数体ふるい法による素因数分解について

小島 聡史

平成22年3月1日

目 次

1　はじめに

本修士論文は数体ふるい法のアルゴリズムについての Lenstra と Lenstra の論文 [5] の解説である. これは非常に大きい自然数を素因数分解するアルゴリズムであり, コンピューターで主に使用されている RSA 暗号の強度は大きい自然数の素因数分解の困難さに依存している. よって, 高速な素因数分解の実現は RSA 暗号が解読されてしまうことを意味するため, このアルゴリズムの研究は実用的に重要な意味を持つ. 数体ふるい法は現在知られているアルゴリズムの中では最も高速なものであるが, RSA 暗号を解読できるほどではない. 数体ふるい法の計算量は分解したい数を n とすると, およそ

$$\exp((64/9)^{1/3}(\log n)^{1/3}(\log\log n)^{2/3})$$

程度であり, これは $n = 10^{150}$ とするとおよそ 10^{19} 程度の数となり, また $n = 10^{300}$ とするとおよそ 6.5×10^{25} 程度の数となる.

最初に注意しておくが, 数体ふるい法は必ず成功するとは限らない. つまりアルゴリズムを実行しても自明な約数しか得られない場合がある. それでもたいていの場合に成功することが期待できるアルゴリズムである.

RSA 暗号について簡単に述べておく. まず適当な自然数 e と大きい 2 つの素数 p, q を選び, $n = pq$ を求める. 次に $de \equiv 1 \pmod{(p-1)(q-1)}$ を満たす d を計算する. そして平文 m を暗号化するときに用いる暗号化鍵 (e, n) を公開し, 暗号文 c を復号化するときに用いる復号化鍵 d を秘密に保管する. 暗号化と復号化は,

$$\begin{cases} \text{暗号化} \cdots c \equiv m^e \pmod{n}, \\ \text{復号化} \cdots m \equiv c^d \pmod{n} \end{cases}$$

という計算により実行される. 暗号化は e と n が公開されているので誰でも簡単にできるが, 復号化に必要な d は p と q を知らないと計算が困難であり, p と q を知るためには n を素因数分解する必要がある. この素因数分解の困難さが RSA 暗号の安全性の根拠である. ただし, n の素因数 p と q が 10 進で数桁しか違わないような近いものである場合は Fermat 法と呼ばれる方法を用いることで n が高速に因数分解されてしまうので, 暗号に用いる素数の選び方には注意が必要である. Fermat 法は n が 2 つの平方数の差として表され, これら 2 つの平方数の一方が非常に小さいという事実を用いる方法である.

はじめに本論文で用いる代数的整数論の定義や定理をいくつか述べておく.

定義 1.1 (ノルム). 代数体 K の元 α に対してその共役元を $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_d$ とする. このとき α のノルム $N(\alpha)$ とトレース $T(\alpha)$ を

$$\begin{aligned} N(\alpha) &= \alpha_1\alpha_2\cdots\alpha_d, \\ T(\alpha) &= \alpha_1 + \alpha_2 + \cdots + \alpha_d \end{aligned}$$

と定義する.

α の最小多項式を $f(x) = c_d x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0$ とすると $N(\alpha) = (-1)^d (c_0/c_d)$ である. また, $a + b\alpha$ $(a, b \in \mathbb{Q}, b \neq 0)$ ならば,

$$N(a + b\alpha) = (-1)^d \frac{f(-a/b)}{c_d/b^d} = (-b)^d \frac{f(-a/b)}{c_d}$$

であるから,

$$c_d N(a + b\alpha) = c_d a^d + c_{d-1} a^{d-1}(-b) + \cdots + c_1 a(-b)^{d-1} c_0 (-b)^d$$

となる.

定義 1.2 (**多項式の判別式**). 既約多項式 $f(x)$ の根を $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_d$ とする. このとき f の判別式 D_f を

$$D_f = \Big(\prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j) \Big)^2$$

と定義する.

定義 1.3 (**体の判別式**). d 次の既約多項式 $f(x)$ の根を α とし, 代数体 $K = \mathbb{Q}(\alpha)$ の整数基底を $\omega_1,\ \omega_2,\ \cdots,\ \omega_d$ とする. このとき体 K の判別式 D_K を

$$D_K = \big(\det(\omega_j^{(j)}) \big)^2$$

と定義する.

これらの判別式に対して次の定理が成り立つ.

定理 1.4. O_K を体 K の整数環とし, K の代数的整数 α の d 次の最小多項式を $f(x)$ とする. このとき

$$D_f / D_K = (O_K : \mathbb{Z}[\alpha])^2$$

が成り立つ.

この定理より D_f が平方因子を持たなければ, $(O_K : \mathbb{Z}[\alpha]) = 1$ すなわち $O_K = \mathbb{Z}[\alpha]$ であり, $1,\ \omega,\ \cdots,\ \omega^{d-1}$ は K の整数基底となる.

整数環のイデアルについては一般に次の定理が成り立つ.

定理 1.5. 整数環のイデアルは必ず有限個の素イデアルの積に分解され, その分解の仕方は一意的である.

数体ふるい法では素数の素イデアル分解に関する次の定理が重要である.

定理 1.6. 代数的整数 α の最小多項式を $f(x)$ とし, 体 $K = \mathbb{Q}(\alpha)$ の整数環を O_K とする. さらに, 素数 p を指数 $(O_K : \mathbb{Z}[\alpha])$ を割らないものとする. このとき $f(x)$ が $\bmod p$ で

$$f(x) \equiv q_1(x)^{e_1} q_2(x)^{e_2} \cdots q_l(x)^{e_l} \pmod{p}$$

と既約分解されるならば, $P_i = (p,\ q_i(\alpha))$ とおくと P_i は素イデアルであり, 単項イデアル (p) は,

$$(P) = P_1^{e_1} P_2^{e_2} \cdots P_l^{e_l}$$

と素イデアル分解される.

謝辞

セミナーや論文作成にあたり親切に指導してくださった雪江先生に深く感謝致します. また, セミナーで共に学び, 数多くのアドバイスをいただいた五十嵐健太君, 佐々木万喜夫君, 田中修平君, 山田洋輔君にも感謝致します.

2 概要

数体ふるい法による因数分解では次の事実を利用する.

$$x^2 \equiv y^2 \pmod{n} \text{ かつ } x \not\equiv \pm y \pmod{n} \implies 1 < \gcd(x \pm y,\ n) < n \tag{2.1}$$

この仮定を満たす x, y を構成するアルゴリズムが数体ふるい法である. また, $x^2 \equiv y^2 \pmod{n}$ である x, y に対して高々50 %の確率で $x \equiv \pm y \pmod{n}$ となってしまい, n の非自明な約数がみつからないことがあるので, 数体ふるい法は確率的アルゴリズムである.

数体ふるい法は名前の通り, 代数体を用いた因数分解法である. ここでは基になるアイデアを述べることにし, 具体的な内容は次節以降に述べる.

まずは代数体を構成する. 整数係数多項式 $f(x)$ を 1 つ固定し, その根を $\alpha \in \mathbb{C}$ とし, $m \in \mathbb{Z}/n\mathbb{Z}$ を n を法とする f の根とする.

この α を用いて代数体を $K = \mathbb{Q}(\alpha)$ と定義する. さらに K の整数環 O_K を考えるのだが, ここでは簡単のために $\mathbb{Z}[\alpha] = O_K$ であることと, $\mathbb{Z}[\alpha]$ が UFD であることを仮定する. これらを仮定しない場合については後に述べる.

そして次の環準同型を考える.

$$\varphi : \mathbb{Z}[\alpha] \longrightarrow \mathbb{Z}/n\mathbb{Z} \quad (\alpha \longmapsto m)$$

次が数体ふるい法の重要なアイデアである.

$\gcd(a, b) = 1$ を満たす $a, b \in \mathbb{Z}$ に対して次の図式を考える.

$$\begin{array}{ccc} a + b\alpha & \longrightarrow & \mathbb{Z}[\alpha] \text{ の素元の積} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ a + bm & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \text{ の元の積} \end{array}$$

ここで, $a + bm$ は n より小さい数を考えるので, "$a + bm \longrightarrow \mathbb{Z}/n\mathbb{Z}$ の元の積"は, $\mathbb{Z}$ での素因数分解と同様である. この図式により得られる 2 つの分解の違いを利用する事で得られる, n を法とした合同式を複数個集め, それらをかけ合わせることで (2.1) で書いた $x^2 \equiv y^2 \pmod{n}$ という形の合同式を構成するのである.

例 2.2. $n = 2117$, $m = 46$, $f(x) = x^2 + 1$, $\alpha = \sqrt{-1}$ のとき

$$\begin{array}{ccc} 1 + 5\sqrt{-1} & \longrightarrow & (1 + \sqrt{-1})(3 + 2\sqrt{-1}) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ 1 + 5 \times 46 = 231 & \longrightarrow & 3 \cdot 7 \cdot 11 \equiv 47 \cdot 95 \pmod{2117} \end{array}$$

前の図式において $a_0 + a_1\alpha + a_2\alpha^2 + \cdots$ という $\mathbb{Z}[\alpha]$ の任意の元ではなく, $a + b\alpha$ という形の元を用いた理由は, $a + b\alpha$ の $\mathbb{Z}[\alpha]$ での分解の様子を分かりやすくするための補題 2.3 が成り立つからである.

$\mathbb{Z}[\alpha]$ の素イデアル P のノルムは通常

$$N(P) := \#(\mathbb{Z}[\alpha]/P) = p^f \quad (p : \text{素数},\ f \in \mathbb{Z})$$

という素数のべきで表されるが, $a + b\alpha$ を含む素イデアルの場合は次の補題が成り立つ.

補題 2.3. $a, b \in \mathbb{Z},\ \gcd(a, b) = 1$ とする. このとき $a + b\alpha$を含む $\mathbb{Z}[\alpha]$ の素イデアルのノルムは素数である.

証明. P を $a + b\alpha$ を含む素イデアルとし, 有限体 F に対して環準同型 ψ を

$$\psi : \mathbb{Z}[\alpha] \longrightarrow F,\quad \mathrm{Ker}\psi = P$$

と定義する. すなわち, $\mathbb{Z}[\alpha]/P \cong F$ が成り立つような F を考える. F の標数を p (素数) とすると $\mathbb{F}_p$ は F の部分体である. $a+b\alpha \in P$ なので, $\psi(a+b\alpha) = 0$ である. よって

$$\psi(a) = -\psi(b)\psi(\alpha)$$

が成り立つ. $a, b \in \mathbb{Z}$ より $\psi(a), \psi(b) \in \mathbb{F}_p$ であることに注意しておく. もし $\psi(b) = 0$ ならば $\psi(a) = 0$ であるから, a, b が共に p で割り切れることになり, $\gcd(a, b) = 1$ に矛盾する. よって, $\psi(b) = 0$ であり, $\psi(\alpha) = -\psi(a)\psi(b)^{-1} \in \mathbb{F}_p$ となる.

したがって $F = \mathbb{F}_p$ となり,

$$\mathbb{Z}[\alpha]/P \cong \mathbb{F}_p$$

が成り立つので, ノルムの定義より $N(P) = p$ が成り立つ. □

実際に $a + b\alpha$ を $\mathbb{Z}[\alpha]$ の素元の積に分解するのは手間がかかるが, 補題 2.3 により $a+b\alpha$ の分解のおおまかな様子を $N(a+b\alpha)$ の素因数分解を用いて知ることができる.

例 2.4. $a + b\alpha = 1 + 7\sqrt{-1}$ に対して

$$\begin{cases} N(1 + 7\sqrt{-1}) = 50 = 2 \times 5^2, \\ 1 + 7\sqrt{-1} = -\sqrt{-1}(1 + \sqrt{-1})(1 + 2\sqrt{-1})^2. \end{cases}$$

ここで, $N(1 + \sqrt{-1}) = 2,\ N(1 + 2\sqrt{-1}) = 5.$

この例では $1 + 7\sqrt{-1}$ のノルムが 2 で 1 回割れ, 5 で 2 回割れることに対応して, $1 + 7\sqrt{-1}$ がノルム 2 の元 $1 + \sqrt{-1}$ で 1 回割れ, ノルム 5 の元 $1 + 2\sqrt{-1}$ で 2 回割れ

ることが分かる. よって, $a+b\alpha$ を素元分解する場合にその素因数が分かったなら, ノルムの計算によって素因数のべき指数を知ることができる.

$a+bm, N(a+b\alpha)$ の分解を考える際, これら自身は大きくてもかまわないが, その素因数は小さいほうが扱いやすい. そこで, 次の定義を与える.

定義 2.5. B を正の定数とする. このとき, $k \in \mathbb{Z}$ が B-smooth であるということを k の全ての素因数が B 以下であることと定義する. また $\gamma \in O_K$ が B-smooth であるということを $N(\gamma)$ の全ての素因数が B 以下であることと定義する.

3　アルゴリズム

各段階での詳しい説明は次節以降にすることにして, この節ではアルゴリズムの大まかな流れを述べる.

Step 1. $f(x)$ を構成する.

前節で述べたような多項式を構成するのであるが, その係数がなるべく小さくなるようにとりたい. ここでは base m method と呼ばれる方法を用いる. このアルゴリズムの目標は $f(m) = n$ を満たす多項式を構成することである.

まず $n > 2^{d^2}$ を満たす $d \in \mathbb{Z}_{>1}$ を 1 つ選び, $m = [n^{1/d}]$ とおく. 次に n を

$$n = c_d m^d + c_{d-1} m^{d-1} + \cdots + c_0 \quad (c_i \in \mathbb{Z}) \tag{3.1}$$

と m 進展開し,

$$f(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_0$$

とする. この f は $f(m) = n$ を満たす.

この方法を用いる利点は $f(x)$ がモニックになることである.

命題 3.2. (3.1) において, $c_d = 1$ と $c_{d-1} \leq d$ が成り立つ.

