MATEMATIKA

Faktorizacija pomoću eliptičkih krivulja

Bernadin Ibrahimpašić[1]

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 brojevi i α_i prirodni. Naivna metoda faktorizacije broja n je dijeljenje broja n s prostim brojevima manjim ili jednakim $\sqrt{n}$. Kako prostih brojeva manjih od $\sqrt{n}$ ima približno $2\sqrt{n}/\ln n$ to je ova metoda spora za veliki n, ali se može koristiti u kombinaciji s nekim boljim metodama za odbacivanje eventualnih malih prostih faktora broja n.

Metode faktorizacije dijelimo na opće i specijalne. Kod općih metoda očekivani broj operacija ovisi samo o veličini broja n, a kod specijalnih ovisi također i o svojstvima prostih faktora broja n. U [3] su detaljno opisane Pollardova ρ-metoda, Pollardova $(p-1)$-metoda i Fermatova metoda, koje spadaju u grupu specijalnih metoda, te faktorske baze koja pripada općim metodama. U [1] su detaljno opisane metoda verižnih razlomaka i metoda kvadratnog sita, koje spadaju u grupu općih metoda.

U ovom radu, koji predstavlja nastavak na [3] i [1], opisat ćemo metodu faktorizacije koja koristi eliptičke krivulje koju je H. W. Lenstra predložio 1987. godine kao modifikaciju Pollardove $(p-1)$-metode (*Elliptic Curve Method* – ECM). To je jedan subeksponencijalni algoritam koji i danas predstavlja jedan od najefikasnijih poznatih algoritama za faktorizaciju.

Eliptičke krivulje

Neka je $\mathbb{K}$ polje s neutralnim elementima 1 za množenje i 0 za zbrajanje. Najmanji prirodan broj k takav da je $k \cdot 1 = 1 + 1 + \cdots + 1 = 0$ se naziva *karakteristika polja*. Ako takav broj ne postoji, kažemo da je polje $\mathbb{K}$ karakteristike 0. Treba napomenuti da se u poljima karakteristike različite od 2 i 3 smije nadopunjavati na potpun kvadrat i potpun kub, dijeleći s 2 i 3 ako je potrebno.

Definicija 1. Neka je polje $\mathbb{K}$ karakteristike različite od 2 i 3. *Eliptička krivulja* $E(\mathbb{K}) : y^2 = x^3 + ax + b$ nad poljem $\mathbb{K}$, je skup rješenja (x, y), $x, y \in \mathbb{K}$, jednadžbe

$$y^2 = x^3 + ax + b, \tag{1}$$

gdje su $a, b \in \mathbb{K}$ konstante takve da je $4a^3 + 27b^2 \neq 0$, zajedno sa specijalnom točkom $\mathcal{O}$ koja se zove *točka u beskonačnosti*.

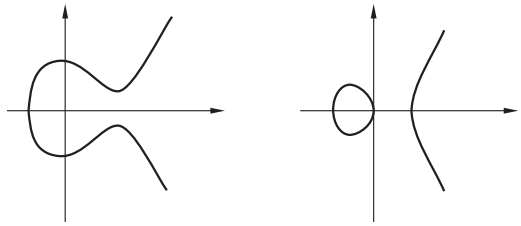
[1] Autor je profesor s Pedagoškog fakulteta Univerziteta u Bihaću; e-pošta: bernadin@bih.net.ba

Uvjet $4a^3 + 27b^2 \neq 0$ je potreban i dovoljan da jednadžba $x^3 + ax + b = 0$ nema višestrukih korijena. Ako je $4a^3 + 27b^2 = 0$, odgovarajuća se krivulja zove *singularna kubna krivulja*.

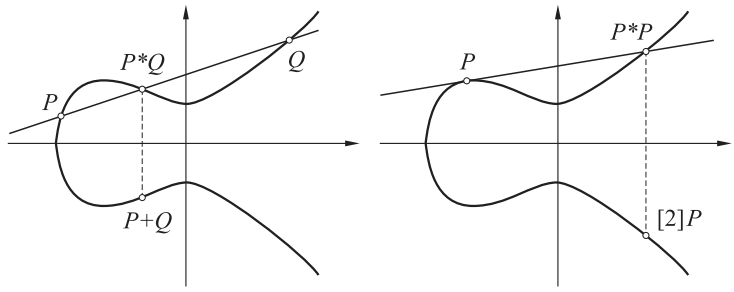
Ukoliko je polje $\mathbb{K}$ karakteristike 2, eliptička je krivulja nad $\mathbb{K}$ skup rješenja jedne od jednadžbi oblika $y^2 + cy = x^3 + ax + b$ ili $y^2 + xy = x^3 + ax^2 + b$, a ako je polje $\mathbb{K}$ karakteristike 3, tada je eliptička krivulja nad $\mathbb{K}$ skup rješenja jednadžbe $y^2 = x^3 + ax^2 + bx + c$, zajedno s točkom u beskonačnosti $\mathcal{O}$. Opći oblik jednadžbe, koji je dobar nad svim poljima, je $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Ovu jednadžbu nazivamo *Weierstrassova forma* od E. Napomenimo da se oblik (1), koji ćemo koristiti, naziva *kratka Weierstrassova forma* od E.

