2 \pmod{q}$$

を得る．よって $y_1 = y_2 \pmod{q}$ または $y_1 = -y_2 \pmod{q}$ だが（後述するように幾何的には明かな結果だ[*8]），(2)の場合は $y_1 \neq -y_2 \pmod{q}$ であったので, $y_1 = y_2 \pmod{q}$ のみとなる．よって，$y_1 \neq -y_2 \pmod{q} \Longleftrightarrow 2y_1 \neq 0 \pmod{q}$ となり，$2y_1$ は q の倍数ではないことがわかる．よってあとは $2y_1$ が p の倍数であること, $x_1 = x_2 \pmod{n}$ を示せばよい．$x_1 = x_2 \pmod{n}$ であることは，いま $x_1 = x_2 \pmod{p}$ で $x_1 = x_2 \pmod{q}$ なので $x_1 = x_2 \pmod{pq = n}$ であることからわかる．またこの $x_1 = x_2 \pmod{n}$ であることから，楕円曲線は x 軸対称であるから，元々の $P_1 = (x_1, y_1)$ と $P_2 = (x_2, y_2)$ という n 上の楕円曲線 $y^2 = x^3 + ax + b$ における有理点の位置関係は，$y_1 = y_2 \pmod{n}$ かまたは $y_1 = -y_2 \pmod{n}$ のいずれかしかない．しかし後者の $y_1 = -y_2 \pmod{n}$ であることはない．なぜならばこのとき $y_1 + y_2$ は n の倍数になってしまうが，n が q の倍数であることから $y_1 + y_2 = 0 \pmod{q} \Longleftrightarrow y_1 = -y_2 \pmod{q}$ となり(2)の仮定に反するからだ．そこで前者の $y_1 = y_2 \pmod{n}$ を考えると，$y_1 - y_2$ が n の倍数なので p の倍数でもある．よって $y_1 = y_2 \pmod{p}$ より，(2)の条件でもあった $y_1 = -y_2 \pmod{p}$ と合わせて $2y_1 = 0 \pmod{p}$ である．よって $2y_1$ は p の倍数であるが，q の倍数ではないことになり，補題 1 の結果を得る．□

以上から，補題 1 の状況，すなわち $n = pq, P_1 + P_2 = \mathcal{O} \pmod{p}, P_1 + P_2 \neq \mathcal{O} \pmod{q}$ であれば,

$$gcd(n, x_1 - x_2) = \mathrm{p} \quad \text{または} \quad gcd(n, 2y_1) = p$$

と n の素因数が得られることになった．よって次の問題は，どうやって $n = pq$ という素因数分解を知らない状態で，$P_1 + P_2 = \mathcal{O} \pmod{p}, P_1 + P_2 \neq \mathcal{O} \pmod{q}$ という状況を作り，確認するのかということになる．

まず $P_1 + P_2 = \mathcal{O} \pmod{p}, P_1 + P_2 \neq \mathcal{O} \pmod{q}$ という状況を作ることを考えてみる．補題 1 は強力だが，都合よく適当に作成した 2 点 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ でそのような状況を作ることは難しい（それは実質，適当な数でもって n を割ってみて素因数を探すことと同じことだ）．楕円曲線上の加法の式を見てもわかるように，通常の和を計算すると $P_1 + P_2 \neq \mathcal{O}$ になる．そこで，ひとまずは $P_1 + P_2 = \mathcal{O} \pmod{p}$ を作りたいがそんなことは可能だろうか？次のことが言える．

＜**補題 2**＞
p を素数とし，$P \neq \mathcal{O}$ を p 上の楕円曲線 $y^2 = x^3 + ax + b$ の有理点とする．このとき，

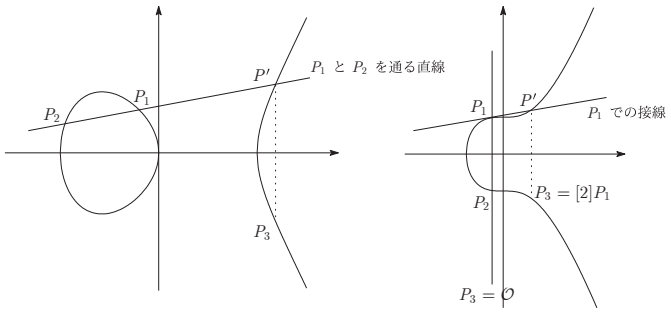
$$\underbrace{P + P + \cdots + P}_{k\text{個}} = [k]P = \mathcal{O} \pmod{p}$$

となる自然数 k が存在する．

[*8] 素数上の楕円曲線であれば，代数的にも容易な結果だ.

