Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Andrzej Chmielowiec
Nr albumu: 181080

Obliczeniowe aspekty problemu dzielników

Praca magisterska
na kierunku MATEMATYKA

Praca wykonana pod kierunkiem
dra hab. Jacka Pomykały

2 grudnia 2003

Pracę przedkładam do oceny

Data Podpis autora pracy:

Praca jest gotowa do oceny przez recenzenta

Data Podpis kierującego pracą:

Streszczenie

Niniejsza praca prezentuje strukturę grupy multiplikatywnej pierścienia skończonego, który jest pierścieniem ilorazowym pewnego pierścienia euklidesowego. Zaprezentowane tu podejście pozwala spojrzeć na problem faktoryzacji i testowania pierwszości z nieco ogólniejszej perspektywy. Okazuje się bowiem, że niektóre algorytmy faktoryzacji i testowania pierwszości mają swoje odpowiedniki w innych pierścieniach niż pierścień liczb całkowitych.

Słowa kluczowe

pierścień euklidesowy, grupa multiplikatywna, rozkład, czynnik, największy wspólny dzielnik, element pierwszy

Klasyfikacja tematyczna

13F07, 11A51, 11T04, 12E05

Spis treści

Wstęp

Współczesne algorytmy kryptograficzne wykorzystują założenie o złożoności obliczeniowej różnych problemów algebraicznych. Przykładem może tu być logarytm dyskretny w grupie multyplikatywnej ciała skończonego i faktoryzacja liczb całkowitych. Oczywiście problem trudny w jednej strukturze może okazać się prosty w innej. Doskonałym tego przykładem jest problem faktoryzacji. Dla pierścienia liczb całkowitych nie mamy do tej pory efektywnego algorytmu rozkładającego zadaną liczbę na czynniki, podczas gdy w pierścieniu wielomianów nad ciałem skończonym problem ten nie jest aż tak złożony. Oczywiście mówiąc o faktoryzacji nie sposób pominąć jej szczególnego przypadku, którym jest odpowieź na pytanie, czy dany element w ogóle jest złożony. Jest to powszechnie znany problem testowania pierwszości. Tematem niniejszej pracy jest właśnie jednoczesne spojrzenie na faktoryzację i testowanie pierwszości w wielu dziedzinach euklidesowych.

Rozdział 1

Podstawowe definicje i twierdzenia

Celem tej pracy jest badanie podzielności w pierścieniach euklidesowych. W związku z tym przez pierścień będziemy rozumieli pierścień euklidesowy, czyli pierścień przemienny z jedynką, w którym zadana jest norma definiowana następująco:

Definicja 1.1 Normą euklidesową w pierścieniu R nazywamy funkcję $\mathrm{N} : R \to \mathbb{Z}_+ \cup \{0\}$, spełniającą następujące warunki

(a) $\mathrm{N}(x) = 0 \Leftrightarrow x = 0$,

(b) $\forall_{a,b \in R} \quad \mathrm{N}(ab) = \mathrm{N}(a)\mathrm{N}(b)$,

(c) $\forall_{a \in R}\ \forall_{b \in R \setminus \{0\}}\ \exists_{q,r \in R} \quad a = qb + r, \quad 0 \leq \mathrm{N}(r) < \mathrm{N}(b)$.

□

Przykład 1.1 Przykładami pierścieni euklidesowych są

(a) pierścień liczb całkowitych $\mathbb{Z}$, w którym normą jest wartość bezwzględna liczby

$$\mathrm{N}(n) = |n|$$

(b) pierścień liczb całkowityuch Gaussa $\mathbb{Z}[i]$, w którym norma elementu $a + bi \in \mathbb{Z}[i]$ zdefiniowana jest jako

$$\mathrm{N}(a + bi) = a^2 + b^2$$

(c) pierścień wielomianów nad ciałem $K[X]$, gdzie normę elementu $f \in K[X]$ definiujemy jako

$$\mathrm{N}(f) = c^{\deg(f)}, \qquad \text{dla pewnego } c \in \mathbb{Z}, c > 1.$$

□

Przypomnę teraz kilka podstawowych definicji i twierdzeń związanych z pierścieniami euklidesowymi i teorią podzielności. Będą stanowiły one podstawę do moich dalszych rozważań.

Definicja 1.2 Powiemy, że element $a \in R$ dzieli $b \in R$ jeśli istnieje taki element $c \in R$, że

$$ac = b.$$

□

Definicja 1.3 Powiemy, że element p pierścienia R jest pierwszy, gdy zachodzi

$$p \mid ab \quad \Longleftrightarrow \quad p \mid a \text{ lub } p \mid b.$$

□

Definicja 1.4 Pierścień R jest dziedziną całkowitości, gdy z faktu, że $ab = 0$ wynika $a = 0$ lub $b = 0$. Powiemy, że R jest dziedziną ideałów głównych, gdy dla każdego ideału $I \subset R$ istnieje $a \in R$ taki, że $(a) = I$.

□

Definicja 1.5 Dziedzinę całkowitości R nazywamy dziedziną z jednoznacznością rozkładu, jeżeli

(a) każdy element rozkładalny jest iloczynem pewnej liczby elementów nierozkładalnych,

(b) przedstawienie elementu rozkładalnego w postaci elementów nierozkładalnych jest jednoznaczne z dokładnością do kolejności czynników i pomnożenia przez element odwracalny.

□

Definicja 1.6 Ideał właściwy I pierścienia R jest ideałem maksymalnym, jeżeli dla każdego ideału $J \neq I$ zachodzi

$$I \subset J \Rightarrow J = R.$$

□

Twierdzenie 1.1 Pierścień euklidesowy jest dziedziną ideałów głównych.

Dowód: Twierdzenie wystarczy udowodnić dla ideału właściwego, gdyż jeśli R jest danym pierścieniem euklidesowym, to $(1) = R$ i $(0) = 0$. Niech zatem $I \subset R$ będzie ideałem właściwym pierścienia R, a $b \in I \setminus \{0\}$ będzie takim elementem, że

$$\forall_{x \in I \setminus \{0\}} \quad \mathrm{N}(b) \leq \mathrm{N}(x).$$

Twierdzimy, że $(b) = I$. Załóżmy, że tak nie jest. Wtedy istnieje element $a \in I \setminus \{0\}$ taki, że $a \notin (b)$. Na mocy definicji normy euklidesowej możemy zatem zapisać

$$a = qb + r,$$

gdzie $0 < \mathrm{N}(r) < \mathrm{N}(b)$, gdyż $a \notin (b)$. Przeczy to założeniu, że b jest elementem minimalnym $I \setminus \{0\}$ w sensie normy. Pokazana sprzeczność dowodzi równości $(b) = I$.

■

Twierdzenie 1.2 Pierścień euklidesowy jest dziedziną całkowitości.

Dowód: Niech R będzie pierścieniem euklidesowym, a $a, b \in R$ spełniają równanie

$$ab = 0.$$

Wtedy $0 = \mathrm{N}(0) = \mathrm{N}(ab) = \mathrm{N}(a)\mathrm{N}(b)$. Oznacza to, że $\mathrm{N}(a) = 0$ lub $\mathrm{N}(b) = 0$ i na mocy własności normy euklidesowej dostajemy $a = 0$ lub $b = 0$.

■

Należy pamiętać, że w definicji 1.1 ani q, ani r nie są dane jednoznacznie. Jako przykład rozważmy pierścień liczb całkowitych $\mathbb{Z}$. Nie trudno zauważyć, że $5 = 1 \cdot 3 + 2 = 2 \cdot 3 + (-1)$. Pokażemy jednak, że element r nie może być zupełnie dowolny. Okazuje się bowiem, że jest on dany w sposób jednoznaczny z dokładnością do warstwy względem ideału generowanego przez b. Poniższe twierdzenie precyzuje tą obserwację.

Stwierdzenie 1.1 Jeśli R jest pierścieniem euklidesowym i $a = q_1 b + r_1 = q_2 b + r_2$, to $r_1 + (b) = r_2 + (b)$.

Dowód: Zauważmy, ze warstwy względem ideału (b) tworzą podział pierścienia R. W związku z tym element a należy do dokładnie jednej warstwy. Jeśli zatem $a = q_1 b + r_1 = q_2 b + r_2$, to $a \in r_1 + (b)$ i $a \in r_2 + (b)$, co oznacza, że $r_1 + (b) = r_2 + (b)$.

■

Powyższe stwierdzenie daje nam podstawę do przyjęcia następującej, jednoznacznej definicji reszty z dzielenia i ilorazu z dzielenia.

Definicja 1.7 Niech R będzie pierścieniem euklidesowym, a $(b) \subset R$ ideałem generowanym przez $b \neq 0$. Wykorzystując własności normy euklidesowej wybieramy zbiór reprezentantów $\mathcal{R} \subset R$ taki, że

(a) $\forall r \in \mathcal{R} \quad \mathrm{N}(r) < \mathrm{N}(b)$,

(b) $\bigcup_{r \in \mathcal{R}} r + (b) = R$,

(c) $\forall_{r_1, r_1 \in \mathcal{R}} \quad r_1 \neq r_2 \Rightarrow r_1 + (b) \neq r_2 + (b)$.

Wtedy przez resztę z dzielenia elementu a przez b rozumiemy taki element $r \in \mathcal{R}$, że

$$a = qb + r,$$

a związane z nim q nazywamy ilorazem z dzielenia. Resztę i iloraz oznaczamy odpowiednio przez $(a \mod b)$ i $(a \operatorname{div} b)$.

□

Przykład 1.2 (a) W przypadku pierścienia $\mathbb{Z}$ i elementu b jako reprezentację będziemy przyjmowali zbiór

$$\{0, 1, \ldots, |b| - 1\}.$$

(b) Dla pierścienia wielomianów $K[X]$ można natomiast przyjąć, że taką reprezentację stanowią wielomiany, które mają niższy stopień niż dzielnik.

□

Twierdzenie 1.3 Jeżeli R jest dziedziną całkowitości, to R jest dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy, gdy

(a) każdy element rozkładalny w R jest iloczynem elementów nierozkładalnych

(b) każdy element nierozkładalny jest pierwszy.

Dowód: J. Browkin [Bro77, str. 63].

■

Twierdzenie 1.4 Dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.

Dowód: J. Browkin [Bro77, str. 63].

■

Z tych dwóch twierdzeń płyną dość oczywiste, ale bardzo ważne dla dalszej analizy wnioski.

Wniosek 1.1 Pierścień euklidesowy jest dziedziną z jednoznacznością rozkładu.

■

Wniosek 1.2 Ideał pierścienia euklidesowego jest pierwszy wtedy i tylko wtedy, gdy jest maksymalny.

■

Wyżej przytoczone własności stanowią podstawę dalszych rozważań, których celem będzie opisanie grupy multiplikatywnej pierścienia ilorazowego.

Rozdział 2

Elementy ortogonalne w sensie NWD

Niech R będzie pierścieniem euklidesowym takim, że dla każdego $a \in R \setminus \{0\}$ mamy

$$|R/(a)| < \infty, \tag{2.1}$$

gdzie (a) oznacza ideał generowany przez element a. W dalszej części będą nas interesowały tylko takie pierścienie euklidesowe, dla których zachodzi (2.1).

Przykład 2.1 Rozważmy pierścień $K[X]$ wielomianów o współczynnikach z ciała K. Ponieważ $K[X]$ jest pierścieniem ideałów głównych, to każdy ideał generowany jest przez jakiś wielomian $f(X)$, a pierścień $K[X]/(f)$ ma strukturę przestrzeni liniowej wymiaru $\deg(f)$ nad K. Możemy zatem wyróżnić dwa przypadki

(a) $|K| < \infty$ i wtedy $K[X]$ spełnia warunek 2.1,

(b) $|K| = \infty$ i wtedy każdy pierścień ilorazowy jest nieskończony.

□

Definicja 2.1 Przez największy wspólny dzielnik elementów $a, b \in R$ rozumiemy taki element $d \in R$, że $d \mid a, d \mid b$ oraz

$$\forall_{r \in R} \quad r \mid a \text{ i } r \mid b \Rightarrow \mathrm{N}(r) \leq \mathrm{N}(d).$$

Największy wspólny dzielnik oznaczamy przez (a, b). Jeśli $(a, b) = 1$, to mówimy, że elementy są względnie pierwsze.

□

Definicja 2.2 Oznaczmy przez R_a zbiór reszt z dzielenia przez element a

$$R_a = \{b \mod a : \ b \in R\},$$

niech $R_a^{\perp}$ oznacza zbiór R_a obcięty do elementów względnie pierwszych z a, czyli

$$R_a^{\perp} = \{b \in R_a : \ (a, b) = 1\}.$$

□

Jednoznaczność określenia reszty z dzielenia zapewnia, że funkcja $\mod a$ jest identycznością na R_a.

Naszym celem będzie teraz analiza przestrzeni $R_a^\perp$. Postaramy się na jej podstawie powiedzieć coś na temat rozkładu elementu a na czynniki. Zacznijmy od utożsamienia zbioru R_a z pierścieniem $R/(a)$.

Stwierdzenie 2.1 Funkcja $\imath : R_a \to R/(a)$ zdefiniowana jako

$$\imath(x) = x + (a),$$

$$\imath^{-1}(x + (a)) = (x \mod a)$$

jest bijekcją.

Dowód: Ze względu na skończoność R_a i $R/(a)$ wystarczy wykazać, że zarówno $\imath$ jak i $\imath^{-1}$ są "na". Ponieważ R_a jest niczym innym jak zbiorem reprezentantów R, to z punktu (b) definicji 1.7 mamy, że $\imath$ jest "na". W przypadku $\imath^{-1}$ wiemy, że jeśli $x \in R_a \subset R$, to $(x \mod a) = x$, co daje

$$\imath^{-1}(x + (a)) = (x \mod a) = x$$

i kończy dowód.

■

Stwierdzenie 2.2 $\imath(R_a^\perp)$ jest grupą multiplikatywną pierścienia $R/(a)$, czyli

$$\imath(R_a^\perp) = R/(a)^*.$$

Dowód: Pokażemy najpierw, że obraz każdego elementu z $R_a^\perp$ jest elementem odwracalnym w $R/(a)$. Niech zatem $x \in R_a^\perp$. Wtedy na mocy odwrotnego algorytmu Euklidesa [Coh96, str. 12, 315] istnieją takie elementy $b, y \in R$, że

$$ab + xy = 1,$$

co oznacza, że $(x + (a))(y + (a)) = xy + (a) = 1 + (a)$ i pokazuje, że $\imath(x) \in R/(a)^*$. Aby pokazać zawieranie w drugą stronę załóżmy, że $x + (a)$ jest elementm odwracalnym, a $y + (a)$ jest jego odwrotnością. Wtedy $(1 - xy) \in (a)$, co oznacza, że istnieje $b \in R$, dla którego $1 - xy = ab$. Teraz zauważmy, że $x = (x \operatorname{div} a)a + (x \mod a)$, co daje

$$1 = ab + xy = a(b + (x \operatorname{div} a)y) + (x \mod a)y,$$

Stąd na podstawie algorytmu Euklidesa mamy, że $((x \mod a), a) = 1$ i $\imath^{-1}(x) \in R_a^\perp$.

■

Udowodnione powyżej stwierdzenia pozwalają na utoższamianie zbiorów R_a i $R/(a)$ oraz $R_a^\perp$ i $R/(a)^*$. W związku z tym w dalszej części nie będziemy ich specjalnie rozróżniać. Oznacza to, że jeśli zaistnieje taka potrzeba, to zbiór R_a będziemy traktowali jako pierścień $R/(a)$, a zbiór $R_a^\perp$ jako grupę $R/(a)$.

2.1. Twierdzenia umożliwiające rozkład $R_a^\perp$

Skoro wiemy już, że nasza przestrzeń ma algebraiczną strukturę skończonej grupy abelowej, to warto zastosować do niej twierdzenie o skończenie generowanych grupach abelowych, którego zredukowaną do naszych potrzeb treść, przypominam poniżej.

Definicja 2.3 Niech G będzie grupą skończoną, a p ustaloną liczbą pierwszą taką, że

$$|G| = p^k m, \quad p \nmid m.$$

Powiemy, że $H \lhd G$ jest p-podgrupą Sylowa w G, jeśli

$$|H| = p^k.$$

□

Twierdzenie 2.1 Niech G będzie skończoną grupą abelową. Wtedy mamy

$$G \simeq P_1 \oplus \cdots \oplus P_r,$$

gdzie P_i jest p_i-podgrupą Sylowa w G oraz dla każdego i zachodzi

$$P_i \simeq \mathbb{Z}_{p_i^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{r_s}}.$$

Dowód: J. Rotman [Rot95].

■

Jak można zauważyć powyższe twierdzenie daje pewien obraz struktury grupy abelowej i jej rozkładu na iloczyn prosty p-podgrup Sylowa. Niewiele jednak mówi o strukturze samych podgrup Sylowa. Aby więc mieć pełen obraz przestrzeni $R_a^{\perp}$ musimy powiedzieć coś o strukturze samych podgrup Sylowa. Ponieważ R jest pierścieniem euklidesowym, to wykorzystamy w tym celu twierdzenie chińskie o resztach.

Twierdzenie 2.2 (chińskie o resztach) Niech $a, b_1, b_2 \in R$ takie, że $a = b_1 b_2$ i $(b_1, b_2) = 1$. Wtedy zachodzi

$$R_a \simeq R_{b_1} \oplus R_{b_2}.$$

Dowód: Rozważmy homomorfizm $h : R_a \to R_{b_1} \oplus R_{b_2}$, który ma postać

$$h(x) = (x \mod b_1,\ x \mod b_2).$$

Aby pokazać, że h jest izomorfizmem wystarczy udowodnić, że układ równań

$$\begin{cases} x \equiv c \mod b_1 \\ x \equiv c \mod b_2 \end{cases}$$

ma jednoznaczne rozwiązanie modulo a. Zauważmy, że skoro $(b_1, b_2) = 1$, to na mocy odwrotnego algorytmu Euklidesa [Coh96, str. 12, 315] istnieją elementy $b_1^{-1} \mod b_2$ i $b_2^{-1} \mod b_1$ takie, że

$$\begin{aligned} b_2 b_2^{-1} &\equiv 1 \mod b_1 \\ b_1 b_1^{-1} &\equiv 1 \mod b_2. \end{aligned}$$

W związku z powyższym łatwo można sprawdzić, że element

$$x = (c \mod b_1)(b_2^{-1} \mod b_1)b_2 + (c \mod b_2)(b_1^{-1} \mod b_2)b_1$$

jest rozwiązaniem naszego układu równań. W celu wykazania jednoznaczności załóżmy, że x i x' spełniają zadany układ. Wtedy

$$\begin{cases} x \equiv x' \mod b_1 \\ x \equiv x' \mod b_2 \end{cases},$$

$$\begin{cases} x - x' = m_1 b_1 \\ x - x' = m_2 b_2 \end{cases}.$$

Z rozszerzonego algorytmu Euklidesa wiemy, że istnieją takie elementy $n_1, n_2 \in R$, że

$$n_1 b_1 + n_2 b_2 = 1.$$

Mnożąc teraz równania odpowiednio przez $n_2 b_2$ i $n_1 b_1$ otrzymujemy

$$\begin{cases} (x - x')n_2 b_2 = m_1 b_1 n_2 b_2 \\ (x - x')n_1 b_1 = m_2 b_2 n_1 b_1 \end{cases},$$

co po dodaniu równań stronami daje

$$(x - x')(n_1 b_1 + n_2 b_2) = b_1 b_2 (m_1 n_2 + m_2 n_1),$$

$$x - x' \equiv 0 \mod b_1 b_2,$$

$$x \equiv x' \mod a,$$

to kończy dowód.