Jedno od najvažnijih svojstava eliptičkih krivulja je da se na njima može definirati binarna operacija, koju obično nazivamo zbrajanje, tako da točke na eliptičkoj krivulji s danom operacijom čine Abelovu grupu. Neutralni element je točka u beskonačnosti $\mathcal{O}$ a inverzni element točke $P = (x, y)$ je $-P = (x, -y)$.

Da bismo to objasnili, uzmimo da je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva. Tada eliptičku krivulju nad poljem $\mathbb{R}$, bez točke u beskonačnosti, možemo prikazati kao podskup ravnine. Polinom $f(x) = x^3 + ax + b$ može imati ili 1 ili 3 realna korijena. Tako graf pripadne eliptičke krivulje ima jednu ili dvije komponente, kao što je prikazano na slici.



Opišimo operaciju zbrajanja točaka na eliptičkoj krivulji geometrijski. Neka su $P, Q \in E(\mathbb{R})$. Ako je $P \neq Q$, onda povučemo sekantu, tj. pravac kroz točke P i Q. On siječe krivulju E u tri točke. Treću točku označimo s $P * Q$. Točku $P + Q$ definiramo kao osnosimetričnu točku točke $P * Q$ u odnosu na os x. Ako je $P = Q$, onda umjesto sekante povučemo tangentu na krivulju E u točki P. Ta tangenta siječe krivulju u još jednoj točki koju označavamo s $P * P$. Točku $P + P = [2]P$ definiramo kao osnosimetričnu točku točke $P * P$ u odnosu na os x.



Ovaj geometrijski zakon se može opisati i eksplicitnim formulama za koordinate zbroja točaka P i Q. Te formule mogu poslužiti za definiciju zbrajanja točaka na eliptičkoj krivulji nad proizvoljnim poljem, uz malu modifikaciju ako je polje karakteristike 2 ili 3.

Neka su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke na E. Tada je:

1. $-\mathcal{O} = \mathcal{O}$,
2. $-P = (x_1, -y_1)$,
3. $\mathcal{O} + P = P + \mathcal{O} = P$,
4. ako je $Q = -P$, onda je $P + Q = Q + P = \mathcal{O}$,
5. ako je $Q \neq -P$, onda je $P + Q = Q + P = (x_3, y_3)$ gdje je

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

pri čemu je

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } P \neq Q, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{ako je } P = Q. \end{cases}$$

Napomenimo također da se eliptičke krivulje nad konačnim poljem $\mathbb{F}_q$ definiraju analogno. U slučaju polja $\mathbb{F}_p$, gdje je p prost broj, operacije se izvode modulo p. U tom slučaju se pod dijeljenjem a/b u $\mathbb{F}_p$ podrazumijeva množenje ab^{-1} elementa a i multiplikativnog inverza b^{-1} elementa b po modulu p.

Primjer 1. *Odrediti točke na krivulji zadanoj jednadžbom*

$$E\,(\mathbb{F}_5) : y^2 = x^3 + 2x + 1.$$

Rješenje. Kako je krivulja definirana nad $\mathbb{F}_5$ imamo

$$y^2 \equiv x^3 + 2x + 1 \pmod 5.$$

Da bismo odredili točke na E, možemo računati $x^3 + 2x + 1 \pmod 5$ za sve moguće $x \in \mathbb{F}_5$ i pokušati riješiti jednadžbu $y^2 \equiv x^3 + 2x + 1 \pmod 5$.

x	0	1	2	3	4
$x^3 + 2x + 1$	1	4	13	34	73
$x^3 + 2x + 1 \pmod 5$	1	4	3	4	3
y	0	1	2	3	4
y^2	0	1	4	9	16
$y^2 \pmod 5$	0	1	4	4	1

Dobili smo

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (1,2), (1,3), (3,2), (3,3)\}. \qquad \diamondsuit$$

Primjer 2. *Na eliptičkoj krivulji nad $\mathbb{F}_5$, zadanoj jednadžbom $y^2 = x^3 + 2x + 1$, odrediti:*

a) $A + B$, *ako je* $A = (1,3)$ *i* $B = (0,4)$,

b) $[2]C$, *ako je* $C = (1,2)$.