上のように，k 個の有理点 P の和を $[k]P$ と表すことにする．補題 2 自体の結果は，大学数学の群論の立場に立てば，一般論として処理できるが，この場合は群論に頼らなくてもわかる；

証明. 楕円曲線 $y^2 = x^3 + ax + b$ の有理点は有限個であり，加法公式から，



のように，$P_1 \neq \mathcal{O}, P_2 \neq \mathcal{O}$ であれば $P_1 + P_2 \neq P_1, P_1 + P_2 \neq P_2$ である[*9]．逆に言えば，$P + P_3 = P$ となるような P_3 があれば，それは $P_3 = \mathcal{O}$ ということになる．しかし有理点は有限個しかないので，$P + P + \cdots$ とすると，いつかは P になるはずなのでそれを $k + 1$ 個，つまり $[k + 1]P = P$ だったと仮定すると

$$[k+1]P = P \Longleftrightarrow P + (\underbrace{P + \cdots + P}_{k\text{個}}) = P$$

となるので，$[k]P = \mathcal{O}$ となる． □

さらに次のことを証明してみよう．

＜補題 3＞
p を素数とし，p 上の楕円曲線 $y^2 = x^3 + ax + b$ の有理点を s 個とする．その s 個の有理点の集合を

$$E = \{P_1, P_2, \ldots, P_s\}$$

とするとき，$P_1, \ldots, P_s$ の中の任意の有理点 P に対して $[s]P = \mathcal{O} \pmod{p}$ が成立する．

証明. もし P_i, P_j が異なる E の有理点とすると，

$$P + P_i \neq P + P_j$$

である．なぜならば，もし $P + P_i = P + P_j$ とすると，$P_i = P_j$ となってしまうからだ．よって，

$$E' = \{P + P_1, P + P_2, \ldots, P + P_s\}$$

は集合 E の元を並び替えただけ集合ということになる．よって E の元の総和と E' の元の総和は一致するので

[*9] 群論でいえば，単位元の一意性ということになる．

$$\begin{aligned} P_1+P_2+\cdots+P_s &= (P+P_1)+(P+P_2)+\cdots+(P+P_s) \\ &= [s]P+(P_1+P_2+\cdots+P_s) \end{aligned}$$

を得る．よって $[s]P=\mathcal{O}$ である． □

補題 2 と補題 3 は，ラグランジュの定理という定理によって広く一般化され，k は s の約数であるという，より強い結果もあることを言及しておく．

＜**補題 4**＞
m を任意の自然数，p を素数とし，p 上の楕円曲線 $y^2=x^3+ax+b$ の有理点を s 個とする．P を任意の $y^2=x^3+ax+b$ の有理点とすると，

$$[ms]P=\mathcal{O}$$

が成立する．

証明. 補題 3 の結果から

$$[ms]P=\underbrace{[s]P+[s]P+\cdots+[s]P}_{m\text{ 個}}=\mathcal{O}$$

である． □

補題 1 と補題 4 を組み合わせると，

$$[ms]P=\mathcal{O}\Longleftrightarrow P+[ms-1]P=\mathcal{O}\ (\mathrm{mod}\ p)$$