証明. $1 \leq i \leq d-1$ である i に対して $2^d = (1+1)^d = \sum_{i=1}^{d-1} \binom{d}{i} + 2$ であるから, 各 i に対して $\binom{d}{i} \leq 2^d - 2 < n^{1/d} - 2 \leq m - 1$ が成り立つ. さらに,

$$(m+1)^d = m^d + \binom{d}{1} m^{d-1} + \binom{d}{2} m^{d-2} + \cdots + \binom{d}{d-1} m + 1 \tag{3.3}$$

であるから, これは $(m+1)^d$ の m 進展開を与えている. よって (3.1) と (3.3) の係数を比較して, $c_d \neq 1$ とすると $m^d \leq n < (m+1)^d$ に矛盾する. したがって $c_d = 1$ である. また, $c_{d-1} > d$ とするとやはり $m^d \leq n < (m+1)^d$ に矛盾するので $c_{d-1} \leq d$ である. □

d は n が 200 桁以上なら $d = 6$, 100 桁以上なら $d = 5$, 80 桁程以上なら $d = 4$, 60 桁以下なら $d = 3$ ととればいい.

f が可約であれば, 次の操作を行う. まず,

$$f(x) = g(x)h(x) \quad (g, h \in \mathbb{Z}[x])$$

と分解する. f がモニックなので, g と h もモニックにとれる. 次に m を代入して,

$$n = f(m) = g(m)h(m)$$

とする. $g(m) \neq 1, n$ ならば n の非自明な因数が見つかったことになるので, アルゴリズムは終了する. $g(m) = n$ であれば, この条件を満たす既約多項式を求めることが base m method の目標だったので, f を g で置き換えればいい.

整数係数多項式を既約多項式の積に分解するアルゴリズムについては [6] の Section 3 を参照のこと.

Step 2. 素因数の候補を求める.

B を 10^8 程度の定数とし, 集合

$$\begin{cases} F = \{p : \text{prime} \mid p \leq B\}, \\ G = \{\pi_P : \mathbb{Z}[\alpha] \text{の素元} \mid |N(\pi_P)| \leq B\}, \\ U = \{\mathbb{Z}[\alpha]^\times \text{の生成元}\} \end{cases} \tag{3.4}$$

を求める.

今, $\mathbb{Z}[\alpha]$ は UFD だと仮定しているので, π_P は $\mathbb{Z}[\alpha]$ の素イデアルの生成元である. また, $P = (\pi_P)$ であるとき, $N(P) = |N(\pi_P)|$ であることを注意しておく.

Step 3. B-smooth な数を求める.

$a + bm$ と $a + b\alpha$ が条件

$$\begin{cases} \gcd(a, b) = 1 \\ a + bm = \displaystyle\prod_{p \in F} p^{e_p} \\ a + b\alpha = \displaystyle\prod_{\gamma \in G \cup U} \gamma^{e_\gamma} \end{cases}$$

を満たすような整数の組 (a, b) を $\#(F \cup G \cup U)$ 個より多くみつける. 2 番目の条件は $a + bm$ が B-smooth であるという意味で, 3 番目の条件は $a + b\alpha$ が B-smooth であるという意味である.

このような (a, b) を見つけるためには a, b をある範囲で動かして $a + bm, a + b\alpha$ が B-smooth かどうかを確かめるという方法をとるが, 動かす範囲はそれぞれ

$$-10^7 \leq a \leq 10^7, \quad 1 \leq b \leq 10^7$$

程度であればいいとされている.

$a + b\alpha$ を φ でうつして,

$$\begin{cases} a + bm = \displaystyle\prod_{p \in F} p^{e_p}, \\ \varphi(a + b\alpha) = \displaystyle\prod_{\gamma \in G \cup U} \varphi(\gamma)^{e_\gamma} \end{cases}$$

という 2 つの $\mathbb{Z}/n\mathbb{Z}$ の元の積の形を得る. これらは $\mathbb{Z}$ で等しいとは限らないが, $\mathbb{Z}/n\mathbb{Z}$ では等しいので,

$$\prod_{p\in F} p^{e_p} \equiv \prod_{\gamma\in G\cup U} \varphi(\gamma)^{e_\gamma} \pmod{n} \tag{3.5}$$

という合同式が得られる.

Step 4. $x^2 \equiv y^2 \pmod{n}$ という形の合同式を求める.

(3.5) の合同式と, その指数部分を 2 を法として考えて得られるベクトル

$$((e_p \bmod 2), ((e_\gamma \bmod 2))_{p\in F,\gamma\in G\cup U}$$

を対応させる. このようなベクトルは $\#(F\cup G\cup U)$ 個より多くあるので線型従属である. そこで, 行列の掃き出しを用いて, 和が 2 を法としてゼロベクトルになるベクトルの組を見つける. この組のベクトルに対応する合同式を掛け合わせると

$$\prod_{p\in F} p^{2w_p} \equiv \prod_{\gamma\in G\cup U} \varphi(\gamma)^{2w_\gamma} \pmod{n}$$

という形の条件が得られるので,

$$x = \prod_{p\in F} p^{w_p},\ y = \prod_{\gamma\in G\cup U} \varphi(\gamma)^{w_\gamma}$$

とおくと, $x^2 \equiv y^2 \pmod{n}$ を満たす x, y が得られる. この x, y に対して $x \not\equiv \pm y \pmod{n}$ であれば n の約数がみつかり, アルゴリズムは終了する. $x \equiv \pm y \pmod{n}$ となってしまった場合は Step 4. でベクトルの組を選びなおす.

4　素イデアルの生成元の求め方

この節では主に (3.4) の G の元, 即ち $\mathbb{Z}[\alpha]$ の素イデアルの生成元の求め方について述べる. U の元は G の元を求める過程で同時に求めることになる. なお, この節で述べるアルゴリズムは G の元を全て求めるものではなく, 数体ふるいを実行するために十分な数の元を求めるものである.

素数 p に対して

$$f(x) \equiv (x-c)g(x) \pmod{p} \quad (c \in \mathbb{Z} \text{ は } p \text{ に依存する定数})$$

であるとき, $P = (p,\ \alpha - c)$ とおくと

$$\begin{aligned} \mathbb{Z}[\alpha]/(p,\ \alpha - c) &\cong \mathbb{Z}[x]/(f(x), p, \alpha - c) \\ &\cong \mathbb{F}_p[x]/(x-c) \\ &\cong \mathbb{F}_p \end{aligned}$$

が成り立つので, P は $\mathbb{Z}[\alpha]$ の素イデアルとなる. このとき, $\gamma \in \mathbb{Z}[\alpha]$ が P の生成元であるためには $|N(\gamma)| = p$ かつ $\gamma \in P$ であればいいので,

$$(4.1)\quad \gamma = \sum_{i=0}^{d-1} s_i \alpha^i \in \mathbb{Z}[\alpha] \text{ が } P \text{ の生成元} \iff |N(\gamma)| = p \text{ かつ } \sum_{i=0}^{d-1} s_i c^i \equiv 0 \pmod{p}$$

が成り立つ.

