WSTĘP DO KRYPTOGRAFII

Grzegorz Szkibiel

Jesień 2012/13

Spis treści

1 Kryptografia a steganografia **5**
- 1.1 Steganografia . . . 6
- 1.2 Szyfry przestawieniowe . . . 8
- 1.3 Systemy kryptograficzne . . . 9

2 Klasyczne metody szyfrowania **12**
- 2.1 Szyfry cykliczne . . . 12
- 2.2 Monoalfabetyczny szyfr Beauforta . . . 13
- 2.3 Kody afiniczne jednowymiarowe . . . 14
- 2.4 Permutacje alfabetu . . . 15
- 2.5 Analiza częstości występowania liter . . . 16
- 2.6 Homofony i nulle . . . 17
- 2.7 Jednostki dwuliterowe czyli digramy . . . 18
- 2.8 Szyfr Playfaira . . . 20
- 2.9 Podwójny szyfr Playfaira . . . 21
- 2.10 szyfr Delastelle'a . . . 22
- 2.11 Jednostki wieloliterowe . . . 23
- 2.12 Szyfry polialfabetyczne . . . 23
- 2.13 Łańcuch szyfrów i DES . . . 28

3 Maszyny szyfrujące **32**
- 3.1 Zasada działania . . . 32
- 3.2 Jak złamano szyfr ENIGMY . . . 36

4 Macierze szyfrujące **41**
- 4.1 Algebra liniowa modulo N . . . 41
- 4.2 Szyfry Hill'a . . . 44
- 4.3 Afiniczne przekształcenia szyfrujące . . . 48

5 Pakowanie plecaka **50**
5.1 Postawienie problemu 50
5.2 Szybko rosnące ciągi 51
5.3 Kryptosystem oparty na problemie pakowania plecaka 53

6 Systemy z publicznym kluczem **56**
6.1 Numeryczna funkcja jednokierunkowa 57
6.2 Funkcje skrótu 58
6.3 poufność i autentyczność. 58
6.4 Wymiana kluczy 60
6.5 2-1 funkcje jednokierunkowe 60

7 System RSA **62**
7.1 Rozkład liczb na czynniki 62
7.2 Liczby wybrane losowo 63
7.3 Zasada działania systemu RSA 64
7.4 Wpadka systemowa wspólny moduł 65
7.5 Wpadka systemowa niski wykładnik 65

8 Teorio-liczbowe podstawy RSA **67**
8.1 Systemy pozycyjne 67
8.2 Iterowane podnoszenie do kwadratu 69
8.3 Twierdzenie Eulera i Małe Twierdzenie Fermata 69
8.4 liczby pseudo-pierwsze 71
8.5 Chińskie twierdzenie o resztach 74
8.6 Kongruencje stopnia 2 77
8.7 Gra w orła i reszkę przez telefon 80

9 Zastosowania arytmetyki modulo m do rozkładu liczb **83**
9.1 Wzory skróconego mnożenia 83
9.2 Metoda ρ rozkładu na czynniki 85
9.3 Metoda faktoryzacji Fermata 87
9.4 Bazy rozkładu 88

10 Logarytm dyskretny **92**
10.1 Pojęcie logarytm dyskretny 92
10.2 System Diffiego–Hellmana uzgadniania klucza 93
10.3 System kryptograficzny Masseya-Omury 95
10.4 System ElGamala 96

11 Protokoły o zerowej wiedzy i przekazy nierozróżnialne **97**
11.1 Kolorowanie mapy 97
11.2 Logarytm dyskretny 99
11.3 Przekazy nierozróżnialne 100
11.4 Dowód faktoryzacji 102

Rozdział 9

Zastosowania arytmetyki modulo m do rozkładu liczb

Najpopularniejszą metodą łamania szyfru RSA jest próba znalezienia klucza deszyfrującego. Jest to równoważne znalezieniu rozkładu liczby n na czynniki. Zaproponujemy tu kilka metod opartych o Twierdzenie Eulera oraz Małe Twierdzenie Fermata.