と書くことができることから，補題 1 の $P_1+P_2=\mathcal{O}\ (\mathrm{mod}\ p)$ という状況を作れそうだ．よって n の素因数 p をあぶりだすことができそうである．$p-1$ 法の場合は

$$a^{m(p-1)}-1\equiv 0\ (\mathrm{mod}\ p)$$

であることなどから，$p-1$ の倍数を作ることが目標であると説明した．きちんとしたアルゴリズムは後述するにしても，楕円曲線法の場合は，p 上の楕円曲線 $y^2=x^3+ax+b$ の有理点の個数 s の倍数を作れば

$$[ms]P=\mathcal{O}\ (\mathrm{mod}\ p)$$

となり，素因数を得ることができそうだ．そして，その s 個という有理点の個数は当然 $y^2=x^3+ax+b$ の a, b の値を変更すれば，それを満たす有理点の個数も変化するはずだ．よって見つけたい素因数 p の値は変更できなくても，有理点の個数が変更がきくので，s の倍数を作りやすいような s が見つかるかもしれない（s を構成する素数が小さい素数が多いと，この可能性は高くなる）！　このことが $p-1$ 法よりも高い確率で n の素因数 p を発見することを可能にしている．

よって最後の問題は，$n=pq$ という p, q の組み合わせを知らずに，先ほどのような

$[ms]P = P + [ms-1]P = P_1 + P_2 = \mathcal{O} \pmod p$ となっているかを確認することだ．$p-1$ 法の場合は，単に $a^\ell \pmod n$ のように単純に mod n として計算すればよかった．楕円曲線法の場合には以下のようにする．これが最後の準備となる．再び補題 1 の状況に戻ってみよう．

＜**補題 5**＞

p, q を異なる素数とし，$n = pq$ とする．$\mathcal{O}$ ではない点 $P = (x_1, y_1)$ を n 上の（擬）楕円曲線 $y^2 = x^3 + ax + b$ の有理点とする．このとき，素数上の楕円曲線の加法を n でも同じように計算してみる．すなわち

＜**合成数 n 上の（擬）楕円曲線の加法**＞

$P_1 = (x_1, y_2), P_2 = (x_2, y_2)$ とし，この 2 点が楕円曲線 $y^2 = x^3 + ax + b \pmod n$ 上の有理点とする．

（1）$-\mathcal{O} = \mathcal{O}$ と定める．

（2）$-P_1 = (x_1, -y_1)$ と定める．

（3）$P_1 + \mathcal{O} = P_1$，$\mathcal{O} + P_2 = P_2$ と定める．

（4）P_1，$P_2 \neq \mathcal{O}$ とし，$P_2 = -P_1$ のときは，$P_1 + P_2 = P_1 - P_1 = \mathcal{O}$ と定める．

（5）P_1，$P_2 \neq \mathcal{O}$ とし，$P_2 \neq -P_1$ であるならば，

$$x_3 = m^2 - x_1 - x_2 \pmod n, \quad y_3 = m(x_1 - x_3) - y_1 \pmod n$$

に対して，$P_1 + P_2 = (x_3, y_3) \pmod n$ と定める．ただし上の m は 2 点 P_1, P_2 を通る直線の傾きかまたは接線の傾きである．すなわち，

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \pmod n & (x_1 \not\equiv x_2 \pmod n) \\ \dfrac{3x_1^2 + a}{2y_1} \pmod n & (x_1 = x_2 \pmod n) \end{cases}$$

である．

を，行う．この加法において，$[k]P$ を計算していき，

$$[k]P = \mathcal{O} \pmod p \quad \text{または} \quad [k]P = \mathcal{O} \pmod q$$

のどちらか片方のみが成立しているとき，加法は計算不能になってしまう（計算が止まる）．

証明．ここまでの準備があれば，結果はほぼ明らかであろう．上の合成数 n における加法は傾き m を求めるとき，mod n において $x_2 - x_1$ または $2y_1$ という分母に残ってしまったときは m の計算ができない（話は整数で行われている）．逆に他は mod n でも計算可能なことにも注目すると，mod n において加法が計算できなくなるのはその傾きにおける分母の処理のみだ．いま，仮定から $[k]P = \mathcal{O} \pmod p$ または $[k]P = \mathcal{O} \pmod q$ の一方のみが成立しているので，ここでは $[k]P = \mathcal{O} \pmod p$, $[k]P \neq \mathcal{O} \pmod q$ としてみる．$[k]P = \mathcal{O} \pmod p$ $\iff P + [k-1]P = \mathcal{O} \pmod p$ かつ $[k]P \neq \mathcal{O} \pmod q \iff P + [k-1]P \neq \mathcal{O} \pmod q$ とみることで，$[k-1]P = (x_2, y_2)$ とすると補題 1 から