Rješenje.

a) Prvo odredimo pripadni λ, a zatim izračunajmo koordinate točke $A+B=(x_3,y_3)$.

$$\begin{aligned}\lambda &\equiv (y_2-y_1)(x_2-x_1)^{-1} \pmod p \equiv (4-3)(0-1)^{-1} \pmod 5\\ &\equiv 1\cdot(-1)^{-1} \pmod 5 \equiv 4^{-1} \pmod 5 = 4\\ x_3 &\equiv \lambda^2 - x_1 - x_2 \pmod p \equiv 4^2 - 1 - 0 \pmod 5 \equiv 15 \pmod 5 = 0\\ y_3 &\equiv \lambda(x_1-x_3) - y_1 \pmod p \equiv 4\cdot(1-0) - 3 \pmod 5 = 1\\ &\Longrightarrow A+B=(0,1).\end{aligned}$$

b) Ponovo moramo odrediti pripadni λ, a zatim koordinate točke $[2]C=(x_3,y_3)$.

$$\begin{aligned}\lambda &\equiv \left(3x_1^2+a\right)(2y_1)^{-1} \pmod p \equiv \left(3\cdot 1^2+2\right)(2\cdot 2)^{-1} \pmod 5\\ &\equiv 5\cdot 4^{-1} \pmod 5 \equiv 5\cdot 4 \pmod 5 = 0\\ x_3 &\equiv \lambda^2 - x_1 - x_2 \pmod p \equiv 0^2 - 1 - 1 \pmod 5 \equiv -2 \pmod 5 = 3\\ y_3 &\equiv \lambda(x_1-x_3) - y_1 \pmod p \equiv 0\cdot(1-3) - 2 \pmod 5\\ &\equiv -2 \pmod 5 = 3\\ &\Longrightarrow [2]C=(3,3).\end{aligned}$$

♢

U primjenama eliptičkih krivulja često je potrebno računati višekratnik $[k]P$ točke P na eliptičkoj krivulji, gdje je

$$[k]P = \underbrace{P+P+\cdots+P}_{k \text{ pribrojnika}}.$$

To je specijalan slučaj potenciranja u Abelovoj grupi. Zbog toga za računanje $Q=[k]P$ višekratnika točke P na eliptičkoj krivulji E možemo iskoristiti "binarnu metodu". To je algoritam koji se u multiplikativnoj notaciji naziva "kvadriraj i množi", dok se u aditivnoj notaciji, što je slučaj kod eliptičkih krivulja, algoritam naziva "udvostruči i zbroji".

$Q=\mathcal{O}$
`za` $i=s-1,\ldots,1,0$ `radi`
  $Q=[2]Q$
  `ako je` $k_i=1$ `tada je` $Q=Q+P$

gdje je

$$k=\sum_{i=0}^{s-1} k_i 2^i = k_0 + 2\cdot k_1 + 2^2\cdot k_2 + \cdots + 2^{s-1}\cdot k_{s-1}$$

binarni zapis broja k.

Primjer 3. *Na eliptičkoj krivulji* $y^2=x^3+3x+1$ *nad* $\mathbb{F}_{1153}$ *izračunati* $[75](30,72)$.

Rješenje. Prvo odredimo binarni zapis broja 75,

$$75=(1001011)_2.$$

Nakon toga primijenimo binarnu metodu i izračunamo $[75](30,72)$, uz napomenu da za udvostručavanje i zbrajanje točaka na E koristimo već navedene formule.

i	$Q = [2]Q$	k_i	$Q = Q + P$
	$\mathcal{O}$		
6	$\mathcal{O}$	1	$\mathcal{O} + (30, 72) = (30, 72)$
5	$[2](30, 72) = (472, 519)$	0	
4	$[2](472, 519) = (157, 1087)$	0	
3	$[2](157, 1087) = (675, 127)$	1	$(675, 127) + (30, 72) = (439, 1064)$
2	$[2](439, 1064) = (361, 499)$	0	
1	$[2](361, 499) = (385, 952)$	1	$(385, 952) + (30, 72) = (485, 895)$
0	$[2](485, 895) = (282, 94)$	1	$(282, 94) + (30, 72) = (108, 31)$

Dobili smo

$$[75](30, 72) = (108, 31).$$

♢

Faktorizacija pomoću eliptičkih krivulja

Metoda za faktorizaciju koja koristi eliptičke krivulje je analogon Pollardove $(p-1)$-metode za faktorizaciju. