Metode faktorizacije

Bernardin Ibrahimpašić, Bihać

Uvod

Cilj faktorizacije prirodnih brojeva je zapisati prirodan broj n u obliku produkta $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gdje su p_i različiti prosti i α_i prirodni brojevi. Jednostavna i dobro poznata metoda faktorizacije je dijeljenje s prostim brojevima manjim ili jednakim $\sqrt{n}$. Budući da prostih brojeva manjih od $\sqrt{n}$ ima približno $2\sqrt{n}/\ln n$, ova metoda je spora za velike n koji se javljaju, npr. u primjenama u kriptografiji. Međutim, ta metoda je vrlo korisna za brojeve $n < 10^{12}$.

Postoje efikasni testovi određivanja da li je neki prirodan broj prost, a čije je polazište mali Fermatov teorem. Ukoliko prirodan broj n ne prođe neki od testova prostih brojeva, onda je n sigurno složen, ali ti testovi ne daju nam niti jedan netrivijalni faktor od n. Problem pronalaženja prostog faktora za složeni broj n je mnogo teži od samog problema utvrđivanja da li je n prost ili složen. Ovaj problem je vrlo važan za pitanje sigurnosti nekih kriptosustava, kao što je naprimjer RSA. Metode faktorizacije, zavisno od toga da li očekivani broj operacija zavisi samo o veličini broja n ili i o svojstvima prostih faktora od n, dijelimo na opće i specijalne. Neke od specijalnih metoda su Pollardova ρ-metoda, Pollardova $(p-1)$-metoda i Fermatova metoda, dok opće metode uglavnom koriste faktorske baze. U ovom članku ćemo opisati upravo spomenute metode. Prije toga ćemo pokazati kako se polazna metoda dijeljenja s prostim brojevima do $\sqrt{n}$ može poboljšati koristeći informacije o tome koji prosti brojevi uopće dolaze u obzir da budu djelitelji od n.

Teorem 1 (mali Fermatov teorem). *Neka je p prost broj. Tada za svaki cijeli broj b, takav da je $M(b,p) = 1$, vrijedi*

$$b^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Napomenimo da obrat ovog teorema ne vrijedi, jer p može biti i složen, a da ipak za neki b vrijedi (1).

Primjer 1. Za složen broj $n = 341 = 11 \cdot 31$ postoji cijeli broj b, takav da je $M(b,n) = 1$ i da je $b^{n-1} \equiv 1 \pmod{n}$.

Za $b = 2$, koji je relativno prost s n, imamo

$$2^{340} = \left(2^{10}\right)^{34} \equiv 1^{34} = 1 \pmod{341},$$

pa je

$$2^{341-1} = 2^{340} \equiv 1 \pmod{341}.$$

Propozicija 1. Neka je b cijeli i n prirodan broj. Tada je

$$b^n - 1 = (b-1)\left(b^{n-1} + b^{n-2} + \ldots + b^2 + b + 1\right).$$

Korolar 1. Neka je b cijeli, a m i n prirodni brojevi. Tada je

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

Propozicija 2. Neka je $M(b,n) = 1$, a a i c prirodni brojevi takvi da je $b^a \equiv 1 \pmod{n}$ i $b^c \equiv 1 \pmod{n}$. Ako je $d = M(a,c)$, tada je $b^d \equiv 1 \pmod{n}$.

Dokaz. Koristeći Euklidov algoritam, možemo zapisati d u obliku $ua + vc$, gdje je jedan od brojeva u i v prirodan, a drugi nula ili negativan cijeli broj. Bez smanjenja

općenitosti, možemo pretpostaviti da je $u > 0$ i $v \leqslant 0$. Sada obje strane kongruencije $b^a \equiv 1 \pmod{n}$ potenciramo s u, a drugu kongruenciju $b^c \equiv 1 \pmod{n}$ s v, pa dobivene rezultate pomnožimo. Dobijemo $b^{au+cv} \equiv 1 \pmod{n}$. Kako je $au + cv = d$, tvrdnja je dokazana.