9.1 Wzory skróconego mnożenia

Zaczniemy od następującego prostego wniosku, który znamy z tzw. „wzorów skróconego mnożenia"

9.1 Twierdzenie. *Dla dowolnej liczby całkowitej b i dowolnej liczby naturalnej n liczba $b^n - 1$ jest podzielna przez $b - 1$. Iloraz jest równy*

$$b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1.$$

Dowód. Korzystamy ze znanej tożsamości

$$b^n - 1 = (b-1)(b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1). \qquad \square$$

Zamieniając b na b^m otrzymujemy natychmiast następujący wniosek.

9.2 Wniosek. *Dla każdej liczby całkowitej b i dowolnych liczb naturalnych n i m zachodzi równość*

$$b^{mn} - 1 = (b^m - 1)(b^{m(n-1)} + b^{m(n-2)} + \cdots + b^{2m} + b^m + 1).$$

Jako przykład zastosowania powyższego wniosku zobaczmy, że $2^{35}-1$ dzieli się przez 31 oraz przez 127. Ciekawszym spostrzeżeniem jest tu fakt, że jeśli 2^n-1 jest liczbą pierwszą, to n jest także liczbą pierwszą. Liczby złożone Mersenne'a (tzn. liczby postaci 2^p-1, gdzie p jest liczbą pierwszą) są kontrprzykładem na to, że twierdzenie odwrotne nie zachodzi.

9.3 Twierdzenie. *Niech liczba b będzie względnie pierwsza z liczbą m i niech a i c będą liczbami naturalnymi. Jeśli $b^a \equiv 1 \pmod m$, $b^c \equiv 1 \pmod m$ oraz $d = \mathtt{NWD}(a, c)$, to $b^d \equiv 1 \pmod m$.*

Dowód. Zapiszmy $d = ua+vc$, gdzie u i v są liczbami całkowitymi. Ponieważ a i c są dodatnie, więc jedna z liczb u, v jest dodatnia, a druga ujemna lub równa 0. Załóżmy, że $u > 0$, $v \leq 0$. Mamy $b^{au} \equiv 1 \pmod m$ oraz $b^{c(-v)} \equiv 1 \pmod m$. Z drugiej kongruencji wynika, że $(b^{c(-v)})^{-1} \equiv 1 \pmod m$. Mnożąc stronami pierwszą kongruencję oraz tę ostatnią, otrzymujemy $b^{au+vc} \equiv 1 \pmod m$, co dowodzi tezę. □

9.4 Twierdzenie. *Jeśli p jest dzielnikiem pierwszym liczby b^n-1, to (i) dla pewnego dzielnika $d < n$ liczby n mamy $p \mid b^d-1$, lub (ii) $p \equiv 1 \pmod n$. Jeśli $p > 2$ oraz liczba n jest nieparzysta, to wówczas w przypadku (ii) mamy $p \equiv 1 \pmod{2n}$.*

Dowód. Ponieważ $p \mid b^n-1$, więc p nie jest dzielnikiem b. Zatem w myśl małego twierdzenia Fermata $b^{p-1} \equiv 1 \pmod p$. Z poprzedniego twierdzenia otrzymujemy $b^d \equiv 1 \pmod p$, gdzie $d = \mathtt{NWD}(n, p-1)$. Jeżeli $d < n$, to $p \mid b^d-1$, czyli zachodzi *(i)*. Jeśli $d = n$, to $d \mid p-1$, więc mamy *(ii)*. Jeżeli p i n są obie nieparzyste i $n \mid p-1$, to także $2 \mid p-1$ i $p \equiv 1 \pmod{2n}$. □

Przykłady. Jeśli chcemy rozłożyć na czynniki jakąkolwiek liczbę n to sprawdzamy po kolei czy liczby pierwsze mniejsze od $\sqrt{n}$ są dzielnikami n. Jeśli n jest duża pojawiają się tu przynajmniej dwa problemy. Po pierwsze liczb pierwszych robi się dużo, a po drugie rozpoznawanie liczb pierwszych powyżej 100 staje się kłopotliwe i często wymaga iterowania algorytmu. Powyższe twierdzenie znacznie zawęża ilość dzielników pierwszych liczby n.

9.5. Rozłóżmy na czynniki liczbę 2047. Zauważmy, że $2047 = 2^{11}-1$ oraz $\sqrt{2047} < 46$. Z twierdzenia 9.4 wynika, że jeśli $p \mid 2047$, to $p \equiv 1 \pmod{22}$ gdyż p i 11 są nieparzyste a jedynym właściwym dzielnikiem jedenastu jest 1. Zatem jeśli jakaś liczba pierwsza mniejsza od 46 dzieli 2047 to musi to być 23. Po podzieleniu przekonujemy się, że $2047 = 23 \cdot 89$.

9.6. Rozłóżmy na czynniki liczbę $3^{12} - 1 = 531440$. Z wniosku 9.2 wynika natychmiast, że $3^1 - 1$, $3^2 - 1$, $3^3 - 1$, $3^4 - 1$ oraz $3^6 - 1$ dzielą 531440. Zatem nasza liczba na pewno dzieli się przez 2^4, 5, (dzielniki $3^4 - 1$), 13 (dzielnik $3^3 - 1$) i 7 (dzielnik $3^3 + 1$, bo $3^6 - 1 = (3^3 - 1)(3^3 + 1)$). Po podzieleniu otrzymujemy $531440 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73$. Ponieważ 73 jest liczbą pierwszą otrzymaliśmy nasz rozkład.

9.7. Rozłóżmy na czynniki pierwsze liczbę $34359738367 = 2^{35} - 1$. Po pierwsze, mamy natychmiast dzielniki pierwsze $2^5 - 1 = 31$ i $2^7 - 1 = 127$. Po podzieleniu otrzymujemy $34359738367 = 31 \cdot 127 \cdot 8727391$. Liczba 8727391 jest jednak zbyt duża aby orzec, czy jest to liczba pierwsza, czy nie. Pierwiastek z tej liczby jest mniejszy od 2955, więc w dalszym ciągu mamy wiele kłopotliwych dzielników pierwszych do sprawdzenia. Z Twierdzenia 9.4 wynika jednak, że mamy do sprawdzenia tylko liczby pierwsze spośród 36, 71, 106, 141, i tak dalej aż do 2955. Od razu odrzucamy 36, a skoro 71 jest liczbą pierwszą, dzielimy i otrzymujemy $8727391 = 71 \cdot 122921$. Pierwiastek z tej ostatniej liczby wynosi „już tylko" 351. Z naszego ciągu możliwych dzielników pierwszych wyszukujemy liczby 211 i 281 mniejsze od 351 i sprawdzamy, że nie są one dzielnikami 122921. Zatem 122921 jest liczbą pierwszą i naszym rozkładem na czynniki jest $34359738367 = 31 \cdot 71 \cdot 127 \cdot 122921$.

Twierdzenie 9.4 oraz powyższe przykłady pokazują dlaczego wszystkie „rekordowe" liczby pierwsze są liczbami Mersenne'a. Przestaje też dziwić fakt, że pod koniec lat siedemdziesiątych XX wieku rekord największej liczby pierwszej $2^{21701} - 1$ należał do uczniów liceum.

9.2 Metoda ρ rozkładu na czynniki

Metoda rozkładu liczby złożonej na czynniki, którą teraz zaprezentujemy została przedstawiona przez J.M. Pollarda. Nazywana jest ona również *metodą Monte Carlo*. Możemy stosować ją do każdej liczby naturalnej i przy odpowiednim doborze parametrów jest ona szybsza niż dzielenie przez kolejne liczby pierwsze mniejsze od $\sqrt{n}$.

Pierwszy krok w metodzie ρ polega na wyborze łatwo obliczalnej funkcji przekształcającej zbiór $\mathbb{Z}_n$ w siebie. Jak zwykle, w pierwszej kolejności próbujemy wielomianów. W drugim kroku wybieramy pewną początkową wartość x_0, a następnie obliczamy kolejne iteracje funkcji f:

$$x_1 = f(x_0), \qquad x_2 = f(x_1), \qquad x_3 = f(x_2), \qquad \ldots$$

Po otrzymaniu pewnej liczby początkowych wyrazów tak zdefiniowanego ciągu, rozważamy różnice wyrazów tego ciągu w nadziei, że pewna z tych różnic, powiedzmy $x_i - x_j$, nie jest względnie pierwsza z n. Jeśli taka sytuacja nastąpi, to wówczas $\mathrm{NWD}(x_i - x_j,\, n)$ jest jednym z dzielników n.

Powyższy algorytm zilustrujemy na w miarę prostym przykładzie. Niech więc $n = 15857$, $f(x) = x^2 + 1$, $x_0 = 2$. Obliczamy kolejne wartości x_j otrzymując

$$\begin{array}{lll} x_0 = 2, & x_1 = 5, & x_2 = 26, \\ x_3 = 677, & x_4 = 14334, & x_5 = 4408, \\ x_6 = 5640, & x_7 = 459, & x_8 = 4541. \end{array}$$

Następnie badamy kolejne różnice, tj. najpierw odejmujemy x_0 od wszystkich pozostałych i zauważamy, że za każdym razem wychodzi iż liczby $x_j - x_0$ oraz 15857 są względnie pierwsze. Następnie, ponieważ $x_0 - x_1$ już badaliśmy, więc rozważamy różnice $x_j - x_1$ dla $j > 1$, a potem $x_j - x_2$ dla $j > 2$ itd. W końcu mamy $\mathrm{NWD}(x_7 - x_6,\, 15857) = \mathrm{NWD}(-5181,\, 15857) = 157$. Zatem $15857 = 157 \cdot 101$. Jeżeli chodzi o wielomian, który używamy, to jest to, niestety, kwestia wyczucia.

Opisany algorytm można nieco ulepszyć, a mianowicie dla każdego indeksu k wystarczy obliczyć tylko jeden NWD. Aby opisać to ulepszenie, zauważmy najpierw, że jeśli pewne indeksy k_0 i j_0 spełniają kongruencję $x_{k_0} \equiv x_{j_0} \pmod{r}$ dla pewnego dzielnika r liczby n, to kongruencja ta jest spełniona dla wszystkich indeksów $k > k_0$, $j > j_0$ takich, że $k - j = k_0 - j_0$. Wynika to z następującej własności kongruencji:

$$\text{jeżeli } y \equiv z \pmod{m}, \text{ to } f(y) \equiv f(z) \pmod{m},$$

a dokładnie, jeśli $x_{k_0} \equiv x_{j_0} \pmod{r}$, to również $x_{k_0+1} = f(x_{k_0}) \equiv f(x_{j_0}) = x_{j_0+1} \pmod{r}$, więc i $x_{k_0+2} \equiv x_{j_0+2} \pmod{r}$ itd.

Opiszemy więc wspomnianą modyfikację. W dalszym ciągu obliczamy kolejne wartości x_k. Załóżmy, że k jest liczbą $(h+1)$–bitową, tj. $2^h \le k < 2^{h+1}$. Za j weźmy $2^h - 1$, czyli największą liczbę h–bitową. Porównujemy wtedy x_k z x_j. Tak zmodyfikowany algorytm pozwala nam tylko raz obliczyć wartość $\mathrm{NWD}(x_k - x_j,\, n)$ dla każdego k. W powyższym przykładzie $n = 157857$ ograniczamy się więc do następujących obliczeń:

$$\begin{array}{ll} x_1 - x_0 = 3, & \mathrm{NWD}(3,\, 15857) = 1 \\ x_2 - x_1 = 21, & \mathrm{NWD}(21,\, 15857) = 1 \\ x_3 - x_1 = 672, & \mathrm{NWD}(672,\, 15857) = 1 \end{array}$$

$$
\begin{aligned}
x_4 - x_3 &= 3657, & \mathtt{NWD}(3657,\, 15857) &= 1\\
x_5 - x_3 &= 3731, & \mathtt{NWD}(3731,\, 15857) &= 1\\
x_6 - x_3 &= 4963, & \mathtt{NWD}(4963,\, 15857) &= 1\\
x_7 - x_3 &= -218, & \mathtt{NWD}(-218,\, 15857) &= 1\\
x_8 - x_7 &= 4082, & \mathtt{NWD}(4082,\, 15857) &= 157.
\end{aligned}
$$

i w tym momencie algorytm staje się szybszy od metody dzieleń przez kolejne liczby pierwsze.