注 4.2. (4.1) において 2 つめの条件がないと, γ が $P = (p,\ \alpha - c)$ の生成元なのか $P' = (p,\ \alpha - c')$ の生成元なのかが分からない. 即ちこれは γ が P の生成元であることを保証するための条件である. どのイデアルの生成元なのかをはっきりさせておくことは, 次節で $a + b\alpha$ の素元分解を求める際に非常に役に立つ.

次に素元を効率的に求める際に有効な 2 つの定数 L, M について述べる.

記号の準備からはじめる. K の整数環 O_K の判別式 Δ を $\Delta = D_f/[O_K : \mathbb{Z}[\alpha]]^2$ で定義する. また, ω_d を $\mathbb{R}^d$ の単位球の体積 $\omega_d = \pi^{d/2}/\Gamma(1+\frac{1}{2})$ とし, $v_d = (4/d)^{(d/2)}/\omega_d$ とおく. このとき定数 L, M を

$$L = (v_d \cdot \sqrt{\Delta} \cdot B)^{2/d}, \quad M = [v_d \cdot \sqrt{\Delta}]$$

と定義する. ここで B は B-smooth の B, すなわち素因数の大きさの上限である.

$\gamma = \sum_{i=0}^{d-1} s_i \alpha^i \in O_K$ で, $\sum_{i=0}^{d-1} |s_i N(\alpha)^{i/d}|^2 \leq L$ を満たすものを考える. このような γ に対して,

$$\begin{aligned} |N(\gamma)| &= |\sum_{i=0}^{d-1} s_i^d N(\alpha)^i| \leq \sum_{i=0}^{d-1} |s_i^d N(\alpha)^i| \\ &\leq \sum_{i=0}^{d-1} |s_i^2 N(\alpha)^{2i/d}|^{d/2} \leq (\sum_{i=0}^{d-1} |s_i^2 N(\alpha)^{2i/d}|)^{d/2} \leq L^{d/2} \leq M \cdot B \end{aligned}$$

が成り立つ. これはどういうことかというと, 素元を効率よく求めるためには $|N(\gamma)| = p$ を満たす γ だけではなく, $|N(\gamma)| = kp$ $(k \in \mathbb{Z})$ のようにノルムが素数の整数倍となっているものも利用する必要があるが, 上で述べたような γ を考えた場合には k があまり大きくない数 M で抑えられるということである.

上の議論より G, U の元を求めるアルゴリズムは次のようになる.

1. $P = (p,\ \alpha - c)$ という形の $\mathbb{Z}[\alpha]$ の素イデアルを全て求める. つまり, $f(x)$ の 1 次因子を全て求める.
2. $\sum_{i=0}^{d-1} |s_i N(\alpha)^{i/d}|^2 \leq L$ を満たす $\gamma = \gamma(\alpha) = \sum_{i=0}^{d-1} s_i \alpha^i$ に対して $N(\gamma)$ を求める.
3. $|N(\gamma)| = 1$ である γ を U の元とする.
4. ある $(p,\ \alpha - c)$ に対して, $|N(\gamma)| = p$ かつ $\gamma(c) \equiv 0 \pmod{p}$ を満たす γ を G の元とする. また, γ がどのイデアルの生成元かという情報も記録しておく.

これだけでは十分な数が集まらない可能性があるのでさらに次を実行する.

5. $|N(\gamma)/N(\gamma')| = 1$ となる γ, γ' がある場合, $\gamma/\gamma' \in \mathbb{Z}[\alpha]$ ならば γ/γ' を U の元とする.
6. $|N(\gamma)| = kp$ かつ $|N(\gamma')| = k$ $(k \in \mathbb{Z})$ である γ, γ' がある場合, $\gamma(c)/\gamma'(c) \equiv\ 0 \pmod{p}$ を満たす $(p,\ \alpha - c)$ があり, かつ $\gamma/\gamma' \in \mathbb{Z}[\alpha]$ ならば γ/γ' を G の元とする.

次に, $f(x)$ の p を法とした一次因子の求め方について述べる. 基本になるのは次の式である.

$$x^p - x = \prod_{i=0}^{p-1} (x - i) \pmod{p}$$

これより

$$f_1(x) = \gcd(f(x),\ x^p - x)$$

は $f(x)$ の全ての 1 次因子の積となる. この $f_1(x)$ を 1 次因子に分解したい.

pが小さければ$k = 0, 1, \cdots, p-1$に対して$f_1(k) \equiv 0 \pmod{p}$かどうかを確かめればよい.

pが大きいときは次の式を用いたほうが高速に実行できる.

$$x^p - x = (x+a)((x+a)^{(p-1)/2} + 1)((x+a)^{(p-1)/2} - 1) \qquad (a = 0, 1, \cdots, p-1)$$

これより, まず$a = 0$に対して

$$g_1(x) = \gcd(f_1(x),\ (x+a)^{(p-1)/2} + 1)$$

を計算する. $1 \leq \deg g_1 < \deg f_1$であれば$h_1(x) = f_1(x)/g_1(x)$とおくと

$$f_1(x) = g_1(x)h_1(x)$$

と分解される. そうでなければ$a = 1$に対して$g_1(x)$を求め, 同様の処理をする. さらに$g_1(x), h_1(x)$を同様に分解することで$f_1(x)$を完全に分解する.

5　ふるいの実行

$a+bm, a+b\alpha$ が共に B-smooth であるような整数の組 (a,b) を見つけたい. 具体的には, a,b を動かして $a+bm$ が B-smooth になる (a,b) を求める. そしてこの (a,b) に対して $a+b\alpha$ が B-smooth かどうかを調べる, という方法をとる.

$a+bm$ の分解は容易であるが, $a+b\alpha$ を実際に $\mathbb{Z}[\alpha]$ の素元で割るのは手間がかかる. この手間を避けるために $a+b\alpha$ の素イデアル分解と $N(a+b\alpha)$ の素因数分解を対応させる. これについては 2 節で簡単な例をあげてある.

まず, 素イデアル $(\pi_P) = P = (p,\ \alpha - c)$ に対して

$$\begin{aligned} \pi_P \mid a+b\alpha &\iff P = (p, \alpha - c) \mid (a+b\alpha) \\ &\iff a + bc \equiv 0 \pmod{p} \end{aligned}$$

が成り立つ. これにより, π_P が $a+b\alpha$ を割るかどうかをたしかめることは π_P と対応する組 (p,c) が $a+bc \equiv 0 \pmod{p}$ を満たすかどうかを調べることに帰着できる.
また, 例 2.4 で触れたとおり

$$p^k \mid N(a+b\alpha) \iff \pi_P^k \mid a+b\alpha$$

であるから, $a+b\alpha$ の分解の指数部分は $N(a+b\alpha)$ の素因数分解の指数部分に帰着される.

注 5.1. $a+b\alpha$ は同じ素数 p を用いた 2 つの素イデアル $(p,\ \alpha-c)$ と $(p,\ \alpha-c')$ で同時に割れることはない.

以上の議論より, 目的の組 (a,b) を求めるアルゴリズムは次のようになる.