$$\begin{cases} x_1 - x_2 \text{ は } p \text{ の倍数かつ } q \text{ の倍数ではない } (x_1 \neq x_2 \pmod n) \\ 2y_1 \text{ は } p \text{ の倍数かつ } q \text{ の倍数ではない } (x_1 = x_2 \pmod n) \end{cases}$$

を得る．よって傾き m の計算において，$x_1 \neq x_2 \pmod n$ のときを考えると，m の分数は分子を見なければ $\dfrac{1}{x_2 - x_1}$ であるが，上のことから分母にあたる $x_1 - x_2$ は p の倍数だが q の倍数ではないことになる．このとき

$$\frac{1}{x_2 - x_1} \equiv s \pmod n \Longleftrightarrow 1 \equiv s\,(x_2 - x_1) \pmod n$$

を満たす整数 s は存在しない．もし存在すれば $s(x_2 - x_1) - 1$ が n の倍数になるので $s(x_2 - x_1) - nt = 1$ を満たすような整数 t が存在することになる．しかし $x_1 - x_2$, n が p の倍数であるから $s(x_2 - x_1) - nt$ は p の倍数になるので，1 になることはないので矛盾する．$x_1 = x_2 \pmod n$ のときの議論も同様である．よって n における加法が計算できなくなり，計算不能，計算が止まることになる． □

証明は以上になるが，上の『計算が止まる，不能になる』というところをもう少し見ておくことにしたい．ここは少し大学数学の知識を要する．例 7 で見たように，n 上の有理点 $(x, y) \pmod n$ からは p 上の有理点 $(x, y) \pmod p$ と q 上の有理点 $(x, y) \pmod q$ が対応している．p, q から n の点と見るには，ペアとして見て，中国の剰余定理によって求められていた．特に $\mathcal{O} \pmod n$ は $\mathcal{O} \pmod p$ かつ $\mathcal{O} \pmod q$ と対応していた．すると例えば $P + [k-1]P = [k]P \pmod n$ を計算していく過程で p, q 上の有理点で起きていることは次の 3 通りになる．

（1）$P + [k-1]P = (x_1, y_1) \pmod p \neq \mathcal{O}$ かつ $P + [k-1]P = (x_2, y_2) \pmod q \neq \mathcal{O}$ から中国の剰余定理によって $[k]P = (x, y) \pmod n$ の点が復元できる．

（2）$P + [k-1]P = \mathcal{O} \pmod p$ かつ $P + [k-1]P = \mathcal{O} \pmod q$ から $[k]P = \mathcal{O} \pmod n$ が復元できる．

（3）$P + [k-1]P \pmod p$ または $P + [k-1]P \pmod q$ のどちらかが $\mathcal{O}$ となって，$[k]P \pmod n$ が復元できない．

つまり n における有理点が座標ならば，ペアとして p 上の有理点と q 上の有理点の 2 つの座標が必要になるし，n における $\mathcal{O}$ が対応するためにはペアとして p, q 上ともに $\mathcal{O}$ が必要となる．片方のみが $\mathcal{O}$ になってしまっているときには，そのような n 上の有理点は定義できない．が，p 上または q 上の点としては代数計算できてしまうことになる．ここで矛盾がおきて，補題 5 のようなことが発生していることになる．楕円曲線上の有理点の集合を $E(p), E(q), E(n)$ とすれば