9.3 Metoda faktoryzacji Fermata

Opisane dotychczas metody rozkładu dużych liczb na czynniki działały bądź z pewnym prawdopodobieństwem, bądź też tylko dla bardzo szczególnych liczb. Okazuje się jednak, że jak dotąd, nie znaleziono skutecznej metody rozkładu, która zawsze zadziała i nie wymaga męczących obliczeń. Omówimy teraz metodę, która działa skutecznie dla liczb, których dzielniki są zbyt blisko siebie. Opiera się ona na następującym twierdzeniu.

9.8 Twierdzenie. *Niech n będzie dodatnią liczbą nieparzystą. Istnieje wówczas wzajemnie jednoznaczna odpowiedniość pomiędzy rozkładami (a, b) liczby $n = ab$ i zapisami (t, s) liczby $n = t^2 - s^2$.*

Dowód. Wystarczy sprawdzić, że następujące odwzorowania są wzajemnie jednoznaczne.

$$(a, b) \mapsto \left(\frac{a+b}{2}, \frac{a-b}{2}\right); \qquad (t, s) \mapsto (t+s, t-s). \qquad \square$$

W naszych dalszych rozważaniach będziemy stosować oznaczenia przyjęte w twierdzeniu 9.16 oraz zakładać, że liczba n jest nieparzysta.

Zauważmy, że jeżeli $n = ab$ oraz a, b są blisko siebie, to $s = (a-b)/2$ jest małą liczbą, czyli liczba t niewiele różni się od $\sqrt{n}$. Szukając zatem rozkładu (a, b) liczby n próbujemy kolejnych wartości t od $[\sqrt{n}]+1$ aż znajdziemy taką liczbę t, że $t^2 - n$ jest pełnym kwadratem. Jest to nasza liczba s^2.

9.9 Przykład. Rozłóżmy na czynniki liczbę $n = 200819$. W tym celu obliczamy $\left[\sqrt{200819}\right] + 1 = 449$ i sprawdzamy, czy liczby $449^2 - 200819 = 782$, $450^2 - 200819 = 1681$ itd. są kwadratami. Okazuje się, że 782 nie jest kwadratem, ale $1681 = 41^2$. Zatem

$$200819 = 450^2 - 41^2 = 491 \cdot 409.$$

Oczywiście, często się zdarza, że opisana powyżej metoda nie przynosi rezultatu. Istnieje pewne ulepszenie, które teraz opiszemy. Mianowicie, możemy spróbować wartości $t = \left[\sqrt{kn}\right] + 1$, $\left[\sqrt{kn}\right] + 2$ itd. dla $k \in \mathbb{N}$. Tym razem otrzymamy $t^2 - s^2 = kn$, czyli rozkład liczby kn. Jeśli k jest małą liczbą, to $\text{NWD}(t+s,\, n) > 1$, czyli poznamy nietrywialny dzielnik właściwy liczby n.

9.10 Przykład. Rozłóżmy na czynniki liczbę 141467. Sprawdzając $t = 377$, 378, ... dochodzimy do wniosku, że do niczego nie dojdziemy. Próbujemy zatem $k = 3$ i sprawdzamy liczby 652, 653, 654 oraz 655. Otrzymujemy $655^2 - 141467 = 68^2$. Następnie obliczamy $\text{NWD}(655 + 68,\, 141467) = 241$ i otrzymujemy rozkład

$$141467 = 241 \cdot 587.$$

Pokażemy, że jeśli metoda Fermata nie przyniosła pożądanego skutku i chcemy zastosować opisane ulepszenie, to nie warto brać tu pod uwagę $k = 2$. Istotnie, jeśli $t^2 - s^2 = 2n$, to jedna z liczb $t + s$, $t - s$ musi być parzysta. Zatem obie liczby t i s są parzyste bądź obie są nieparzyste. Zatem i $t - s$ jest parzysta. Wynika stąd, że $4|2n$, czyli n jest liczbą parzystą. Jest to sprzeczność, ponieważ rozważamy tu tylko liczby n nieparzyste. Można pokazać (dowód wymaga znajomości pewnych nie wprowadzonych tu pojęć), że również $k = 4$ jest „złą" liczbą.

9.4 Bazy rozkładu

Metoda baz rozkładu jest ulepszeniem metody Fermata opisanej w poprzednim podrozdziale. Opiera się ona na następującej obserwacji. Jeżeli $t^2 \equiv s^2 \pmod{n}$, ale $t \not\equiv \pm s \pmod{n}$, to $n|t^2 - s^2$ ale $n \nmid t - s$ ani $t + s$. Zatem $\text{NWD}(t - s,\, n) > 1$ lub $\text{NWD}(t + s,\, n) > 1$. Dla przykładu rozważmy liczbę 4633. Zauważmy, że $4633|77^2 - 36^2$. Mamy $\text{NWD}(77 - 36,\, 4633) = 41$, więc $4633 = 41 \cdot 113$. Istotnym problemem jest tu znalezienie 77 i 36.

Wprowadzimy teraz kilka pojęć. *Bezwzględnie najmniejszą resztą* z dzielenia liczby całkowitej a przez $n \in \mathbb{Z}$ nazywamy liczbę całkowitą r taką, że $a \equiv r \pmod{n}$ oraz jeśli $a \equiv s \pmod{n}$, to $|r| \leq |s|$. *Bazą rozkładu* nazywamy zbiór $B = \{-1, p_1, p_2, \ldots, p_{h-1}\}$, gdzie p_i są różnymi liczbami pierwszymi. Liczba b jest *B–liczbą,* jeżeli bezwzględnie najmniejsza reszta z dzielenia b^2 przez n rozkłada się na iloczyn liczb należących do zbioru B.

Powróćmy do przykładu liczby $n = 4633$. Niech $B = \{-1, 2, 3\}$. Wówczas 67, 68 i 69 są B–liczbami, ponieważ

$$\begin{aligned} 67^2 &\equiv -144 \pmod{4633}, & -144 &= -1 \cdot 2^4 \cdot 3^2; \\ 68^2 &\equiv -9 \pmod{4633}, & -9 &= -1 \cdot 3^2; \\ 69^2 &\equiv 128 \pmod{4633}, & 128 &= 2^7. \end{aligned}$$

Niech teraz $\mathbb{Z}_2^h$ oznacza h–wymiarową przestrzeń wektorową nad ciałem $\mathbb{Z}_2$. Dla każdej liczby n i danej bazy rozkładu B zawierającej h liczb, każdej B–liczbie b przypisujemy wektor $\varepsilon \in \mathbb{Z}_2^h$ w następujący sposób.

Jeżeli $b^2 \bmod n = \prod_{i=0}^{h-1} p_i^{\alpha_i}$ niech $\varepsilon_i = \alpha_i \bmod 2$.
Wówczas $\varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{h-1})$.

W naszym przykładzie ($n = 4633$, $B = \{-1, 2, 3\}$) B–liczbie 67 odpowiada wektor $(1, 0, 0)$, B–liczbie 68 odpowiada także $(1, 0, 0)$, a B–liczbie 69 odpowiada wektor $(0, 1, 0)$.

Przypuśćmy, że mamy dany pewien zbiór B–liczb b_j takich, że odpowiadajace im wektory $\varepsilon_j = (\varepsilon_{0j}, \varepsilon_{1j}, \ldots, \varepsilon_{h-1,j})$ sumują się do zera. Oznaczmy przez a_j bezwzględnie najmniejszą resztę z dzielenia b_j^2 przez n i zapiszmy

$$a_j = \prod_{i=0}^{h-1} p_i^{\alpha_{ij}}.$$

Ponieważ ε_j sumują się do zera, a_j jest kwadratem. Zatem iloczyn liczb a_j jest kwadratem. Oznaczmy $\gamma_i = \frac{1}{2} \sum_j \alpha_{ij}$. Niech teraz

$$c = \prod_i p_i^{\gamma_i} \bmod n, \qquad b = \prod_j b_j \bmod n.$$

Wówczas mamy $b^2 \equiv c^2 \pmod{n}$. Jeżeli mamy pecha, to $b \equiv \pm c \pmod{n}$. Szukamy wtedy nowego zbioru B–liczb.

Sprawdzimy, czy mieliśmy pecha w naszym przykładzie, gdzie $n = 4633$, $B = \{-1, 2, 3\}$. Ponieważ $(1, 0, 0) + (1, 0, 0) = (0, 0, 0)$, więc możemy przyjąć $b_1 = 67$ oraz $b_2 = 68$. Wówczas $a_1 = -1 \cdot 2^4 \cdot 3^2$ oraz $a_2 = -1 \cdot 3^2$. Po pomnożeniu otrzymujemy $a_1 a_2 = 2^4 \cdot 3^4$, $c = 2^2 \cdot 3^2 \bmod 4633 = 36$ oraz $b = 67 \cdot 68 \bmod 4633 = -77$. Ponieważ $-77 \not\equiv \pm 36 \pmod{4)633}$, więc mamy szczęście!

Zastanówmy się teraz, jak często możemy mieć pecha. Skoro n jest liczbą złożoną, która rozkłada się na iloczyn r czynników pierwszych, to liczba b^2 ma $2^r \geq 4$ pierwiastków. Zatem losowy pierwiastek z b^2 jest równy $\pm b$ z prawdopodobieństwem $\frac{2}{2^r} \leq \frac{1}{2}$. Zatem w k próbach mamy przynajmniej jedną „dobrą" parę (b, c) z prawdopodobieństwem większym niż $1 - \frac{1}{2^k}$.

W dalszym ciągu nie wiemy, jak wybrać odpowiednią bazę rozkładu B oraz zbiór B–liczb b_j. Zwykle stosuje się tu dwa sposoby.

1. Za B bierzemy -1 oraz $h-1$ początkowych liczb pierwszych. Następnie zbieramy „na żywioł" dużo B–liczb mając nadzieję, że w końcu nam się poszczęści.

2. Najpierw zbieramy b_j tak, aby b_j^2 miało małą bezwzględną resztę przy dzieleniu przez n (na przykład rozważamy liczby bliskie $\left[\sqrt{kn}\right]$, itd.). Następnie za B bierzemy dokładnie to co potrzeba, aby zbiór wszystkie b_j były B–liczbami.

Stosując 1, wzięliśmy w naszym przykładzie $B = \{-1, 2, 3\}$ oraz za B–liczby wzięlismy 67, 68, 69. $(68^2 = 4624)$. Spróbujmy się uprzeć, że 68, 69 oraz 96 mają być B-liczbami $(96^2 \approx 2 \cdot 4633)$. Ponieważ $96 = -50 \bmod 4633$, więc za B przyjmujemy zbiór $\{-1, 2, 3, 5\}$. Mamy

$-9 = -1 \cdot 3^2 \qquad \varepsilon_1 = (1, 0, 0, 0)$
$128 = 2^7 \qquad \varepsilon_2 = (0, 1, 0, 0)$
$-50 = -1 \cdot 2 \cdot 5^2 \quad \varepsilon_2 = (1, 1, 0, 0).$

Dalej, $b = 68 \cdot 69 \cdot 96 \bmod 4633 = 1031$ oraz $c = 2^4 \cdot 3 \cdot 5 \bmod 4633 = 240$. Obliczamy teraz $\texttt{NWD}(1031 - 240, 4633)$ otrzymując 113. Zatem

$$4633 = 113 \cdot 41.$$

Na zakończenie podamy jeszcze jeden przykład.

9.11 Przykład. Niech $n = 1829$. Szukamy liczb b_j w pobliżu $\sqrt{kn}$ i jednocześnie nie chcemy, żeby w rozkładzie $b_j^2 \bmod n$ były liczby pierwsze większe od 13. Rezultat przedstawimy w poniższej tabelce.

b_j	-1	2	3	5	7	11	13
42	1			1			1
43		2		1			
61			2		1		
74	1					1	
85	1				1		1
86		4		1			

Możemy więc za b_j wziąć 43 i 86 lub 42, 43, 61 oraz 85. W pierwszym przypadku mamy pecha, ponieważ $43 \cdot 86 \bmod 1829 = 40$ oraz $2^3 \cdot 5 = 40$. W drugim przypadku nie jest juz tak źle, ponieważ $42 \cdot 43 \cdot 61 \cdot 85 \bmod 1829 = 1459$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \bmod 1829 = 901$ i $\mathtt{NWD}(1459 + 901, 1829) = 59$. Zatem $1829 = 59 \cdot 31$.