Propozicija 3. Ako prost broj p dijeli $b^n - 1$, tada ili

1. $p | b^d - 1$ za neki netrivijalni djelitelj d od n, ili
2. $p \equiv 1 \pmod{n}$.

Ako je $p > 2$ i n neparan, tada je $p \equiv 1 \pmod{2n}$.

Dokaz. Kako je $b^n \equiv 1 \pmod{p}$, a prema malom Fermatovom teoremu je $b^{p-1} \equiv 1 \pmod{p}$. Prema propoziciji 2 to znači $b^d \equiv 1 \pmod{p}$, gdje je $d = M(n, p-1)$. Ako je $d < n$, tada p dijeli $b^d - 1$, za neki netrivijalni djelitelj d od n, pa je 1. slučaj dokazan. Ako je $d = n$, pošto d dijeli $p - 1$, imamo $p \equiv 1 \pmod{n}$. Konačno, ako su p i n oba neparna i n dijeli $p - 1$, tada očito i $2n$ dijeli $p - 1$.

Primjer 2. Faktorizirajmo broj $2^{35} - 1$.

Kako je $35 = 5 \cdot 7$, to $2^{35} - 1$, prema korolaru 1, mora biti djeljivo s $2^5 - 1 = 31$ i $2^7 - 1 = 127$. Kako je $2^{35} - 1 = 34\,359\,738\,367$, imamo

$$\frac{2^{35} - 1}{(2^5 - 1)(2^7 - 1)} = 8\,727\,391.$$

Još nam preostaje faktorizacija broja 8 727 391. Kako je $\lfloor \sqrt{8\,727\,391} \rfloor = 2\,954$, to trebamo ispitati proste brojeve manje ili jednake 2 954. Ali, prema propoziciji 3, svaki eventualni sljedeći prosti faktor p od $2^{35} - 1$ mora zadovoljavati kongruenciju $p \equiv 1 \pmod{2 \cdot 35}$, tj. $p \equiv 1 \pmod{70}$, pa zato ispitujemo samo brojeve $71, 211, 281, 421, 491, \ldots$. Odmah dobivamo $8\,727\,391 = 71 \cdot 122\,921$. Kako je $\lfloor \sqrt{122\,921} \rfloor = 350$, to nam preostaje ispitati još samo brojeve 211 i 281, ali nijedan nije prosti faktor od 122 921 pa zaključujemo da je 122 921 prost broj. Dakle $2^{35} - 1 = 31 \cdot 71 \cdot 127 \cdot 122\,921$.

Pollardova ρ-metoda

Uobičajen zahtjev kod ove metode, koja spada u specijalne metode faktorizacije, je da su prosti faktori od n maleni.

Ukoliko želimo faktorizirati prirodan n, onda se prvo izabere preslikavanje $f : \mathbf{Z}_n^* \longrightarrow \mathbf{Z}_n^*$, gdje je $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$, a $\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n : M(a, n) = 1\}$. Jednostavno se uzme polinom f s cjelobrojnim koeficijentima, koji nije linearan niti je bijekcija. Često se uzima $f(x) = x^2 \pm a$, za slučajan a, $0 < a \leqslant n - 3$. Najjednostavnije je za polinom f uzeti $f(x) = x^2 - 1 \pmod{n}$. Odaberimo slučajan x_0, $(0 < x_0 \leqslant n - 1)$, za početak iterativnog procesa $x_{j+1} = f(x_j)$, $(j = 0, 1, 2, \ldots)$. Najčešće se uzima $x_0 = 2$.

Neka je d netrivijalni faktor od n. Želimo naći x_k i x_l, takve da je

$$x_k \equiv x_l \pmod{d} \quad \text{i} \quad x_k \not\equiv x_l \pmod{n}.$$

Međutim, kako d nije unaprijed poznat, računamo $M(x_k - x_l, n)$ sve dok ne dobijemo netrivijalni faktor od n.

Primjer 3. Ilustrirajmo faktorizaciju broja $n = 1387$ Pollardovom ρ-metodom.