■

Wniosek 2.1 Niech $a, b_1, \ldots, b_k \in R$ takie, że $a = b_1 \ldots b_k$ i $(b_i, b_j) = 1$ dla dowolnego $i \neq j$. Wtedy

$$R_a \simeq R_{b_1} \oplus \cdots \oplus R_{b_k},$$

co w szczególności daje nam izomorfizm odpowiednich grup multiplikatywnych, czyli

$$R_a^{\perp} \simeq R_{b_1}^{\perp} \oplus \cdots \oplus R_{b_k}^{\perp}.$$

■

Wniosek 2.2 Jeśli

$$a = \prod_{i=1}^{n} p_i^{\alpha_i}$$

jest rozkładem elementu a na czynniki pierwsze, to

$$\begin{aligned} R_a &\simeq R_{p_1^{\alpha_1}} \oplus \cdots \oplus R_{p_n^{\alpha_n}} \\ R_a^{\perp} &\simeq R_{p_1^{\alpha_1}}^{\perp} \oplus \cdots \oplus R_{p_n^{\alpha_n}}^{\perp}. \end{aligned}$$

■

Przykład 2.2 Pokażemy, że funkcja ϕ Eulera [Kob95, str. 29] jest multiplikatywna. Niech $R = \mathbb{Z}$ i niech $a \in R$ takie, że

$$a = bc, \quad (b, c) = 1.$$

Wtedy z wniosku 2.1 mamy

$$\mathbb{Z}_a^\perp \simeq \mathbb{Z}_b^\perp \oplus \mathbb{Z}_c^\perp,$$

a ponieważ

$$|\mathbb{Z}_a^\perp| = |\{x \in \mathbb{Z}_+ \cup \{0\} : (x, a) = 1,\ x < a\}| = \phi(a),$$

to

$$\phi(a) = \phi(b)\phi(c).$$

□

Jak się niedługo okaże, te dwa twierdzenia, czyli twierdzenie o skończeniegenerowanych grupach abelowych i twierdzenie chińskie o resztach, są wystarczające z naszego punktu widzenia do opisu przestrzeni $R_a^\perp$.

Rozdział 3

Rozkład $R_a^{\perp}$

Definicja 3.1 Jeśli R jest ustalonym pierścieniem euklidesowym, to $a^{\perp}$ definiujemy jako

$$a^{\perp} = |R_a^{\perp}|.$$

□

W dalszej części będą nas interesowały dość szczególne rodzaje rozkładów na składniki proste.

Definicja 3.2 Jeśli $p \in R$ jest elementem pierwszym, to grupa $R_{p^\alpha}^{\perp}$ jest rozkładalna względem liczby pierwszej q, jeśli dla pewnej nieujemnej liczby całkowitej β zachodzi

$$R_{p^\alpha}^{\perp} \simeq \mathbb{Z}_{q^\beta} \oplus G \quad \text{i} \quad q \nmid |G|.$$

Jeśli natomiast $a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \in R$, to grupa $R_a^{\perp}$ jest rozkładalna względem q jeśli każda z grup $R_{p_i^{\alpha_i}}^{\perp}$ jest rozkładalna względem q. W przypadku gdy wspomniane grupy są rozkładalne względem wszystkich liczb pierwszych, mówimy, że są rozkładalne.

□

Twierdzenie 3.1 Jeżeli p jest elementem pierwszym pierścienia euklidesowego R, to pierścień ilorazowy R_p jest ciałem skończonym.

Dowód: Ponieważ $(p) = \{ap : a \in R\}$, to dla $bc \in (p)$ i dla pewnego $d \in R$ mamy

$$bc = dp.$$

Ale p jest elementem pierwszym, więc $p \mid b$ lub $p \mid c$, skąd wynika, że

$$b \in (p) \quad \text{lub} \quad c \in (p).$$

Zatem (p) jest ideałem pierwszym, co w połączeniu z wnioskiem 1.2 daje nam, że (p) jest maksymalny. To kończy dowód, gdyż pierścień ilorazowy ideału maksymalnego jest ciałem, a skończoność wynika z warunków nałożonych na R (to jest $|R_p| < \infty$).

■

Wniosek 3.1 Jeżeli $p \in R$ jest elementem pierwszym, to $R_p^{\perp}$ jest cykliczna.

Dowód: Z poprzedniego twierdzenia wiemy, że dla p pierwszego pierścień R_p jest ciałem skończonym . Stwierdzenie 2.2 mówi nam natomiast, że $R_p^\perp$ jest grupą multiplikatywną R_p, a grupa multiplikatywna ciała skończonego jest cykliczna.

■

Załóżmy, że a jest elementem bezkwadratowym i

$$a^\perp = \prod_{j=1}^{s} q_j^{\beta_j}$$

jest rozkładem $a^\perp$ na czynniki pierwsze. Ponieważ $a^\perp = p_1^\perp \dots p_r^\perp$, to możemy przyjąć

$$p_i^\perp = \prod_{j=1}^{s} q_j^{\beta_{i,j}}.$$

Przy takich oznaczeniach sformułujemy twierdzenie, które da nam dokładny opis rozkładu przestrzeni $R_a^\perp$ dla a bezkwadratowego.

Twierdzenie 3.2 (o rozkładzie $R_a^\perp$) Jeżeli $a \in R$ jest elementem bezkwadratowym, to $R_a^\perp$ jest rozkładalna.

Dowód: Skoro a jest elementem bezkwadratowym, to

$$R_a^\perp \simeq R_{p_1}^\perp \oplus \dots \oplus R_{p_r}^\perp,$$

gdzie

$$R_{p_i}^\perp \simeq \mathbb{Z}_{q_1^{\beta_{i,1}}} \oplus \dots \oplus \mathbb{Z}_{q_s^{\beta_{i,s}}}.$$

Przy czym ostatni izomorfizm wynika bezpośrednio z z twierdzenia 2.1 (o skończenie generowanych grupach abelowych) i wniosku 3.1 (o cykliczności każdej z grup $R_{p_j}^\perp$). Niech teraz q będzie dowolną liczbą pierwszą. Jeśli $q \mid (p_i^{\alpha_i})^\perp$, to q jest równe pewnemu q_j, a grupa $R_{p_i}^\perp$ jest rozkładalna względem q_j, gdyż liczby $q_1, \dots q_s$ są parami różne. Jeśli natomiast $q \nmid (p_i^{\alpha_i})^\perp$, to

$$R_{p_i}^\perp \simeq \mathbb{Z}_{q^0} \oplus R_{p_i}^\perp,$$

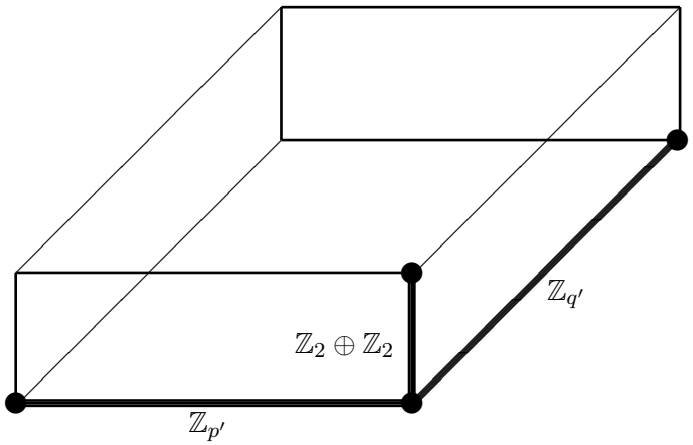
co kończy dowód.

■

Powodem prawdziwości twierdzenia o rozkładzie jedynie dla elementów bezkwadratowych jest fakt, że w ogólności grupa $R_{p^\alpha}^\perp$ nie musi być cykliczna. Jest tak na przykład w pierścieniu liczb całkowitych, w którym dla $n > 2$ mamy

$$\mathbb{Z}_{2^n}^* \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}.$$

Tym niemniej można uogólnić powyższe twierdzenie w przypadku gdy $R_{p^\alpha}^\perp$ jest cykliczna.



Rysunek 3.1: Rozkład przestrzeni $\mathbb{Z}_n^\perp$

Wniosek 3.2 Jeśli $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ i dla każdego $p_i^{\alpha_i}$ grupa $R^\perp_{p_i^{\alpha_i}}$ jest cykliczna to $R_a^\perp$ jest rozkładalna i mamy

$$R_a^\perp \simeq R^\perp_{p_1^{\alpha_1}} \oplus \cdots \oplus R^\perp_{p_r^{\alpha_r}},$$

gdzie

$$R^\perp_{p_i^{\alpha_i}} \simeq \mathbb{Z}_{q_1^{\beta_{i,1}}} \oplus \cdots \oplus \mathbb{Z}_{q_s^{\beta_{i,s}}}, \qquad (p_i^{\alpha_i})^\perp = \prod_{j=1}^{s} q_j^{\beta_{i,j}}.$$

■

Wprowadzone twierdzenia zilustrujemy teraz na przykładach pierścienia liczb całkowitych i pierścienia wielomianów nad ciałem skończonym. Powinny one dać pewną intuicję co do wyglądu $R_a^\perp$.

Przykład 3.1 Niech $n \in \mathbb{Z}$ takie, że $n = pq$, gdzie

$$\begin{aligned} p &= 2p' + 1, \\ q &= 2q' + 1, \end{aligned}$$

dla pewnych liczb pierwszych p, q, p', q'. Przy takich założeniach mamy

$$n^\perp = (p-1)(q-1) = 2 \cdot 2 \cdot p' \cdot q'.$$

W związku z tym z twierdzenia (3.2) dostajemy

$$\mathbb{Z}_n^\perp \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{p'} \oplus \mathbb{Z}_{q'},$$

co ilustruje rysunek 3.1. Z punktu widzenia problemu faktoryzacji najistotniejszą podgrupą tego rozkładu jest jej niecykliczny składnik $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Okaże się w kolejnych częściach, że niektóre jego elementy można wykorzystać do rozkładu n na czynniki.