・まず $a+bm$ が B-smooth になる (a,b) を求める
1. $b=1,\ p=2$ として、$p|a+bm$ となる a を探す. これは $a = 0, \pm1, \pm2, \cdots$ と順番に試していけばいい. そのような a が見つかったら, $(a+ip)+(b+jp)m$ が p で割れることを記録しておく.
2. p を p のべきで置き換えて 1 を実行する.
3. $p \le B$ に対して 1,2 を実行する.
4. b を $b+1$ で置き換えてはじめからくり返す.

これはつまり, b を 1 つ固定して a を動かし, $a+bm$ が F の元で割れるかどうかを調べ, 全ての a について調べたら b を 1 つ動かして同様の処理をする, ということである. これにより

$$a + bm = \prod_{p \le B} p^{e_p} \times r$$

という分解が得られるが, r が $B < r < B^2$ であるもの以外は捨てる.

・次に上で得られた (a, b) に対して $a + b\alpha$ を G の元で分解する.

1. 全ての $P = (\pi_P) = (p, \alpha - c)$ に対して $a + bc \equiv 0 \pmod{p}$ が成り立つかどうか調べる.
2. 1 の合同式が成り立つ (p, c) に対応する素元 π_P を素因子として選び出す. これらのノルムは相異なる
3. $N(a + b\alpha) = \prod_{p \leq B} p^k \times s$ を求め, $a + b\alpha = \prod_{p \leq B} \pi_{P(p)}^k \times \sigma$ を得る.
   ここで, $\pi_{P(p)}$ はノルムが p の素元を表し、$N(\sigma) = s$ である.
4. s が $B < s < B^2$ かつ素数であるもの以外は捨てる.

以上のアルゴリズムにより, 次のような a, b がたくさん得られる.

$$\begin{cases} (a, b) = 1, \\ a + bm = \prod_{p \leq B} p^{e_p} \times r, \\ N(a + b\alpha) = \prod_{q \leq B} q^{e_q} \times s \end{cases}$$

本来は $r = s = 1$ であるものだけを求めていたが, それでは十分な数が集まらないので, 1 個ずつ現れることを許してうまく処理する.

・$s = 1$ の場合

$$\begin{cases} a + bm = \prod_{p \leq B} p^{e_p} \times r, \\ N(a + b\alpha) = \prod_{q \leq B} q^{e_q} \end{cases}$$

$$\begin{cases} a' + b'm = \prod_{p \leq B} p^{e_p{}'} \times r, \\ N(a' + b'\alpha) = \prod_{q \leq B} q^{e_q{}'} \end{cases}$$

となる (a', b') を探す. そのような (a', b') があればそれぞれ積をとって

$$\begin{cases} (a + bm)(a' + b'm) = \prod_{p \leq B} p^{e_p + e_p{}'} \times r^2, \\ N(a + b\alpha)N(a' + b'\alpha) = \prod_{q \leq B} q^{e_q + e_q{}'} \end{cases}$$

とする. この積は $r = s = 1$ と同様に扱うことができる. 実際, 目標としていたのは

$$\prod(a + bm) = \left(\prod_{p \leq B} p^{w_p}\right)^2$$

という形だったので, 右辺に r^2 が現れても

$$\prod(a + bm) = \left(\prod_{p \leq B} p^{w_p} \times r\right)^2$$

と, 問題なく処理できる.

r が一致する (a', b') がない場合は (a, b) を捨てる.

・$r = 1$ の場合

$$\begin{cases} a + bm = \prod_{p \leq B} p^{e_p}, \\ N(a + b\alpha) = \prod_{q \leq B} q^{e_q} \times s \end{cases}$$

$$\begin{cases} a' + b'm = \prod_{p \leq B} p^{e_p{}'}, \\ N(a' + b'\alpha) = \prod_{q \leq B} q^{e_q{}'} \times s \end{cases}$$

となる (a', b') を探す. 平方を作るという目標は同じだが, s が一致していてもノルムをとる前のイデアルも一致しているとは限らない. そこで, s とイデアルが共に一致する条件を考える.

$(a + b\alpha)$ を割るイデアルは $(s, \alpha - c)$ と書け, $(a' + b'\alpha)$ を割るイデアルは $(s, \alpha - c')$ と書ける. つまり 2 つのイデアルが一致するということは, $c = c'$ が成り立つということである.

今, c は $c \equiv -ab^{-1} \pmod{s}$ を満たしていたので, $ab^{-1} \equiv a'b'^{-1} \pmod{s}$ であればイデアルは一致する.

よって $r = 1$ の場合は, s が一致し, かつ $ab^{-1} \equiv a'b'^{-1} \pmod{s}$ を満たす (a', b') を見つけて

$$\begin{cases} (a + bm)(a' + b'm) = \prod_{p \leq B} p^{e_p + e_p{}'}, \\ N(a + b\alpha)N(a' + b'\alpha) = \prod_{q \leq B} q^{e_q + e_q{}'} \times s^2 \end{cases}$$

という積を作ることで $r = s = 1$ の場合と同様に処理できる.

6　単数部分の分解

この節では $a+b\alpha$ の単数部分を分解する方法を述べる.
$U=\{u_0,u_1,\cdots,u_l\},\ u_0=-1$ とおき,

$$a+b\alpha=u\cdot\prod_{g\in G}g^{e(g)},\quad u=\prod_{i=0}^{l}u_i^{e(u_i)} \tag{6.1}$$

と表す. この $e(u_i)$ を求めることが目標である. 次に α の共役元 $\alpha_1,\cdots\alpha_l$ に対し, l 個の埋め込み $\psi_1,\cdots\psi_l$ を

$$\psi_i:K\longrightarrow\mathbb{C}\ \ (\alpha\longmapsto\alpha_i)$$

と定める. そして, 0 でない K の元 x に対し, l 次元実ベクトル $\nu(x)$ を

$$\nu(x):=(\log|\psi_1(x)|,\ \log|\psi_2(x)|,\ \cdots,\ \log|\psi_l(x)|)$$

と定めると, $\nu(u)$ の第 i 成分は,

$$e(u_1)\log|\psi_i(u_1)|+e(u_2)\log|\psi_i(u_2)|+\cdots+e(u_l)\log|\psi_i(u_l)|$$

とかけるので,

$${}^t\nu(u)=\begin{pmatrix}\log|\psi_1(u_1)| & \cdots & \log|\psi_1(u_l)|\\ \log|\psi_2(u_1)| & \cdots & \log|\psi_2(u_l)|\\ \vdots & \ddots & \vdots\\ \log|\psi_l(u_1)| & \cdots & \log|\psi_l(u_l)|\end{pmatrix}\begin{pmatrix}e(u_1)\\ e(u_2)\\ \vdots\\ e(u_l)\end{pmatrix}$$

という関係式が成り立つ. これより,

$$\begin{pmatrix}e(u_1)\\ e(u_2)\\ \vdots\\ e(u_l)\end{pmatrix}=\begin{pmatrix}\log|\psi_1(u_1)| & \cdots & \log|\psi_1(u_l)|\\ \log|\psi_2(u_1)| & \cdots & \log|\psi_2(u_l)|\\ \vdots & \ddots & \vdots\\ \log|\psi_l(u_1)| & \cdots & \log|\psi_l(u_l)|\end{pmatrix}^{-1}\cdot\ {}^t\nu(u)$$

の右辺を計算することで $e(u_1),\cdots,e(u_l)$ を求めることができる. では, $\nu(u)$ はどのように求めればいいのだろうか. これには次の命題を用いる.