Neka je $f(x) = x^2 - 1 \pmod{1\,387}$ i $x_0 = 2$.

Pomoću $f(x)$ dobiva se niz x_i

$$2, 3, 8, 63, 1\,194, \overline{1\,186, 177, 814, 996, 310, 396, 84, 120, 529, 1053, 595, 339}$$

gdje se brojevi ispod crte ciklički ponavljaju.

Sada računamo:

$$\begin{aligned}
M(x_1 - x_0, n) &= M(3-2, 1387) &&= M(1, 1387) &&= 1\\
M(x_2 - x_1, n) &= M(8-3, 1387) &&= M(5, 1387) &&= 1\\
M(x_2 - x_0, n) &= M(8-2, 1387) &&= M(6, 1387) &&= 1\\
M(x_3 - x_2, n) &= M(63-8, 1387) &&= M(55, 1387) &&= 1\\
M(x_3 - x_1, n) &= M(63-3, 1387) &&= M(60, 1387) &&= 1\\
M(x_3 - x_0, n) &= M(63-2, 1387) &&= M(61, 1387) &&= 1\\
M(x_4 - x_3, n) &= M(1194-63, 1387) &&= M(1131, 1387) &&= 1\\
M(x_4 - x_2, n) &= M(1194-8, 1387) &&= M(1186, 1387) &&= 1\\
M(x_4 - x_1, n) &= M(1194-3, 1387) &&= M(1191, 1387) &&= 1\\
M(x_4 - x_0, n) &= M(1194-2, 1387) &&= M(1192, 1387) &&= 1\\
M(x_5 - x_4, n) &= M(1186-1194, 1387) &&= M(8, 1387) &&= 1\\
M(x_5 - x_3, n) &= M(1186-63, 1387) &&= M(1123, 1387) &&= 1\\
M(x_5 - x_2, n) &= M(1186-8, 1387) &&= M(1178, 1387) &&= 19
\end{aligned}$$

dakle, nakon 13 koraka dobijemo da je 19 prosti faktor od $n = 1387 = 19 \cdot 73$.

Kao što vidimo, ovdje za svaki k računamo $k-1$ puta $M(x_k - x_l, n)$. Ova metoda se može poboljšati Floydovom metodom, tako da za svaki k ispitujemo samo $M(x_k - x_{2k}, n)$. Sada za svaki k samo jednom računamo $M(x_k - x_{2k}, n)$, a pored toga ne moramo računati $x_{k+1}, x_{k+2}, \ldots, x_{2k-1}$.

Primjer 4. Poboljšanom metodom, faktorizacija broja $n = 1387$ se dobije nakon samo 3 koraka.

$$\begin{aligned}
M(x_2 - x_1, n) &= M(8-3, 1387) &&= M(5, 1387) &&= 1\\
M(x_4 - x_2, n) &= M(1194-8, 1387) &&= M(1186, 1387) &&= 1\\
M(x_6 - x_3, n) &= M(177-63, 1387) &&= M(114, 1387) &&= 19
\end{aligned}$$

Očekivani broj operacija za Pollardovu ρ-metodu je $O\left(n^{1/4} \ln^2 n\right)$.

Pollardovu ρ-metodu je za 24% ubrzao Richard P. Brent, koji je računao $M(x_{2^n-1} - x_j, n)$, gdje je $2^{n+1} - 2^{n-1} \leqslant j \leqslant 2^{n+1} - 1$, tj. koristio je $x_1 - x_3$, $x_3 - x_6$, $x_3 - x_7$, $x_7 - x_{12}$, $x_7 - x_{13}$, $x_7 - x_{14}$, $x_7 - x_{15}$, $x_{15} - x_{24}$, itd.

Pomoću ove metode Brent i Pollard su 1980. godine faktorizirali osmi Fermatov broj $F_8 = 2^{2^8} + 1 = 1\,238\,926\,361\,552\,897 \cdot p_{63}$, gdje je p_{63} prost broj sa 63 znamenke.

Pollardova $p-1$ metoda

Ova metoda također spada u klasu specijalnih metoda za faktorizaciju. Uvjet koji je ovdje poželjan je da za $n = pq$, gdje su p i q prosti brojevi, svi prosti faktori od $p-1$ manji su od nekog broja B. Treba napomenuti, da što je B veći, vjerojatnost uspješne faktorizacije veća je, ali je vrijeme potrebno za izvršavanje dulje. Inače, očekivani broj operacija za ovu metodu je $O\left(B \cdot \ln B \cdot \ln^2 n + \ln^3 n\right)$.

Za neke B ovo može biti polinomijalan algoritam, ali to je samo u specijalnim slučajevima. U općem slučaju, ova metoda nije puno bolja od običnog dijeljenja prostim brojevima manjim od $\sqrt{n}$.

Pogledajmo sada opis ove metode. Kao što je poznato, prema malom Fermatovom teoremu je $a^k \equiv 1 \pmod{p}$, za sve cijele brojeve a koji nisu djeljivi s p. To znači da p dijeli $a^k - 1$. Ako $a^k - 1$ nije djeljivo s n, tada je $d = M\left(a^k - 1, n\right)$ netrivijalni djelitelj od n. Kao kandidat za k se uzima produkt svih potencija prostih faktora koje su manji ili jednaki B. Ako nismo uspjeli pronaći faktor od n, onda odaberimo novi B i pokušajmo ponovo. Za a se obično uzima $a = 2$.

Primjer 5. Faktorizirajmo $n = 1\,241\,143$.

Uzmimo $B = 15$. Tada je $k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 360\,360$.

$$d = M(2^{360\,360} - 1,\ 1\,241\,143),\ M(861\,525, 1\,241\,143) = 547.$$

Dakle, jedan prosti faktor od n je $p = 547$, pa je $n = 1\,241\,143 = 547 \cdot 2\,269$, a kako je i $2\,269$ prost broj, n je faktoriziran.

U slučaju da je $(p-1)/2$ prost broj, ova metoda nije bolja od dijeljenja prostim brojevima manjim od $\sqrt{n}$. Napomenimo da postoji još jedna slična metoda, a to je Williamsova $p+1$ metoda, koja se koristi u slučaju kad je p prosti faktor od n, a $p+1$ nema velike proste faktore.

Fermatova faktorizacija

Ako je cijeli broj n produkt dva bliska cijela broja, onda postoji jednostavna metoda za faktorizaciju broja n. Metoda se zove Fermatova faktorizacija a zasniva se na sljedećoj propoziciji.

Propozicija 4. Neka je n neparan prirodan broj. Tada postoji $1-1$ korespodencija između faktorizacija broja n u obliku $n = pq$, gdje je $0 < q \leqslant p$ i prikaz od n u obliku $n = x^2 - y^2$, gdje su x i y prirodni ili 0. Korespodencija je dana jednadžbama

$$x = \frac{p+q}{2}, \quad y = \frac{p-q}{2}, \quad p = x + y, \quad q = x - y.$$

Dokaz.

$$n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = x^2 - y^2.$$

U slučaju da su p i q bliski, tada je y malen a x je nešto malo veći od $\sqrt{n}$, pa se ispitivanje počne s $x = \lfloor \sqrt{n} \rfloor + 1$.

Primjer 6. Fermatovom faktorizacijom je jednostavno faktorizirati $n = 970\,171$.

Kako je $\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{970\,171} \rfloor = 984$, to počinjemo s $x = 984 + 1 = 985$, pa imamo

x	985	986
$\sqrt{x^2 - n}$	$\sqrt{54} \approx 7.35$	$\sqrt{2\,025} = 45$

Dakle, $x = 986$ i $y = 45$, pa je $n = 986^2 - 45^2$, tj. $p = 986 + 45 = 1\,031$ i $q = 986 - 45 = 941$, pa je tražena faktorizacija jednaka $n = 1\,031 \cdot 941$.

Primjer 7. Fermatovu faktorizaciju treba ponekad malo modificirati. Faktorizirajmo broj $n = 141\,467$.