$$E(n) \ncong E(p) \times E(q)$$

である．$\mathcal{O}$ を除いてしまえば，それは中国の剰余定理と同じ状況なので，同型になる．なので集合としての元の個数は

$$|E(n)| - 1 = (|E(p)| - 1) \times (|E(q)| - 1)$$

となっている． □

以上から，楕円曲線法による素因数分解のアルゴリズムが完成する．

定理＜アルゴリズム 4．楕円曲線法＞

---

0. 与えられた整数 $n = pq$ の素因数分解を得たい．
1. 適当な自然数 B を選び，$1, 2, \ldots, B$ の最小公倍数 k を求める．
2. 適当に（通常は乱数を用いる）整数 a, x, y を選び，$b = y^2 - x^3 - ax \pmod n$ とする．こうすることで（擬）楕円曲線 $y^2 = x^3 + ax + b \pmod n$ とその有理点 $P = (x, y)$ ができる．
3. 念のため，$4a^3 + 27b^2$ と n の最大公約数 $G = gcd(4a^3 + 27b^2, n)$ を計算する．基本的には意味はない．
4. $[k]P$ を計算する．その過程で計算が止まってしまったときは，補題 1 および 5 から n の因数 p または q を得る．
5. 上で計算が止まらなかった場合は，まず 2 に戻って計算をやり直す．それでも駄目なときは 1 の B を大きくする．

証明. 上のアルゴリズムを少し補足する．

（1）1 については $p - 1$ 法と同じ考え方である．

（2）2 については，先に a, b を決めて，楕円曲線 $y^2 = x^3 + ax + b$ から定義すると，有理点 (x, y) の計算が面倒になってしまう．そこで，最後に b を決めてしまえば，自動的に楕円曲線と有理点が定まることになるというアイデアだ．

（3）3 については楕円曲線は $4a^3 + 27b^2 \neq 0 \pmod n$ が要求されていたので，2 で決めた a, b がその条件を満たしているのかを確認している．もし $4a^3 + 27b^2 = 0 \pmod n$ になってしまっているときは，楕円曲線を定義しなおすのではなく，$4a^3 + 27b^2 = 0 \pmod n$ のときは n と共通因数をもっていることになるので，最大公約数を計算することで n の因数 p または q が得られることになり，素因数分解が終了する．しかしそんなことが起こることは極端に小さい（n を適当な数で割ってみることと同じ意味になる）．

（4）4 については，計算が止まったときは補題 5 からある値 s のとき $[s]P = 0 \pmod p$ または $[s]P = 0 \pmod q$ のいずれか片方が成立しているので，$[s]P = P + [s - 1]P$ などと見て（実際のところは，$[8]P$ なら $P + P = [2]P$, $[2]P + [2]P = [4]P$, $[4]P + [4]P = [8]P$ のように高速計算するが，本質的な議論は変わらない），そのときの $P = (x_1, y_1)$ と $[s - 1]P = (x_2, y_2)$ を見る．このとき補題 1 から $x_1 - x_2$ または $2y_1$ が n の素因数の倍数になっているので，$gcd(n, x_1 - x_2)$ および $gcd(n, 2y_1)$ を計算することで p または q を得ることができる．

(5) $p-1$ 法と同様に，うまくいかないときはある．しかし a, b, x, y の値を変更することで，有理点の総数が変化していくため，もしかしたら有理点の総数が小さな素数でのみ構成されているようなときがあるかもしれない．このときは高い確率で素因数を得ることができるため，$p-1$ 法よりもはるかに効率よく素因数分解が得られると見積もれる． □

例 8 2 つ具体例をあげてみる．1 つ目は小さい数で，$p-1$ 法では困難だった例 6 を素因数分解してみる（小さい例でも手計算だとそれなりに重くみえるかもしれない）．

(1) $n=2047$ の素因数分解を考えてみる．

(2) $P=(9,7), a=5, b=1322$ としてみる．$B=3$ としてみると，$k=6$ である．

(3) $[6]P$ を計算してみる；全て mod 2047 している．

$$P+P=[2]P=(630,978),\quad [3]P=P+[2]P=(9,7)+(630,978)$$

となるが，この $P+[2]P$ を計算するところで，計算不能になってしまう．そこで x_1-x_2 を計算すると $630-9=621$ であり，これと $n=2047$ との最大公約数を計算すると

$$gcd(621,2047)=23$$

となって，素因数を得る．実際 $n=2047=23\times 89$ である．

(4) 具体的な計算は省略するが，この例の場合は $P+P=[2]P$, $[2]P+[2]P=[4]P$, $[4]P+[2]P=[6]P$ のようにして $[6]P$ の計算をしても（この場合は $[3]P$ で止まっているので当然だが）因数を得ることができる．補題 3 のように，$[k]P=\mathcal{O}$ は有理点の総数より前に $\mathcal{O}$ になることはある． □