□

Przykład 3.2 Rozważmy ciało $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha+1\}$, gdzie $\alpha^2 = \alpha + 1$ oraz pierścień wielomianów $R = \mathbb{F}_{2^2}[X]$. Nietrudno zauważyć, że wielomian $f = X^2 + X + 1 \in R$ jest iloczynem dwóch różnych wielomianów stopnia 1, a dokładniej

$$f = g \cdot h = (X + \alpha)(X + \alpha + 1).$$

Mając takie dane możemy wypisać elementy R_f i $R_f^\perp$.

$$\begin{array}{lllll} R_f = \{0, & 1, & X, & X+1, & X+\alpha, & X+\alpha+1, \\ & \alpha, & \alpha X, & \alpha X+1, & \alpha X+\alpha, & \alpha X+\alpha+1, \\ & \alpha+1, & (\alpha+1)X, & (\alpha+1)X+1, & (\alpha+1)X+\alpha, & (\alpha+1)X+\alpha+1 \quad \}. \end{array}$$

Jeśli teraz wyeliminujemy z R_f wielokrotności g i h, którymi są

$$\begin{aligned} g \cdot \mathbb{F}_{2^2} &= \{0, X+\alpha, \alpha X+\alpha+1, (\alpha+1)X+1\}, \\ f \cdot \mathbb{F}_{2^2} &= \{0, X+\alpha+1, \alpha X+1, (\alpha+1)X+\alpha\}, \end{aligned}$$

to otrzymamy $R_f^\perp$.

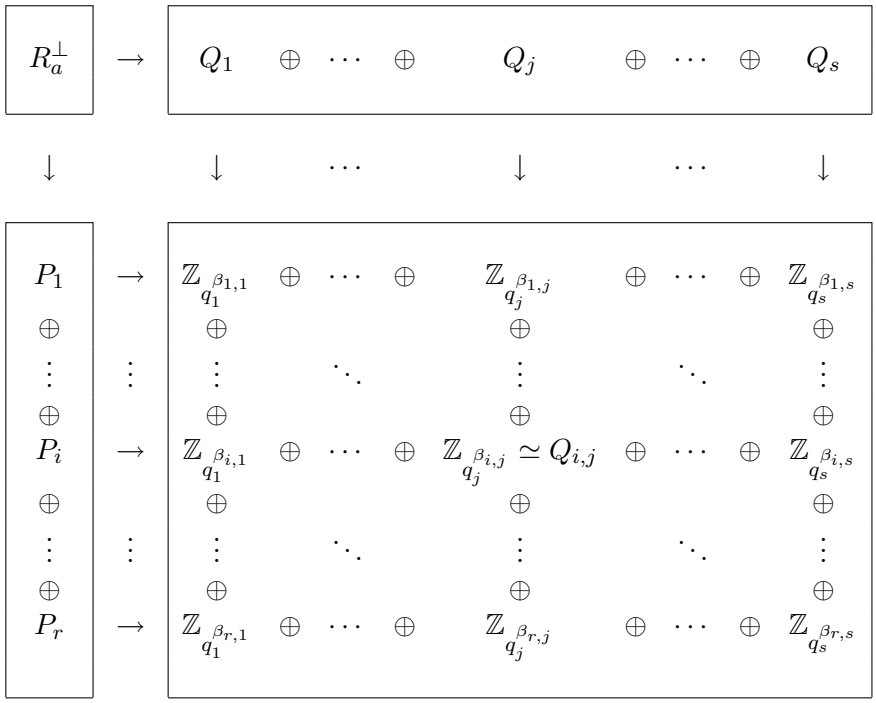
$$\begin{array}{lll} R_f^\perp = \{ & 1, & X, & X+1, \\ & \alpha, & \alpha X, & \alpha X+\alpha, \\ & \alpha+1, & (\alpha+1)X, & (\alpha+1)X+\alpha+1 \quad \}. \end{array}$$

Z drugiej strony, wykorzystując nasze dotychczasowe obserwacje możemy zapisać, że $|R_f^\perp| = f^\perp = g^\perp h^\perp = (2^2-1)(2^2-1) = 9$, co jest zgodne z rzeczywistością. Ponadto grupa $R_f^\perp$ jest izomorficzna z sumą prostą $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, co jest również łatwe do weryfikacji, gdyż wszystkie elementy $R_f^\perp$ są w trzeciej potędze jedynkami.

Dotychczasowe spostrzeżenia można nieco uogólnić. Zauważmy bowiem, że dowolny wielomian $f \in \mathbb{F}_2[X]$ stopnia n rozkłada się w pierścieniu $R = \mathbb{F}_{2^n}[X]$ na iloczyn czynników pierwszego stopnia. W związku z tym

$$R_f^\perp \simeq \bigoplus_{i=1}^{n} \mathbb{Z}_{2^n-1}.$$

□



Rysunek 3.2: Całkowity rozkład przestrzeni $R_a^\perp$

Teraz, gdy już wiemy jaka jest struktura grupy $R_a^\perp$, wprowadzimy nowe oznaczenia, które pozwolą nam na łatwiejsze operowanie wprowadzoną teorią i uproszczą zapis. Przyjmijmy zatem, że $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, grupa $R_{p_i^{\alpha_i}}^\perp$ jest cykliczna oraz

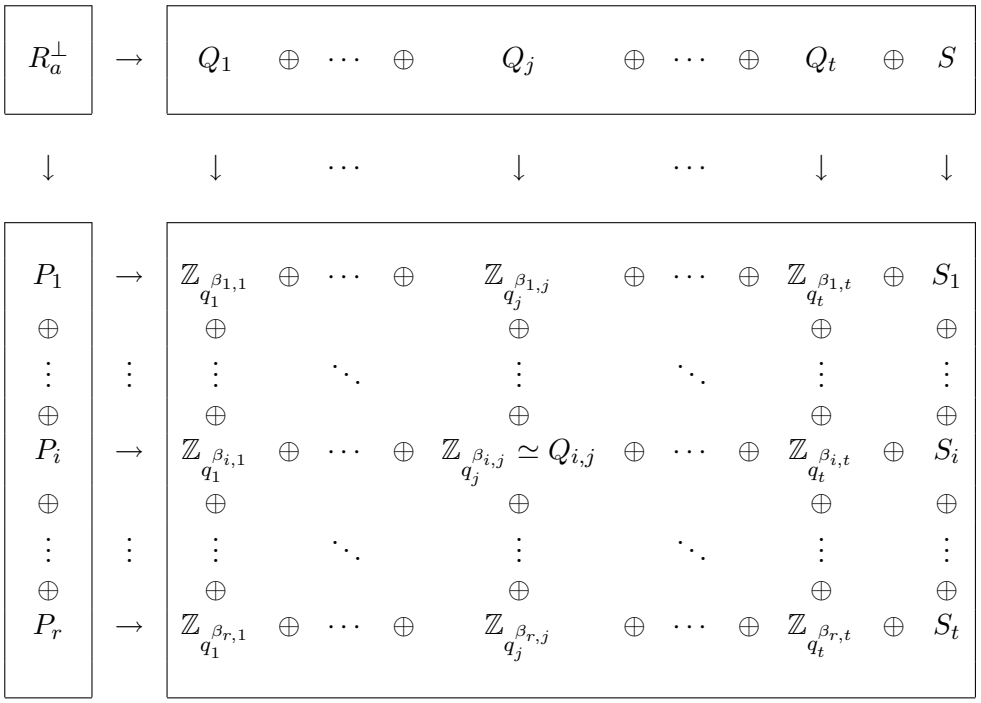
$$a^\perp = \prod_{j=1}^{s} q_j^{\beta_j}, \qquad p_i^\perp = \prod_{j=1}^{s} q_j^{\beta_{i,j}}.$$

Wprowadzamy następujące oznaczenia

$$P_i \simeq \bigoplus_{j=1}^{s} \mathbb{Z}_{q_j^{\beta_{i,j}}}, \qquad Q_j \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{q_j^{\beta_{i,j}}}, \qquad Q_{i,j} \simeq \mathbb{Z}_{q_j^{\beta_{i,j}}}.$$

Można zauważyć, że zbiór elementów P_i jest tym, który otrzymujemy po zastosowaniu do $R_a^\perp$ twierdzenia chińskiego o resztach i jest to po prostu $R_{p_i^{\alpha_i}}^\perp$. Zbiory Q_j są efektem zastosowania twierdzenia o skończenie generowanych grupach abelowych. W związku z tym, jeśli będziemy chcieli podkreślić z jakim konkretnie czynnikiem jest związane Q_j, to będziemy je oznaczać przez Q_{q_j}. Dopełnienie Q_j będziemy oznaczali przez H_j, oznacza to, że $R_a^\perp \simeq Q_j \oplus H_j$. Grupy $Q_{i,j}$ są "przecięciami" grup P_i z grupami Q_j. Doskonałą ilustracją wprowadzonych oznaczeń jest rysunek 3.2.

Oczywiście tak dokładny rozkład dostajemy jedynie wtedy, gdy $R_a^\perp$ jest rozkładalna. Może się jednak zdarzyć, że $R_a^\perp$ jest rozkładalna jedynie względem niektórych liczb pierwszych. Wtedy już nie otrzymamy pełnego obrazu grupy multyplikatywnej, a jedynie jego część. Załóżmy więc (przy oznaczeniach takich jak wyżej), że $R_a^\perp$ nie jest rozkładalna jedynie względem $q_t, \dots, q_s$, gdzie $t < s$. Rysunek 3.3 ilustruje uzyskany rozkład.