命題 6.2. $\nu(u)=\nu(a+b\alpha)-\sum_{g\in G}e(g)\nu(g)$

証明. 両辺の第 i 成分が等しいことを言えばいい

$$\begin{aligned}(\text{右辺の第 }i\text{ 成分}) &= \log|\psi_i(a+b\alpha)|-\sum e(g)\log|\psi_i(g)|\\ &= \log|\psi_i(a+b\alpha)|+\log\prod|\psi_i(g)^{-e(g)}|\\ &= \log|\psi_i\big((a+b\alpha)\prod g^{-e(g)}\big)|\\ &= \log|\psi_i(u)|=(\text{左辺の第 }i\text{ 成分})\end{aligned}$$

□

残る問題は $e(u_0)$ を決定することである.

$f(x)$ が実根を持つ場合, $\mathbb{Q}(\alpha)$ から $\mathbb{R}$ への実埋め込み σ で, $\sigma(u_i),\ \sigma(g) > 0\ (1 < i < l,\ g \in G)$ となるものを考え,

$$e(u_0) = \begin{cases} 0 & (\sigma(a + b\alpha) > 0) \\ 1 & (\sigma(a + b\alpha) < 0) \end{cases}$$

とする.

$f(x)$ が実根を持たないなら複素埋め込みを 1 つ固定し, (6.1) の両辺の埋め込みの偏角が一致するように $e(u_0)$ を定める.

7　UFD ではない場合

これまでの議論では $\mathbb{Z}[\alpha]$ が UFD であるとしていたが, これは非常に強い仮定であるため扱える数が少なくなってしまう. よって, UFD でない場合でも数体ふるい法が実行できるようにしたい. 簡単のためにこの節でもこれまでと同様に $\mathbb{Z}[\alpha] = O_K$ は仮定する.

最初に注意しておくと, $\mathbb{Z}[\alpha]$ が UFD であるための必要十分条件は類数が 1 であることである. K が二次体くらいであれば類数を求めることはそれほど難しくはないが, 次数が大きくなると難しくなる.

まず 4 節で考えた素イデアルに対する指標を定義する.

定義 7.1. 各素イデアル $(p, \alpha - c)$ に対して指標 $\chi = \chi(p, c)$ を

$$\chi(a + b\alpha) = \left(\frac{a + bc}{p}\right)$$

と定義する. ただし, 右辺は平方剰余記号である.

$\mathbb{Z}[\alpha]$ が UFD であることを仮定しない場合, 素元分解はできないが素イデアル分解は可能である. そこで有理整数の集合 F と素イデアルの集合 G に対して, $a + bm$ と $a + b\alpha$ が

$$\begin{cases} a + bm = \displaystyle\prod_{p \in F} p^{e_p} \\ (a + b\alpha) = \displaystyle\prod_{P \in G} P^{e_P} \end{cases} \tag{7.2}$$

と完全に分解されているものとする. これまでと同様に平方を考えたいのであるが, 今回は 2 つの積に“平方数”と“平方イデアルを生成する数”という差がある. そこで, 平方剰余を用いてこの差を埋める.

素イデアル $P = (p, \alpha - c)$ と, どの $a + b\alpha$ も割らないような大きい素数 p を考える. このとき, $a + b\alpha$ が P を法として平方数であることと, $a + bc$ が p を法として平方数であることとがほぼ同値であることがわかる. すなわち, $a + b\alpha$ が O_K で平方数であれば $a + bc$ が p を法として平方剰余でなければならず, $a + bc$ が p を法として平方剰余であれば $a + b\alpha$ が O_K で平方数である可能性が高いといえる (詳しくは [3] の p.290, Lem.6.2.4 を参照).

次に平方数を求める. 指標の集合を H とし, $\chi \in H$ に対して,

$$\chi(a + b\alpha) = (-1)^{e_\chi} \tag{7.3}$$

と表すことにする. ただし, $a + b\alpha$ が χ の法と互いに素であるようにするために, 法を G に含まれる素イデアルで割れないようにとる.

(7.2) と (7.3) を満たす組 (a,b) を $\#(F\cup G\cup H)$ 個より多くみつけると, 各べき指数を 2 を法として考えたベクトル

$$((e_p \bmod 2),\ (e_P \bmod 2),\ (e_\chi))_{p\in F,\ P\in G,\ \chi\in H}$$

は線型従属となり, 2 節と同様に適当に組み合わせることにより,

$$\prod(a+bm) = \Big(\prod_{p\in F} p^{e_p}\Big)^2$$

という $\mathbb{Z}$ の平方数と

$$\Big(\prod(a+b\alpha)\Big) = \Big(\prod_{P\in G} P^{e_P}\Big)^2 \tag{7.4}$$

という O_K の平方イデアルを得ることができ, さらに

$$\chi\Big(\prod(a+b\alpha)\Big) = 1 \tag{7.5}$$

という関係式が成り立つ. (7.4) と (7.5) は $\prod(a+b\alpha)$ が高い確率で平方数となっていることを示している. そして実際に

$$\prod(a+b\alpha) = h(\alpha)^2 \quad h(x)\in\mathbb{Z}[x]$$

と平方数になっていれば, φ でうつして $x^2\equiv y^2 \pmod n$ という形の合同式を得ることができる.

ここで残る問題は, $\prod(a+b\alpha)$ の平方根 $h(\alpha)$ をどのように求めるかということである. そのための前処理としての次の補題を準備する.

補題 7.6. α を代数的整数としてその最小多項式を $f(x)$ とする. このとき $\mathbb{Q}(\alpha)$ の任意の代数的整数 θ に対して $f'(\alpha)\theta$ は $\mathbb{Z}[\alpha]$ の元である.