例 9 もう 1 つは確め算は困難になるが，コンピュータを用いて少しだけ大きな数の素因数分解にしてみたい．

(1) $n=9058633$ の素因数分解を考えてみる．

(2) $P=(7,4), a=5, b=9058271$ とすると，自分のプログラムを動かすと $B=19$ とする必要があった．すなわち $k=232792560$ となり，それなりに大きな数が要求されることになる[*10]．これを見せるのは辞めて，(3)のようにしてみる．

(3) $P=(23,47), a=5, b=9048560$ としてみる．$B=11$ としてみると，$k=27720$ である．

(4) $[27720]P$ を計算してみる；全て mod 9058633 している．
$P+P=[2]P=(5306656,1097717)$, $[2]P+[2]P=[4]P=(2001700,5129463)$ のよう

[*10] 例 8 のようにその途中で計算が止まるときは充分ありえるし，実際には最小公倍数では不満なこともある．例えば $B=3$ とすると最小公倍数は 6 だが，実際には $2^3=8$ のように 2 しか因数にもたなくても最小公倍数よりも大きくなることはある．よって実装面でいえば，もう少し改善の余地がある．最小公倍数にしているのは，あくまでも倍数になりやすいであろうという予測があるからだ．

に順次計算すると

$$[16384]P = (1723334, 760504), \quad [8192]P = (7826354, 3478054)$$
$$[2048]P = (2009013, 94246), \quad [1024]P = (3082565, 724524)$$
$$[64]P = (3000053, 578184), \quad [8]P = (4846137, 3795235)$$

ができ，これらを全て足すと $[27720]P$ になるので，足してみる．すると

$$[16384]P + [8192]P + [2048]P + [1024]P + [64]P = [27712]P = (7542478, 3262288)$$

と最後に $[8]P = (4846137, 3795235)$ を加えようとすると

$$[27712]P + [8]P = (7542478, 3262288) + (4846137, 3795235)$$

この計算のところで，計算が不能になる．そこで $x_1 - x_2$ を計算すると
$7542478 - 4846137 = 2696341$ より $n = 9058633$ との最大公約数は

$$gcd(2696341, 9058633) = 2063$$

となって因数を得る．実際 $n = 2063 \times 4391$ である． □

また機会があれば楕円曲線暗号であったり，この楕円曲線法の実装であったりを説明するために，紀要の場をお借りするかもしれないが，予定されていた 3 回にわたり，暗号の数学的仕組みを中心に話をしてきた．第 1 回では歴史や現代暗号が備えていなければならない機能をさらい，特に RSA 暗号の仕組みを詳しくみた．第 2 回では RSA 暗号を実装することを考え，そのための数学的な準備と結果を示した．第 3 回では RSA 暗号を破る側からみたときの，素因数分解アルゴリズムをさらった．特に楕円曲線法は，素因数分解とは似ても似つかないような楕円曲線上の加法の定義から導かれる性質を用いることで素因数分解をするという，極めて奇妙な方法であるとともに，『計算不能なときに因数が見つかる』という仕組みも相まって，非常に美しい結果になっている．そのため楕円曲線法は基本的に数学（または数学に近いもの）を生業にしている方々向けに説明されることが多く，記述も専門的なことが多い．そのこともあって，この第 3 回は苦労した面もいくつかあった．その苦労によってこれが少しでも読みやすいものになっていることを願うばかりである．

参考文献

［1］Neal Koblitz（訳：櫻井幸一），“数論アルゴリズムと楕円曲線暗号理論入門”，シュプリンガー・ジャパン，1997.
［2］Richad Crandall・Carl Pomerance（監訳：和田秀雄），“素数全書”，朝倉書店，2010.