Rysunek 3.3: Rozkład przestrzeni $R_a^\perp$

Charakterystyczną cechą przytoczonych schematów rozkładów jest to, że jeśli grupa $R_a^\perp$ jest rozkładalna względem jakiegoś q_j, to mamy

$$(|Q_j|, |H_j|) = 1, \tag{3.1}$$

gdyż $|Q_j|$ jest potęgą liczby pierwszej, która nie dzieli $|H_j|$.

3.1. Elementy rozdzielające przestrzeni $R_a^\perp$

Naszym głównym celem będzie zidentyfikowanie tych elementów $R_a^\perp$, które będą w stanie dać nam jakąś informację na temat dzielników elementu a. Przypominam, że zbiór $R_a^\perp$ zawiera elementy nie mające nietrywialnego wspólnego dzielnika z a. W związku z tym informacji na temat rozkładu będziemy szukać w pierwiastkach pewnych równań wielomianowych, a konkretnie w rozwiązaniach równania

$$X^n - 1 \equiv 0 \mod a.$$

Definicja 3.3 Powiemy, że podprzestrzeń Q_j jest prosta, jeżeli $Q_j \simeq Q_{i,j}$ dla pewnego i.

□

Można podać warunek, który mówi kiedy dana podprzestrzeń Q_j jest prosta. Sformułujmy go w postaci stwierdzenia.

Stwierdzenie 3.1 Na to, aby Q_j była prosta potrzeba i wystarcza, żeby q_j dzieliło dokładnie jedno $p_i^\perp$.

■

Definicja 3.4 Definiujemy przekształcenie

$$\pi_{i,j} : R_a^{\perp} \to R_a^{\perp},$$

jako rzut na podprzestrzeń $Q_{i,j}$ oraz przekształcenie

$$ord : R_a^{\perp} \to \mathbb{Z}_+ \cup \{0\},$$

które zwraca rząd argumentu.

□

Poniższy lemat pokazuje elementarne własności wyżej zdefiniowanych przekształceń.

Lemat 3.1 Przekształcenia $\pi_{i,j}$ oraz ord mają następujące własności

(a) jeśli $q_j \nmid n$, to dla każdego $1 \leq i \leq r$ i $b \in R_a^{\perp}$ mamy

$$ord(\pi_{i,j}(b)) = ord(\pi_{i,j}(b^n)),$$

(b) jeśli $n = q_j^k$, to dla każdego $1 \leq i \leq r$ i $b \in R_a^{\perp}$ mamy

$$ord(\pi_{i,j}(b^n)) = \max\{\frac{ord(\pi_{i,j}(b))}{n}, 1\}.$$

Dowód: Zauważmy, że skoro $\pi_{i,j}$ działa w $Q_{i,j} \simeq \mathbb{Z}_{q_j^{\beta_{i,j}}}$, to każdy element przy tym odwzorowaniu przechodzi na element rzędu q_j^l dla pewnego l. Ponieważ $\pi_{i,j}$ jest homomorfizmem, to

$$\pi_{i,j}(b^n) = \pi_{i,j}(b)^n.$$

i dla n takich, że $q_j \nmid n$, podniesienie elementu $\pi_{i,j}(b)$ do potęgi n zachowa rząd, co dowodzi (a). Natomiast jeśli $n = q_j^k$, to rząd elementu $\pi_{i,j}(b)^n$ będzie równy $\max\{q_j^{l-k}, 1\}$, co kończy dowód (b).

■

Definicja 3.5 Element $b \in R_a^{\perp}$ nazwiemy rozdzielającym przestrzeń Q_j, jeżeli istnieją takie $1 \leq i < k \leq r$, że

$$ord(\pi_{i,j}(b)) \neq ord(\pi_{k,j}(b)), \qquad |Q_{i,j}| > 1 \quad \text{i} \quad |Q_{k,j}| > 1.$$

Jeżeli element b jest elementem rozdzielającym przestrzeń Q_j, dla każdego nietrywialnego Q_j, to powiemy, że b jest elementem całkowicie rozdzielającym. Zbiór elementów rozdzielających przestrzeń Q_j oznaczamy przez $\mathcal{Q}_j$, a zbiór elementów całkowicie rozdzielających przez $\mathcal{R}_a$.

□

Przykład 3.3 Zauważmy, że 1 nie jest elementem rozdzielającym w żadnym pierścieniu euklidesowym. Wynika to stąd, że 1 jest elementem neutralnym $R_a^{\perp}$ i jego rzut na dowolną podprzestrzeń (podgrupę) jest, jako obraz homomorficzny elementu neutralnego, elementem neutralnym tej podprzestrzeni. W związku z tym

$$\forall_{i,j} \quad ord(\pi_{i,j}(1)) = 0,$$

co oznacza, że 1 nie jest elementem rozdzielającym.

□

Okazuje się, że elementy rozdzielające niosą informację o czynnikach elementu a. Są więc tymi, których poszukiwaliśmy. Poniższe twierdzenie pokazuje ich własności.

Twierdzenie 3.3 (o rozdzielaniu) Jeśli $b \in \mathcal{Q}_j$ to dla pewnego $k \in \mathbb{N}_0$ zachodzi

$$(b^{h_j q_j^k} - 1, a) = d \neq 1,$$

gdzie $h_j = |H_j|$, a d jest nietrywialnym dzielnikiem elementu a.

Dowód: Skoro $b \in \mathcal{Q}_j$ to istnieją takie $i_0, i_1 \in \{1, \ldots, r\}$, że $ord(\pi_{i_1,j}(b)) < ord(\pi_{i_0,j}(b))$. Niech teraz $k \in \mathbb{Z}_+$ będzie takie, że $q_j^k = ord(\pi_{i_0,j}(b))$. Ponieważ $(q_j, h_j) = 1$, to na mocy lematu 3.1 mamy

$$\begin{aligned} b^{h_j q_j^{k-1}} &\not\equiv 1 \mod p_{i_0}^{\alpha_{i_0}}, \\ b^{h_j q_j^{k-1}} &\equiv 1 \mod p_{i_1}^{\alpha_{i_1}}, \end{aligned}$$

co daje

$$\begin{aligned} p_{i_0}^{\alpha_{i_0}} &\nmid b^{h_j q_j^{k-1}} - 1, \\ p_{i_1}^{\alpha_{i_1}} &\mid b^{h_j q_j^{k-1}} - 1. \end{aligned}$$

Oznacza to, że $(b^{h_j q_j^{k-1}} - 1, a) \neq 1$, co kończy dowód.

■

Przykład 3.4 Niech $n \in \mathbb{Z}$ takie, że $n = pq$, gdzie

$$\begin{aligned} p &= 2p' + 1, \\ q &= 2q' + 1, \end{aligned}$$

dla pewnych liczb pierwszych p, q, p', q'. Przy takich założeniach mamy

$$\mathbb{Z}_n^\perp \simeq Q_2 \oplus Q_{p'} \oplus Q_{q'},$$

gdzie

$$\begin{aligned} Q_2 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ Q_{p'} &= \mathbb{Z}_{p'}, \\ Q_{q'} &= \mathbb{Z}_{q'}. \end{aligned}$$

Zauważmy, że jedyną nietrywialną przestrzenią, którą możemy rozdzielić jest czteroelementowa grupa $Q_2 = \{1, -1, \sqrt{1}, -\sqrt{1}\}$, gdzie $\sqrt{1}$ i $-\sqrt{1}$ są rozwiązaniami następujących układów równań

$$\begin{cases} \sqrt{1} \equiv 1 \mod p \\ \sqrt{1} \equiv -1 \mod q \end{cases}, \qquad \begin{cases} -\sqrt{1} \equiv -1 \mod p \\ -\sqrt{1} \equiv 1 \mod q \end{cases}.$$

W związku z tym warstwy elementów $\sqrt{1}$, $-\sqrt{1}$ względem podgrupy $Q_{p'} \oplus Q_{q'}$ są zbiorami zawierającymi elementy rozdzielające Q_2. Oznacza to, że

$$\mathcal{Q}_2 = (\sqrt{1})(Q_{p'} \oplus Q_{q'}) \cup (-\sqrt{1})(Q_{p'} \oplus Q_{q'}).$$

Więc średnio, co drugi element rozdziela Q_2.

□

3.2. Gęstość elementów rozdzielających

Niech A będzie podzbiorem przestrzeni $R_a^\perp$. Określamy prawdopodobieństwo $\mathcal{P}$ zajścia zdarzenia A jako

$$\mathcal{P}(A) = \frac{|A|}{|R_a^\perp|}.$$

Naszym celem w tej części będzie znalezienie prawdopodobieństwa zajścia zdarzenia polegającego na wylosowaniu z przestrzeni $R_a^\perp$ elementu rozdzielającego przestrzeń Q_j, dla ustalonego j.