Kako je $\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{141\,467} \rfloor = 376$, počinje se s $x = 376 + 1 = 377$ i povećava ga za 1 dok se ne faktorizira n. Međutim, kako je $n = 587 \cdot 241$, vrše se provjere za sve $377 \leqslant x \leqslant 414 = \dfrac{587 + 241}{2}$, a to je ukupno 38 provjera za x. Ali, ukoliko se pokuša s $x = \lfloor \sqrt{3n} \rfloor + 1$, dobivamo za početak $x = \lfloor \sqrt{3n} \rfloor + 1 = \lfloor \sqrt{424\,401} \rfloor + 1 = 651 + 1 = 652$. Provjeravajući redom, dobivamo $655^2 - 3 \cdot 141\,467 = 68^2$. Ako se sada izračuna $M(655 - 68, 141\,467) = 587$, imamo $n = 587 \cdot 241$. Ovdje su se izvršile samo 4 provjere za x.

Faktorske baze

Ideja koja je iskorištena u primjeru 7 je dovela do mnogo efikasnijeg algoritma za faktorizaciju. Cilj je naći dva prirodna broja x i y koji zadovoljavaju Legendreovu kongruenciju, tj. takve da je

$$x^2 \equiv y^2 \pmod{n} \quad \text{i} \quad x \not\equiv \pm y \pmod{n}.$$

Kako je

$$x^2 - y^2 \equiv (x + y)(x - y) \equiv 0 \pmod{n},$$

a kako n nije djelitelj ni od $x + y$ ni od $x - y$, slijedi da neki netrivijalni faktor od n, uzmimo p, dijeli $M(x + y, n)$, a drugi faktor $n/p = q$ dijeli $M(x - y, n)$.

Apsolutno najmanji ostatak broja a modulo n je cijeli broj između $-n/2$ i $n/2$ s kojim je a kongruentan; u oznaci $a \bmod n$.

Definicija 1. Skup $\mathcal{B} = \{p_1, p_2, \ldots, p_k\}$, različitih prostih brojeva, s tim da može biti $p_1 = -1$, zove se **faktorska baza**.

Definicija 2. Kvadrat cijelog broja b je $\mathcal{B}$-**broj** (za dani n), ako se apsolutno najmanji ostatak $b^2 \bmod n$ može zapisati kao produkt brojeva iz $\mathcal{B}$.

Primjer 8. Za dani $n = 4\,171$ i $\mathcal{B} = \{-1, 2, 3, 5\}$ kvadrati brojeva 64 i 65 su $\mathcal{B}$-brojevi, dok kvadrat broja 66 nije.

$$\begin{aligned} 64^2 &\equiv -75 \pmod{4\,171} & -75 &= -1 \cdot 3 \cdot 5^2 \\ 65^2 &\equiv 54 \pmod{4\,171} & 54 &= 2 \cdot 3^3 \\ 66^2 &\equiv 185 \pmod{4\,171} & 185 &= 5 \cdot 37 \end{aligned}$$

Metode za faktorizaciju, koje koriste faktorske baze, rade na sljedeći način. Prvo se odabere cijeli broj w "srednje" veličine. Ako broj n ima s znamenaka, onda se w odabere tako da približno ima l znamenaka, gdje je

$$s = \left\lfloor \frac{\ln n}{\ln 2} \right\rfloor + 1 \quad \text{i} \quad l = \left\lfloor \frac{\ln w}{\ln 2} \right\rfloor + 1.$$

Tako, na primjer, ako n ima 50 nameneka, w se odabere tako da ima 5 ili 6 znamenaka. Zatim se formira faktorska baza $\mathcal{B}$ čiji su elementi -1 i svi prosti brojevi manji ili jednaki w. Neka je $r = |\mathcal{B}|$. Poslije toga se odabere dovoljno brojeva b_i takvih da je apsolutno najmanji ostatak $b_i^2 \bmod n$ moguće napisati kao produkt elemenata iz $\mathcal{B}$. Dovoljno ih je pronaći $|\mathcal{B}| + 1 = r + 1$. Brojeve b_i biramo kao slučajne brojeve manje od n, ili ih biramo u obliku $\lfloor\sqrt{kn}\rfloor$ ili $\lfloor\sqrt{kn}\rfloor + 1$, za prirodan broj k. Sada svaki $b_i^2 \bmod n$ napišemo u obliku produkta elemenata iz $\mathcal{B}$, tj.

$$b_i^2 \bmod n = y_i = \prod_{j=1}^{r} p_j^{\alpha_{ij}}.$$

Nakon toga, za svaki y_i, $(1 \leqslant i \leqslant r+1)$, formiramo vektor $\vec{v}_i \in \mathbf{Z}_2^r$, tj. uređenu r-torku koja se sastoji od nula i jedinica, na način da je komponenta vektora $\vec{v}_i$ na mjestu j, $(1 \leqslant j \leqslant r)$, jednaka 1 ako je α_{ij} neparan, a 0 inače. Zatim nađemo podskup b_i-ova takav da je suma pripadnih $\vec{v}_i$-ova jednaka nulvektoru u $\mathbf{Z}_2^r$. Takav podskup uvijek postoji jer imamo skup od $r + 1$ vektora dimenzije r, pa su oni linearno zavisni. Na kraju x dobivamo množenjem odabranih b_i-ova modulo n, a y raspolavljajući potenciju p_i-ova u produktu odgovarajućih y_i-ova modulo n. Tako dobiveni x i y zadovoljavaju kongruenciju $x^2 \equiv y^2 \pmod n$. Ako je još $x \not\equiv \pm y \pmod n$, onda računajući $M(x+y, n)$ dobijemo netrivijalni faktor od n. U slučaju da je $x \equiv \pm y \pmod n$, onda biramo ili novi podskup od odabranih $r + 1$ b_i-ova ili biramo novih $r + 1$ b_i-ova ili mijenjamo skup $\mathcal{B}$.

Primjer 9. Ilustrirajmo faktorizaciju pomoću faktorske baze na primjeru kada je $n = 2\,041$, $w = 10$.

Imamo $\mathcal{B} = \{-1, 2, 3, 5, 7\}$, pa je $r = 5$. Sada pronađimo $r + 1 = 6$ odgovarajućih b_i-ova oblika $\lfloor\sqrt{k \cdot 2\,041}\rfloor$ ili $\lfloor\sqrt{k \cdot 2041}\rfloor + 1$, za prirodan k. Dobijemo

$$\begin{array}{rclcrcrcl}
b_1 &=& \lfloor\sqrt{2\,041}\rfloor &=& 45 & y_1 &=& 45^2 \bmod 2041 &=& -16 = -1 \cdot 2^4 \\
b_2 &=& \lfloor\sqrt{2\,041}\rfloor + 1 &=& 46 & y_2 &=& 46^2 \bmod 2041 &=& 75 = 3 \cdot 5^2 \\
b_3 &=& \lfloor\sqrt{2 \cdot 2\,041}\rfloor + 1 &=& 64 & y_3 &=& 64^2 \bmod 2041 &=& 14 = 2 \cdot 7 \\
b_4 &=& \lfloor\sqrt{4 \cdot 2\,041}\rfloor &=& 90 & y_4 &=& 90^2 \bmod 2041 &=& -64 = -1 \cdot 2^6 \\
b_5 &=& \lfloor\sqrt{5 \cdot 2\,041}\rfloor &=& 101 & y_5 &=& 101^2 \bmod 2041 &=& -4 = -1 \cdot 2^2 \\
b_6 &=& \lfloor\sqrt{6 \cdot 2\,041}\rfloor + 1 &=& 111 & y_6 &=& 111^2 \bmod 2\,041 &=& 75 = 3 \cdot 5^2
\end{array}$$

Na osnovu rastava od y_i na proste faktore, imamo sljedeće vektore

$$\vec{v}_1 = (1, 0, 0, 0, 0) \qquad \vec{v}_2 = (0, 0, 1, 0, 0) \qquad \vec{v}_3 = (0, 1, 0, 0, 1)$$
$$\vec{v}_4 = (1, 0, 0, 0, 0) \qquad \vec{v}_5 = (1, 0, 0, 0, 0) \qquad \vec{v}_6 = (0, 0, 1, 0, 0)$$

Formirajmo sada tablicu čiji su elementi α_{ij}

b_i	-1	2	3	5	7
45	1	4	–	–	–
46	–	–	1	2	–
64	–	1	–	–	1
90	1	6	–	–	–
101	1	2	–	–	–
111	–	–	1	2	–

Kako u aritmetici modulo 2, zbrajanju vektora $\vec{v}_i$ odgovara zbrajanje redaka u ovoj tablici, za odabir odgovarajućeg podskupa b_i-ova možemo promatrati tablicu. Suma prvog i četvrtog retka jednaka je nulvektoru u $\mathbf{Z}_2^5$, pa je $\{b_1, b_4\}$ jedan odgovarajući podskup b_i-ova, a to su također i $\{b_1, b_5\}$ i $\{b_2, b_6\}$. Pogledajmo slučaj $\{b_1, b_4\}$. Tada je

$$x = b_1 \cdot b_4 \bmod n = 45 \cdot 90 \pmod{2\,041} = -32,$$
$$y = (-1)^{(1+1)/2} \cdot 2^{(4+6)/2} \bmod 2\,041 = (-1)^1 \cdot 2^5 \bmod 2\,041 = -32.$$

Sada je $x^2 \equiv y^2 \bmod 2\,041$ ali i $x \equiv y \bmod 2\,041$, pa nam ovi x i y ne daju netrivijalni faktor od n.

Pogledajmo slučaj $\{b_1, b_5\}$:

$$x = b_1 \cdot b_5 \bmod n = 45 \cdot 101 \bmod 2\,041 = 463.$$
$$y = (-1)^{(1+1)/2} \cdot 2^{(4+2)/2} \bmod 2\,041 = (-1)^1 \cdot 2^3 \bmod 2\,041 = -8.$$

Imamo $463^2 \equiv (-8)^2 \bmod 2\,041$, ali i $463 \not\equiv \pm 8 \pmod{2\,041}$, pa nam ovi x i y daju netrivijalni faktor od n. Daljnjim računanjem se dobiva

$$M(x + y, n) = M(463 - 8, 2\,041),\ M(455, 2\,041) = 13,$$

pa je jedan netrivijalni faktor od n jednak 13. Tada je $2\,041 = 13 \cdot 157$. Također dobivamo

$$M(x - y, n) = M(463 + 8, 2\,041),\ M(471, 2\,041) = 157.$$

Ideja ovdje opisane metode, koja zahtijeva $O\left(e^{(1+\varepsilon)\sqrt{\ln n \cdot \ln(\ln n)}}\right)$ operacija, gdje je ε proizvoljno malen, iskorištena je za mnogo efikasnije metode za faktorizaciju, kao što su metode verižnog razlomka, kvadratnog sita i sita polja brojeva, što su danas najefikasnije poznate opće metode za faktorizaciju velikih prirodnih brojeva.

Literatura

[1] J. A. BUCHMANN, *Introduction to Cryptography*, Springer–Verlag, New York, 2001.

[2] R. CRANDALL, C. POMERANCE, *Prime Numbers. A Computational Perspective*, Springer–Verlag, New York, 2002.

[3] A. DUJELLA, *Kriptografija*, PMF–Matematički odjel, Sveučilište u Zagrebu `http://www.math.hr/~duje/kript.html`

[4] C. POMERANCE, *Factoring*, Proceedings in Applied Mathematics, Vol. 42, 27–47, AMS, Providence, 1990.

[5] N. SMART, *Cryptography. An Introduction*, McGraw–Hill, New York, 2002.

[6] J. STILLWELL, *Elements of Number Theory*, Springer–Verlag, New York, 2003.

[7] D. R. STINSON, *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 1996.

[8] S. Y. YAN, *Number Theory for Computing*, Springer–Verlag, Berlin, 2002.