証明. $f(x)/(x-\alpha) = \theta_0+\theta_1 x+\cdots+\theta_{d-1}x^{d-1}$ $(\theta_i\in\mathbb{Z}[\alpha])$ とおく. また $\sigma_1,\cdots,\sigma_d$ を埋め込みとし, $\sigma_i\alpha=\alpha_i$ とおく. さらに $\mathbb{Q}(\alpha)$ の任意の代数的整数 θ に対して $\sigma_i\theta=\theta^{(i)}$ とおく. このとき $f(x)=(x-\alpha_1)\cdots(x-\alpha_d)$ だから,

$$\frac{f(x)}{x-\alpha_i} = \theta_0^{(i)}+\theta_1^{(i)}x+\cdots+\theta_{d-1}^{(i)}x^{d-1}$$

と

$$f'(\alpha_i) = \prod_{j\neq i}(\alpha_i-\alpha_j) = \theta_0^{(i)}+\theta_1^{(i)}\alpha_i+\cdots+\theta_{d-1}^{(i)}\alpha_i^{d-1}$$

が従う. また $k=0,1,\cdots,d-1$ に対して

$$\sum_{i=1}^{d}\Big(\frac{\theta_0^{(i)}+\theta_1^{(i)}x+\cdots+\theta_{d-1}^{(i)}x^{d-1}}{f'(\alpha_i)}\alpha_i^k\Big) = x^k$$

が成り立つ. このことは上の式の両辺が高々$n-1$次の多項式であり, 異なるn個の値$x=\alpha_1,\alpha_2,\cdots,\alpha_n$に対して成り立つことから従う. 係数を比較すると

$$\sum_{i=1}^{d}\Big(\frac{\theta_j^{(i)}}{f'(\alpha_i)}\alpha_i^k\Big)=\begin{cases}0 & (j\neq k),\\ 1 & (j=k)\end{cases}$$

が言える. 言い換えると

$$T\Big(\alpha^k\frac{\theta_j}{f'(\alpha)}\Big)=\delta_{jk}$$

となり, $\{\theta_0/f'(\alpha),\theta_1/f'(\alpha),\cdots,\theta_{d-1}/f'(\alpha)\}$は$\mathbb{Q}(\alpha)$の$\mathbb{Q}$上の基底となる.

θに対してある有理数$s_0,s_1,\cdots,s_{d-1}$があって

$$\theta=\sum_{j=0}^{d-1}s_j\theta_j/f'(\alpha)$$

と書ける. また$T(\theta\alpha^k)=s_k$ $(k=0,1,\cdots,d-1)$だから, $s_k\in\mathbb{Z}$. したがって

$$f'(\alpha)\theta=\sum_{j=0}^{d-1}s_j\theta_j\in\mathbb{Z}[\alpha]$$

が成り立つ. □

したがって, 平方根を求めたい数に$f'(\alpha)^2$をかけておけば, その平方根は必ず$\mathbb{Z}[\alpha]$で求めることができる. そこで$\gamma=f'(\alpha)^2\prod(a+b\alpha)$とおいて, 以下では$\gamma$の平方根を求める方法について述べる.

奇素数pを$f(x)\bmod p$が$\mathbb{F}_p[x]$で既約になるものとして1つ固定する. さらにpはαを割らないものとする. また, fの次数をdとする. まず,

$$\delta_0^2\gamma\equiv 1\ (\mathrm{mod}\ p)$$

を満たす$\mathbb{Z}_p[\alpha]$の元δ_0を求める. δ_0はγの法pでの平方根の逆数である. 逆数にしたのは, 下の(7.7)において逆数の計算を避けるためである. そして

$$\delta_j\equiv\frac{\delta_{j-1}(3-\delta_{j-1}^2\gamma)}{2}\ (\mathrm{mod}\ n^{2^j}) \tag{7.7}$$

とおくと,

$$\delta_j^2\gamma\equiv 1\ (\mathrm{mod}\ p^{2^j})$$

を満たすδ_j $(j=1,2,\cdots)$がδ_1から順番にみつかる. これをp^{2^k}が十分大きくなるまで求めていくと,

$$\delta_k^2\gamma\equiv 1\ (\mathrm{mod}\ p^{2^k})$$

より

$$(\delta_k\gamma)^2 \equiv \gamma \pmod{p^{2^k}}$$

となり, $\delta_k\gamma$ の係数の絶対値を p^{2^k} より小さくとったものが求めたい γ の平方根となる. p^{2^k} の大きさについては, $2\sqrt{\max|a_i|}$ (a_i は α の係数) より大きくなるまで求めれば十分であるが, 実際に何乗でいいかははっきりとは分からないので平方根が求まるかどうかを試しながら進めていくのが最善である.

次に δ_0 について述べる. 素数 p の仮定から $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ は $\mathbb{F}_p[x]/(f \bmod p)$ と同型な濃度 p^d の体である. したがって, イデアル $P = p\mathbb{Z}[\alpha]$ は $\mathbb{Z}[\alpha]$ の次数 d の素イデアルである. $f \bmod p$ は既約であるから $f'(\alpha) \notin P$ が従う. また, γ の積の中に現れる $a + b\alpha$ に対して $\gcd(a, b) = 1$ であるから $a + b\alpha \notin P$ である. よってこれらの積である γ に対しても $\gamma \notin P$ がいえる. よって, γ の p をほうとした係数を求め, さらに有限体 $\mathbb{Z}[\alpha]/P$ の平方根を求めるアルゴリズム ([4] の Section 4.6.2, Exercise 15 と [8] の pp.169–198 を参照) を適用することで δ_0 を求めることができる.

8　$\mathbb{Z}[\alpha]$ が整数環ではない場合

これまでは $O_K = \mathbb{Z}[\alpha]$ を仮定してきたが, 本節ではこれが成り立たない場合について述べる. この場合には指数を割り切る素数についての考察が必要になるが, その詳細は [2] の Chapter6 を参照することにして, 以下では準同型 φ を O_K から $\mathbb{Z}/n\mathbb{Z}$ への写像に拡張する方法と, 補題 2.3 の拡張について述べる. また, 代数体の整数環を求めるアルゴリズムについては [1] の Section7.2 を参照すること.

まず, φ を拡張する. $l = [O_K : \mathbb{Z}[\alpha]]$ を O_K における $\mathbb{Z}[\alpha]$ の指数とする. $\gcd(l, n) = 1$ と仮定できる. そうでなければ n の非自明な因数が見つかる. よって, l は n を法として可逆であるから, l の n を法とする逆元を u $(\in \mathbb{Z})$ とおく. このとき, O_K の任意の元 γ に対して $l\gamma \in \mathbb{Z}[\alpha]$ であることに注意して,

$$\tilde{\varphi}(\gamma) = u\varphi(l\gamma)$$

とおくと, $\tilde{\varphi}$ は O_K から $\mathbb{Z}/n\mathbb{Z}$ への準同型となる.

次に補題 2.3 の拡張を与える.

補題 8.1. $a, b \in \mathbb{Z},\ \gcd(a, b) = 1$ とする. このとき $a + b\alpha,$ または $l = [O_K : \mathbb{Z}[\alpha]]$ を含む素イデアル P のノルムは素数である.

証明. p を P の下の素数とする. もし $p|b$ であれば $a \in P \cap \mathbb{Z}$ であるから $p|a$ となり, $\gcd(a, b) = 1$ に矛盾する. よって, $p \nmid b$ である. 次に $p \nmid l$ と仮定し, b^{-1} と u をそれぞれ b と l の p を法とした逆元とする. このとき, $\alpha \equiv -ab^{-1} \pmod{P}$ だから, $\gamma \in O_K$ に対して $l\gamma \in \mathbb{Z}[\alpha]$ が成り立つ. したがって, 整数係数多項式 F で, $\gamma \equiv uF(-ab^{-1}) \pmod{P}$ となるものが存在する. よって, O_K の任意の元は P を法として有理整数と合同である. つまり, P を法として $\{0, 1, \cdots, p-1\}$ の元と合同である. □

9 具体例

$n = 2117,\ m = 46,\ f(x) = x^2 + 1,\ \alpha = \sqrt{-1}$ を例として実際の計算を見る. この場合, $O_K = \mathbb{Z}[\alpha]$ であり, $\mathbb{Z}[\alpha]$ は UFD である.