Twierdzenie 3.4 Przy oznaczeniach takich jak w poprzedniej części, niech Q_j będzie podprzestrzenią $R_a^\perp$ (niekoniecznie prostą), $I = \{i : \beta_{i,j} \neq 0\}$, a $\beta = \min\{\beta_{i,j} : \ 1 \leq i \leq r, \beta_{i,j} > 0\}$. Wtedy prawdopodobieństwo wylosowania elementu rozdzielającego przestrzeń Q_j wynosi

$$\mathcal{P}(\mathcal{Q}_j) \quad = \quad 1 - \frac{1}{|Q_j|}\left(1 + \sum_{k=1}^{\beta}(q_j^{k-1}(q_j-1))^{|I|}\right).$$

Dowód: Z treści twierdzenia wynika, że I jest zbiorem tych indeksów i, dla których przestrzeń $Q_{i,j} \simeq \mathbb{Z}_{q_j^{\beta_{i,j}}}$ (patrz rysunek 3.3) jest nietrywialna. Zauważmy ponadto, że element nie jest rozdzielający, jeżeli ma ten sam rząd w każdej z podprzestrzeni $Q_{i,j}$, dla $i \in I$. Zatem

$$\prod_{i \in I} q_j^{k-1}(q_j - 1)$$

określa liczbę elementów rzędu q_j^k, które nie rozdzielają Q_j. Wykonując sumowanie po możliwych rzędach i uwzględniając element jednostkowy otrzymujemy, że liczba elementów nierozdzielających Q_j wynosi

$$1 + \sum_{k=1}^{\beta}\prod_{i \in I} q_j^{k-1}(q_j-1) = 1 + \sum_{k=1}^{\beta}(q_j^{k-1}(q_j-1))^{|I|},$$

co po podzieleniu przez $|Q_j|$ daje nam prawdopodobieństwo wylosowania elementu nierozdzielającego Q_j. Stąd łatwo już uzyskać wzór na prawdopodobieństwo wylosowania elementu rozdzielającego

$$\mathcal{P}(\mathcal{Q}_j) \quad = \quad 1 - \frac{1}{|Q_j|}\left(1 + \sum_{k=1}^{\beta}(q_j^{k-1}(q_j-1))^{|I|}\right).$$

To kończy dowód.

■

Z powyższego twierdzenia wynika kilka użytecznych wniosków dotyczących specyficznych przestrzeni Q_j

Wniosek 3.3 Jeśli Q_j jest prosta, to

$$\mathcal{P}(\mathcal{Q}_j) = 0.$$

Dowód: Skoro Q_j jest prosta, to $|I| = 1$, $|Q_j| = q_j^\beta$ i mamy

$$\begin{aligned}
\mathcal{P}(\mathcal{Q}_j) &= 1 - \frac{1}{q_j^\beta}\left(1 + \sum_{k=1}^{\beta}(q_j^{k-1}(q_j - 1))\right) \\
&= 1 - \frac{1}{q_j^\beta}\left(1 + (q_j - 1)\sum_{k=1}^{\beta} q_j^{k-1}\right) \\
&= 1 - \frac{1}{q_j^\beta}\left(1 + (q_j - 1)\frac{q_j^\alpha - 1}{q_j - 1}\right) \\
&= 0.
\end{aligned}$$

■

Wniosek 3.4 Jeśli Q_j nie jest prosta i $q_j = 2$, to

$$\mathcal{P}(\mathcal{Q}_j) \geq \frac{1}{2}.$$

Dowód: Niech $|Q_j| = 2^{\beta_j}$. Skoro Q_j jest nietrywialna, to mamy $|I| \geq 2$ i $\beta_j \geq 2$. Do dowodu wykorzystamy nierówność

$$\forall_{\beta_j \geq 2} \quad 3 \cdot 2^{\beta_j - 1} = 2^{\beta_j} + 2^{\beta_j - 1} \geq 2^{\beta_j} + 2$$

Z nierówności tej mamy

$$\begin{aligned}
\frac{1}{2} &\geq \frac{1}{2^{\beta_j}}\left(\frac{2}{3}2^{\beta_j - 1} + \frac{2}{3}\right) \\
&\geq \frac{1}{2^{\beta_j}}\left(1 + \frac{2^{\beta_j} - 1}{3}\right) \\
&\geq \frac{1}{2^{\beta_j}}\left(1 + \frac{2^{\beta|I|} - 1}{2^{|I|} - 1}\right),
\end{aligned}$$

przy czym ostatnia nierówność wynika z faktu, że $2^{|I|} - 1 \geq 3$ dla $|I| \geq 2$ oraz, że $\beta|I| \leq \beta_j$. Powyższa nierówność daje nam oszacowanie prawdopodobieństwa wylosowania elementu rozdzielającego Q_j, gdyż mamy

$$\begin{aligned}
\mathcal{P}(\mathcal{Q}_j) &= 1 - \frac{1}{2^{\beta_j}}\left(1 + \sum_{k=1}^{\beta} 2^{(k-1)|I|}\right) \\
&= 1 - \frac{1}{2^{\beta_j}}\left(1 + \frac{2^{\beta|I|} - 1}{2^{|I|} - 1}\right) \\
&\geq 1 - \frac{1}{2} = \frac{1}{2}.
\end{aligned}$$

■

Przykład 3.4 pokazuje, że przedstawionego szacowania nie można już poprawić, gdyż tam $\mathcal{P}(\mathcal{Q}_2)$ wynosi dokładnie $\frac{1}{2}$.

Wniosek 3.5 Jeśli Q_j nie jest prosta, to

$$\mathcal{P}(\mathcal{Q}_j) \geq \frac{q_j - 1}{q_j^2}.$$

Dowód: Niech $|Q_j| = q_j^{\beta_j}$. Skoro Q_j nie jest prosta, to mamy $|I| \geq 2$ i $\beta_j \geq 2$. Z twierdzenia 3.4 wiemy, że

$$\begin{aligned}
\mathcal{P}(\mathcal{Q}_j) &= 1 - \frac{1}{q_j^{\beta_j}} \left(1 + \sum_{k=1}^{\beta} (q_j^{k-1}(q_j - 1))^{|I|} \right) \\
&= 1 - \frac{1}{q_j^{\beta_j}} \left(1 + \frac{q_j^{\beta|I|} - 1}{q_j^{|I|} - 1} (q_j - 1)^{|I|} \right) \\
&= 1 - \frac{1}{q_j^{\beta_j}} \left(1 + (q_j^{\beta|I|} - 1) \frac{(q_j - 1)^{|I|}}{q_j^{|I|} - 1} \right)
\end{aligned}$$

Ponieważ $\beta = \min\{\beta_{i,j} : \ 1 \leq i \leq r, \beta_{i,j} > 0\}$ i $I = \{i : \beta_{i,j} \neq 0\}$, to $\beta_j \geq \beta|I|$, co daje nam

$$\begin{aligned}
\mathcal{P}(\mathcal{Q}_j) &\geq 1 - \frac{1}{q_j^{\beta_j}} \left(1 + (q_j^{\beta_j} - 1) \frac{(q_j - 1)^{|I|}}{q_j^{|I|} - 1} \right) \\
&= 1 - \frac{1}{q_j^{\beta_j}} \left(1 + (q_j^{\beta_j} - 1) \frac{(q_j - 1)^{|I|-1}}{1 + q_j + \cdots + q_j^{|I|-1}} \right) \\
&\geq 1 - \frac{1}{q_j^{\beta_j}} \left(1 + q_j^{\beta_j} \left(\frac{q_j - 1}{q_j} \right)^{|I|-1} \right) \\
&= 1 - (1 - \frac{1}{q_j})^{|I|-1} - \frac{1}{q_j^{\beta_j}} \\
&\geq \frac{1}{q_j} - \frac{1}{q_j^{\beta_j}} \\
&\geq \frac{q_j - 1}{q_j^2}.
\end{aligned}$$

Ostatnia nierówność wynika z faktu, że $\beta_j \geq 2$ i kończy dowód.

■

Rozdział 4

Praktyczne zastosowania

Celem tego rozdziału jest pokazanie kilku praktycznych zastosowań wyłożonej w poprzednich rozdziałach teorii. Pokażę między innymi jak w prosty sposób można uzasadnić poprawność probabilistycznego testu pierwszości Millera-Rabina [Pom01, str. 124] [Coh96, str. 422] [Kob95, str. 161] oraz jak wykorzystać twierdzenia z rozdziału 3 do rozkładania wielomianów nad ciałami skończonymi.

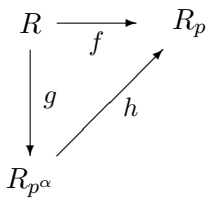
Istotnym dla nas jest również fakt, że rozważania poprzednich rozdziałów dotyczyły niemal dowolnych pierścieni euklidesowych. W związku z tym znaczna część algorytmów oparta na przedstawionej teorii znajduje swoje odpowieniki dla konkretnych pierścieni.

4.1. Testowanie pierwszości

W tej części przedstawię uogólnienie testu Millera-Rabina na rozważane we wcześniejszych rozdziałach pierścienie euklidesowe.

Lemat 4.1 Jeśli p jest elementem pierwszym pierścienia R, to grupa multyplikatywna ciała R_p zanurza się w grupie multyplikatywnej pierścienia R_{p^α}.

Dowód: Niech f i g będą homomorfizmami naturalnymi ideałów $(p^\alpha) \subset (p) \subset R$, a q będzie mocą grupy multyplikatywnej pierścienia R_p. Na mocy twierdzenia o homomorfizmie istnieje dokładnie jeden homomorfizm h, który domyka poniższy diagram.



Niech h^* będzie obcięciem h do odpowiednich grup multyplikatywnych. Ponieważ h^* jest "na", a $R_p^\perp$ jest cykliczna, to istnieje takie $\omega \in R_{p^\alpha}$, że $h^*(\omega)$ jest generatorem. W związku z tym $ord(\omega) = kq$ i element ω^k generuje grupę izomorficzną z $R_p^\perp$, co kończy dowód.

■

Lemat 4.2 Jeśli p jest elementem pierwszym i $|R_p| = q$, to $|R_{p^\alpha}| = q^\alpha$.

Dowód: Zauważmy, że jeśli $a \in R$, to dla $a_0 = (a \mod p)$ zachodzi $a - a_0 \in (p)$. W związku z tym jeśli $a \in (p^i)$, to $\frac{a}{p^i} \in R$ i dla $a_i = (\frac{a}{p^i} \mod p)$ mamy

$$\frac{a}{p^i} - a_i \in (p), \quad \text{co daje} \quad a - a_i p^i \in (p^{i+1}).$$

Teraz dla każdego elementu $a \in R$ definiujemy ciąg $(a_0, a_1, \ldots, a_{\alpha-1})$ jako

$$\begin{aligned} a_0 &= a \mod p, \\ a_i &= \frac{a - (a_0 + a_1 p + \cdots + a_{i-1} p^{i-1})}{p^i} \mod p. \end{aligned}$$

Na mocy poprzednich rozważań stwierdzamy, że

$$a - a_0 \in (p), \quad a - a_0 - a_1 p \in (p^2), \quad \ldots, \quad a - \sum_{i=0}^{\alpha-1} a_i p^i \in (p^\alpha),$$

co oznacza, że każdy element pierścienia R_{p^α} można reprezentować jako α-elementowy wektor o wyrazach z R_p. Jeżeli wykażemy, że taka reprezentacja jest jednoznaczna, to na mocy skończoności zbioru R_p otrzymamy tezę lematu. Niech zatem

$$\sum_{i=0}^{\alpha-1} a_i p^i + (p^\alpha) = \sum_{i=0}^{\alpha-1} a'_i p^i + (p^\alpha)$$

będą różnymi reprezentacjami tego samego elementu. Istnieje zatem takie $i_0 < \alpha$, że $a_{i_0} \neq a'_{i_0} \mod p$. W związku z tym

$$\sum_{i=i_0}^{\alpha-1} (a_i - a'_i) p^i \in (p^\alpha),$$

$$\sum_{i=i_0}^{\alpha-1} (a_i - a'_i) p^{i-i_0} \in (p^{\alpha-i_0}),$$

$$(a_{i_0} - a'_{i_0}) + p \sum_{i=i_0+1}^{\alpha-1} (a_i - a'_i) p^{i-i_0-1} \in (p^{\alpha-i_0}).$$

Ale to niemożliwe, gdyż $i_0 < \alpha$ i lewa strona jest niepodzielna przez p. Otrzymana sprzeczność dowodzi jednoznaczności zapisu i kończy dowód.

■

Lemat 4.3 Jeśli p jest elementem pierwszym i $|R_p| = q$, to $(p^\alpha)^\perp = (q-1)q^{\alpha-1}$.

Dowód: Zauważmy, że zbiór elementów podzielnych przez p tworzy w R_{p^α} ideał. Homomorfizm naturalny względem tego ideału przekształca pierścień R_{p^α} w R_p. Ponieważ pierścienie te są w szczególności addytywnymi grupami abelowymi, to z twierdzenia Lagrange'a mamy

$$|R_{p^\alpha}| = |R_p| \cdot |pR_{p^\alpha}|.$$

Co oznacza, że zbiór elementów nieodwracalnych pierścienia R_{p^α} ma moc $q^{\alpha-1}$. Uwzględniając, że $|R_{p^\alpha}| = q^\alpha$ dostajemy tezę lematu.

■

Przykład 4.1 Rozważmy pierścień $R = \mathbb{F}_{p^n}[X]$ wielomianów nad ciałem skończonym. Jeżeli $f \in \mathbb{F}_{p^n}[X]$ jest wielomianem nierozkładalnym stopnia d, to pierścień reszt modulo wielomian f ma moc $q = p^{nd}$, gdyż składa się ze wszystkich wielomianów stopnia mniejszego niż d. Rozważmy teraz pierścień reszt modulo f^2. Pierścień ten ma q^2 elementów i złożony jest z wielomianów stopnia mniejszego niż $2d$. Ponieważ f jest nierozkładalny, to elementy nieodwracalne w R_{f^2} są postaci $g \cdot f$, gdzie g jest wielomianem stopnia niższego niż d, jest więc ich dokładnie $p^{nd} = q$. W związku z tym mamy

$$R^{\perp}_{f^2} = q^2 - q = q(q-1).$$

□

Udowodnione lematy pozwalają na sformułowanie twierdzenia, które jest kluczowe do udowodnienia poprawności uogólnionego testu Millera-Rabina.

Twierdzenie 4.1 Jeśli $a \in R$ i dla każdego elementu pierwszego p dzielącego a mamy, że R_p jest ciałem charakterystyki różnej od 2, to $R^{\perp}_a$ jest rozkładalna względem 2.

Dowód: Ponieważ R_p nie jest ciałem charakterystyki 2, to $|R_p| = 2^k n + 1$, gdzie $2 \nmid n$ i $k > 1$. Niech teraz α będzie potęgą, z jaką element p wchodzi do rozkładu a na czynniki pierwsze. Wtedy z lematów 4.1 i 4.3 wynika, że $R^{\perp}_{p^\alpha}$ ma moc $2^k n(2^k n + 1)^{\alpha-1}$ i zawiera podgrupę cykliczną rzędu $2^k n$. W związku z tym, na mocy twierdzenia o skończenie generowanych grupach abelowych, mamy

$$R^{\perp}_{p^\alpha} \simeq \mathbb{Z}_{2^k} \oplus S,$$

gdzie $2 \nmid |S| = n(2^k n + 1)^{\alpha-1}$.

■

Przykład 4.2 Rozważmy pierścień $R = \mathbb{F}_3[X]$. W tym pierścieniu wielomian

$$p(X) = X^2 + X - 1$$

jest elementem pierwszym. W związku z tym $R^{\perp}_p$ jest grupą cykliczną, izomorficzną z $\mathbb{Z}_{2^3}$. Z udowodnionego powyżej twierdzenia wynika, że dla dowolnej dodatniej liczby całkowitej α, grupa $R^{\perp}_{p^\alpha}$ zawiera podgrupę rzędu 2^3. Poniżej przedstawiam generatory podgrupy rzędu 2^3 dla α równych 2, 3 i 4.

(a) Jeśli $\alpha = 2$, to $p^2 = X^4 - X^3 - X^2 + X + 1$ i dla $b = (X^3 \mod p^2)$ mamy

$$\begin{aligned} b^2 &= -X^3 + 1 \mod p^2 \\ b^4 &= -1 \mod p^2 \\ b^8 &= 1 \mod p^2 \end{aligned}$$

(b) Jeśli $\alpha = 3$, to $p^3 = X^6 + X^3 - 1$ i dla $b = (X^3 \mod p^3)$ mamy

$$\begin{aligned} b^2 &= -X^3 + 1 \mod p^3 \\ b^4 &= -1 \mod p^3 \\ b^8 &= 1 \mod p^3 \end{aligned}$$

(c) Jeśli $\alpha = 4$, to $p^4 = X^8+X^7-X^6+X^5+X^4-X^3-X^2-X+1$ i dla $b = (-X^7+X^6-X^4+1 \mod p^4)$ mamy

$$\begin{aligned} b^2 &= X^7 - X^6 + X^4 - X \mod p^4 \\ b^4 &= -1 \mod p^4 \\ b^8 &= 1 \mod p^4 \end{aligned}$$

□

Załóżmy, że mamy dany element a, który nie jest potęgą elementu pierwszego, spełnia założenia powyższego twierdzenia, i dla którego wiemy, że $|R_a| = q$. Naszym celem będzie stwierdzenie czy a jest elementem pierwszym. Innymi słowy chcemy zweryfikować hipotezę

$$H: \ a^{\perp} = q - 1.$$

Pokażemy, że weryfikacja hipotezy H jest możliwa z dowolnie dużym prawdopodobieństwem.

Twierdzenie 4.2 Niech $b \in \mathbb{R}_a^{\perp}$ oraz $q - 1 = 2^k m$, gdzie $2 \nmid m$. Rozważmy ciąg

$$b_0 = b^m, b_1 = (b^m)^2, b_2 = (b^m)^{2^2}, \ldots, b_k = (b^m)^{2^k}.$$

Jeżeli hipotezę H będziemy odrzucać zawsze wtedy, gdy prawdziwy jest jeden z następujących warunków

(a) $(b^m)^{2^k} \neq 1$,

(b) jeśli dla ostatniego (o ile taki istnieje) niejednostkowego wyrazu b_i mamy

$$(b_i - 1, n) > 1,$$

to dla $\mathcal{P}(H)$ oznaczającego prawdopodobieństwo błędnego zweryfikowania hipotezy H mamy

$$\mathcal{P}(H) \leq \frac{1}{2}.$$

Dowód: Niech Q będzie przestrzenią związaną z czynnikiem 2. Zauważmy, że jeśli a jest elementem pierwszym, to hipoteza H zostanie zawsze poprawnie zwaryfikowana. Naszym celem jest zatem oszacowanie prawdopodobieństwa błędnej weryfikacji hipotezy w przypadku, gdy a jest elementem złożonym.

$$\mathcal{P}(H) = \mathcal{P}(H|b_k \neq 1)\mathcal{P}(b_k \neq 1) + \mathcal{P}(H|b_k = 1)\mathcal{P}(b_k = 1),$$

ale $\mathcal{P}(H|b_k \neq 1) = 0$, gdyż $q - 1$ nie jest rzędem grupy multypilikatywnej pierścienia R_a i warunek (a) wyklucza hipotezę jako nieprawdziwą. Mamy zatem

$$\begin{aligned} \mathcal{P}(H) &= \mathcal{P}(H|b_k = 1)\mathcal{P}(b_k = 1) \\ &\leq \mathcal{P}(H|b_k = 1) \\ &= \mathcal{P}_{\{b_k=1\}}(H) \\ &= \mathcal{P}_{\{b_k=1\}}(H|b \in \mathcal{Q})\mathcal{P}_{\{b_k=1\}}(b \in \mathcal{Q}) + \\ &\quad \mathcal{P}_{\{b_k=1\}}(H|b \notin \mathcal{Q})\mathcal{P}_{\{b_k=1\}}(b \notin \mathcal{Q}), \end{aligned}$$

ale $\mathcal{P}_{\{b_k=1\}}(H|b \in \mathcal{Q}) = 0$ gdyż wtedy na mocy twierdzenia 3.3 zachodzi (b) i odrzucamy hipotezę. Natomiast $\mathcal{P}_{\{b_k=1\}}(H|b \notin \mathcal{Q}) = 1$ gdyż przyjmujemy hipotezę pomimo tego, że a jest złożone. Dostajemy zatem

$$\begin{aligned}\mathcal{P}(H) &\leq \mathcal{P}_{\{b_k=1\}}(H|b \notin \mathcal{Q})\mathcal{P}_{\{b_k=1\}}(b \notin \mathcal{Q}) \\ &= \mathcal{P}_{\{b_k=1\}}(b \notin \mathcal{Q}) \\ &\leq \mathcal{P}(b \notin \mathcal{Q}) \\ &\leq \frac{1}{2}.\end{aligned}$$

Ostatnia nierówność wynika z wniosku 3.4 i kończy dowód.