まず, 素因数の大きさの上限 B を $B = 17$ ととる. よって, 素数の集合 F は

$$F = \{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17\}$$

である.

$\mathbb{Z}[\sqrt{-1}]$ の素イデアルを求めるために, $p \in F$ に対して $f(x)$ の $\bmod p$ での一次因子を求めると次のようになる.

$$f(x) \equiv \begin{cases} (x-1)^2 \pmod 2, \\ x^2+1 \pmod 3, \\ (x-2)(x-3) \pmod 5, \\ x^2+1 \pmod 7, \\ x^2+1 \pmod{11}, \\ (x-5)(x-8) \pmod{13}, \\ (x-4)(x-13) \pmod{17} \end{cases}$$

よって, 一次因子に対応する素イデアルは

$$(2, \alpha-1),\ (5, \alpha-2),\ (5, \alpha-3),\ (13, \alpha-8),\ (13, \alpha-5),\ (17, \alpha-4),\ (17, \alpha-13)$$

である.

次に素イデアルの生成元を求める. $(5, \alpha-2)$ を例にとる. このイデアルの生成元のノルムは 5 だから, $1+2\sqrt{-1}$ と $2+\sqrt{-1}$ が候補となる (単数倍は除く). 今 $(p, c) = (5, 2)$ だから, $a + bc \bmod p$ を計算すると,

$$\begin{cases} 1+2\sqrt{-1}\text{の場合} \cdots 1 + 2 \cdot 2 = 5 \equiv 0 \pmod 5, \\ 2+\sqrt{-1}\text{の場合} \cdots 2 + 1 \cdot 2 = 4 \not\equiv 0 \pmod 5 \end{cases}$$

となり, $1+2\sqrt{-1}$ が $(5, \alpha-2)$ の生成元であることがわかる. 同様にほかのイデアルの生成元を求めると,

$$\pi_1 = (1+\sqrt{-1}),\ \pi_2 = (1+2\sqrt{-1}),\ \pi_3 = (2+\sqrt{-1}),\ \pi_4 = (2+3\sqrt{-1}),$$
$$\pi_5 = (3+2\sqrt{-1}),\ \pi_6 = (1+4\sqrt{-1}),\ \pi_7 = (4+\sqrt{-1})$$

となる (ただし順番は素イデアルの順番に一致している). また単数はノルムが 1 であるから

$$u_1 = -1,\ u_2 = \sqrt{-1}$$

である.

そこで, $a + bm$ と $a + b\alpha$ がともに B-smooth なものを集めると,

	a	b	2	3	5	7	11	13	17	π_1	π_2	π_3	π_4	π_5	π_6	π_7	u_1	u_2
v_1	1	5		1		1	1			1				1				
v_2	-1	1		2	1					1								1
v_3	-1	2				1		1				1						1
v_4	2	1	4	1								1						
v_5	2	3	2		1	1							1					
v_6	-2	1	2				1				1							1
v_7	-2	3	3						1					1				1
v_8	3	1				2				1	1						1	1
v_9	3	4					1		1			2						
v_{10}	4	1	1		2											1		
v_{11}	-4	1	1	1		1									1			1
v_{12}	5	1		1					1	1			1				1	1
v_{13}	5	3					1	1		1					1		1	1
v_{14}	-7	1		1				1		1	2							
v_{15}	8	1	1	3							1			1			1	1
v_{16}	-11	2		4								3						1

という 16 個の分解を得る. これは例えば v_1 は,

$$\begin{cases} 1+5m = 3\cdot 7\cdot 11, \\ 1+5\sqrt{-1} = \pi_1\cdot\pi_5 = (1+\sqrt{-1})(3+2\sqrt{-1}) \end{cases}$$

と分解されることを表している.

$1+5\sqrt{-1}$ の生成元での分解の例も述べておく. $N(1+5\sqrt{-1}) = 26$ であるから, $1+5\sqrt{-1}$ は π_1 と, π_4 もしくは π_5 で割れることがわかる. いま $(a,b) = (1,5)$ だから, $a+bc \bmod p$ を計算すると,

$$\begin{cases} \pi_4\text{の場合}\cdots 1+5\cdot 8 = 41 \not\equiv 0 \pmod{13}, \\ \pi_5\text{の場合}\cdots 1+5\cdot 5 = 26 \equiv 0 \pmod{13} \end{cases}$$

となり, π_5 で割れることがわかる.

上の分解の表のうち次の 9 個の合同式

$$\begin{aligned}
v_2 &: \ 3^2 \cdot 5 \equiv 47 \cdot 46 \\
v_3 &: \ 7 \cdot 13 \equiv 48 \cdot 46 \\
v_5 &: \ 2^2 \cdot 5 \cdot 7 \equiv 140 \\
v_6 &: \ 2^2 \cdot 11 \equiv 93 \cdot 46 \\
v_8 &: \ 7^2 \equiv -1 \cdot 47 \cdot 93 \cdot 46 \\
v_9 &: \ 11 \cdot 17 \equiv 48^2 \\
v_{12} &: \ 3 \cdot 17 \equiv -1 \cdot 47 \cdot 140 \cdot 46 \\
v_{14} &: \ 3 \cdot 13 \equiv 47 \cdot 93^2 \\
v_{16} &: \ 3^4 \equiv 48^3 \cdot 46
\end{aligned}$$

をかけ合わせることにより,

$$(2^2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17)^2 \equiv (-47^2 \cdot 93^2 \cdot 48^3 \cdot 140 \cdot 46^3)^2 \pmod{2117}$$

という平方数の合同式を得る. これより,

$$\gcd(192972780 + 28792995928396922880,\ 2117) = 73$$

となり,

$$2117 = 73 \cdot 29$$

という素因数分解を得る.

参考文献

[1] J. Buchmann and HW Lenstra. Approximating rings of integers in number elds. *J. Theor. Nombres Bordx*, Vol. 2, pp. 221–260, 1994.

[2] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag, 1993.

[3] R.E. Crandall and C. Pomerance. *Prime numbers: a computational perspective*. Springer Verlag, 2005.

[4] D.E. Knuth. The art of computer programming: Seminumerical algorithms, volume 2, 1981.

[5] A. K. Lenstra and H. W. Lenstra, Jr. *The development of the number field sieve*. Lecture Notes in Mathematics, vol.1554. Springer-Verlag, Berlin, 1993.

[6] AK Lenstra, HW Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, Vol. 261, No. 4, pp. 515–534, 1982.

[7] AK Lenstra, HW Lenstra Jr, MS Manasse, and JM Pollard. The factorization of the ninth Fermat number. *Mathematics of Computation*, Vol. 61, No. 203, pp. 319–349, 1993.

[8] HW Lenstra and R. Tijdeman. *Computational methods in number theory*. Mathematisch Centrum, 1982.

[9] E. Weiss. *Algebraic number theory*. Dover Pubns, 1998.