■

Przedstawiona metoda daje możliwość testowania pierwszości liczb całkowitych. Dla danej liczby całkowitej n wiemy, że $|R_n| = n$. Możemy zatem (o ile n nie jest potęgą liczby pierwszej i nie jest parzysta) zweryfikować hipotezę

$$H: \ n^{\perp} = n - 1.$$

Wielokrotne weryfikowanie tak postawionej hipotezy prowadzi nas do testu pierwszości znanego jako test Millera-Rabina.

Udowodnione twierdzenie pozwala nam również w łatwy sposób testować pierwszość wielomianów nad ciałem skończonym charakterystyki różnej od 2. Jeśli bowiem wielomian f jest elementem pierścienia $\mathbb{F}_{p^n}[X]$ i ma stopień d, to $|R_f| = p^{nd}$ i jeśli f nie jest potęgą jakiegoś wielomianu nierozkładalnego, to testowanie jego pierwszości polega na zweryfikowaniu hipotezy

$$H: \ f^{\perp} = p^{nd} - 1.$$

4.2. Rozkładanie na czynniki

Znamy wiele efektywnych algorytmów, które pozwalają na faktoryzację wielomianów nad ciałem skończonym [Coh96, str. 124] [Knu02, str. 471]. W tej części przeanalizujemy ten problem z punktu widzenia wprowadzonych w poprzednich rozdziałach pojęć.

Z poprzedniej części wynika, że z wielomianu można łatwo wydzielić część bezkwadratową. Wystarczy bowiem dany wielomian $f \in \mathbb{F}_{p^n}[X]$ podzielić przez (f, f'), gdzie f' oznacza pochodną f. Możemy więc bez straty ogólności w naszych rozważaniach ograniczyć się do rozpatrywania wielomianów bezkwadratowych.

Niech zatem $f \in \mathbb{F}_{p^n}[X]$ będzie wielomianem bezkwadratowym stopnia d. Załóżmy ponadto, że znamy jakiś dzielnik pierwszy q liczby $p^n - 1$. W przypadku gdy charakterystyka ciała jest różna od 2, takim dzielnikiem jest $q = 2$, natomiast dla charakterystyki 2 nie możemy explicite podać takiego dzielnika i być może metoda, którą opiszę, nie będzie miała zastosowania.

Zauważmy, że wielomian f może mieć co najwyżej d nierozkładalnych czynników stopnia 1, $\lfloor \frac{d}{2} \rfloor$ czynników stopnia 2 i ogólnie $\lfloor \frac{d}{r} \rfloor$ czynników stopnia r.

Lemat 4.4 Dla każdego bezkwadratowego wielomianu f stopnia d mamy, że $(\mathbb{F}_{p^n}[X])^{\perp}_{f}$ dzieli liczbę

$$m = \prod_{r=1}^{d} (p^{nr} - 1)^{\lfloor \frac{d}{r} \rfloor}.$$

Dowód: Zauważmy, że $(\mathbb{F}_{p^n}[X])^{\perp}_{f}$ zależy tylko od stopni potencjalnych czynników wielomianu f. Załóżmy zatem, że w rozkładzie f występuje t_r różnych czynników stopnia r. Korzystając z twierdzenia 3.2 mamy, że

$$(\mathbb{F}_{p^n}[X])^{\perp}_{f} = \prod_{r=1}^{d} (p^{nr} - 1)^{t_r}.$$

Ale jak już wspomniałem, czynników stopnia r może być co najwyżej $\lfloor \frac{d}{r} \rfloor$, co daje

$$\prod_{r=1}^{d} (p^{nr} - 1)^{t_r} \mid m$$

i kończy dowód.

■

Teraz już możemy wykorzystać metodę elementów rozdzielających do rozkładu wielomianu f na czynniki.

Twierdzenie 4.3 Niech $f \in \mathbb{F}_{p^n}[X]$ będzie wielomianem bezkwadratowym, q będzie pewnym czynnikiem pierwszym liczby $p^n - 1$, a $m = q^k s$ takie jak w lemacie 4.4 i $q \nmid s$. Rozważmy ciąg

$$b_0 = b^s, b_1 = (b^s)^q, b_2 = (b^s)^{q^2}, \ldots, b_k = (b^s)^{q^k},$$

gdzie $b \in (\mathbb{F}_{p^n}[X])^{\perp}_{f}$. Twierdzimy, że jeśli f nie jest pierwszy, to z prawdopodobieństwem

$$\mathcal{P} \geq \frac{q-1}{q^2}$$

istnieje w tym ciągu taki element b_i, że $(b_i - 1, f)$ jest nietrywialnym dzielnikiem f.

Dowód: Niech Q będzie podprzestrzenią związaną z czynnikiem q, a H jej dopełnieniem. Na mocy lematu 4.4 wiemy, że $|H| \mid s$. Zatem spełnione są założenia twierdzenia o rozdzielaniu. W takim razie warunkiem koniecznym i wystarczającym na to, aby (b_i, f) było nietrywialnym dzielnikiem f jest

$$b \in \mathcal{Q},$$

a to, jak wynika z wniosku 3.5, zachodzi dla elementów złożonych z prawdopodobieństwem

$$\mathcal{P} \geq \frac{q-1}{q^2},$$

co kończy dowód.

■

Przykład 4.3 Rozważmy pierścień wielomianów $\mathbb{F}_3[X]$. Niech

$$\begin{aligned} f_1 &= X^2 + X - 1, \\ f_2 &= X^3 + X^2 - 1. \end{aligned}$$

Łatwo można sprawdzić, że wielomiany f_1 i f_2 są nierozkładalne. Celem tego przykładu jest zastosowanie przedstawionej metody do rozłożenia na czynniki iloczynu powyższych wielomianów. Przyjmijmy zatem, że

$$f = f_1 \cdot f_2 = X^5 - X^4 + X^2 - X + 1$$

jest wielomianem, którego rozkład chcemy znaleźć. Ponieważ wielomian jest stopnia 5, a ciało nad którym działamy ma moc 3, to

$$m = \prod_{r=1}^{5} (3^r - 1)^{\lfloor \frac{5}{r} \rfloor} = 2^5 \cdot 8^2 \cdot 26 \cdot 80 \cdot 242 = 2^{17} \cdot 7865 = 2^{17} \cdot s.$$

Wybierzmy $b = X^3 + X^2 + 1$, wtedy

$$\begin{aligned} b_0 = b^s &= X^3 + X + 1, \\ b_1 = b^{2s} &= X^4 + X^3 - X + 1, \\ b_2 = b^{4s} &= -X^4 + X^2 + X, \\ b_3 = b^{8s} &= 1. \end{aligned}$$

Obliczając teraz największy wspólny dzielnik wielomianów $b_2 - 1$ i f dostajemy

$$(b_2 - 1, f) = X^3 + X^2 - 1.$$

□

Wielokrotne zastosowanie powyższego twierdzenia dla losowo wybranych elementów $b \in (\mathbb{F}_{p^n}[x])_f^{\perp}$ daje probabilistyczny algorytm faktoryzacji. Pojedyncza iteracja algorytmu wymaga podniesienia elementu do potęgi m-tej, co w praktyce oznacza wykonanie $O(\log(m))$ mnożeń. Aby wykazać praktyczną przydatność zaproponowanego algorytmu wystarczy udowodnić, że liczba $\log(m)$ zależy w sposób wielomianowy od rozmiaru danych.

Stwierdzenie 4.1 Pojedyncza iteracja algorytmu opartego na twierdzeniu 4.3 wymaga

$$\mathcal{O}(nd^2 \log(p))$$

mnożeń modulo f i jest wielomianowo zależna od liczby bitów potrzebnych do reprezentowania wielomianu f.

Dowód: Oszacujemy wielkość m

$$\begin{aligned} m &= \prod_{r=1}^{d} (p^{nr} - 1)^{\lfloor \frac{d}{r} \rfloor} \\ &\leq \prod_{r=1}^{d} (p^{nr})^{\frac{d}{r}} \\ &= \prod_{r=1}^{d} p^{nd} \\ &= p^{nd^2}. \end{aligned}$$

Aby reprezentować wielomian $f \in \mathbb{F}_{p^n}[X]$ stopnia d musimy na każdy z jego współczynników przeznaczyć $O(\log(p^n)) = O(n\log(p))$ bitów. Ponieważ wielomian ma $O(d)$ takich współczynników, to całkowity jego rozmiar szacuje się przez $O(nd\log(p))$. Liczba mnożeń w zaproponowanym algorytmie wynosi natomiast

$$O(\log(m)) = O(nd^2\log(p))$$

i jak widać, jest wielomianowo zależna od liczby bitów potrzebnych do reprezentowania wielomianu f.

■

Bibliografia

[Bro77] Jerzy Browkin. *Teoria ciał.* Państwowe Wydawnictwa Naukowe, 1977.

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1996.

[Knu02] Donald E. Knuth. *Sztuka programowania.* Wydawnictwa Naukowo–Techniczne, 2002.

[Kob95] Neal Koblitz. *Wykłady z teorii liczb i kryptografii.* Wydawnictwa Naukowo–Techniczne, 1995.

[Pom01] Richard Crandall i Carl Pomerance. *Prime Numbers – A Computational Perspective.* Springer-Verlag, 2001.

[Rot95] Joseph Rotman. *An Intoduction to the Theory of Groups.* Springer-Verlag, 1995.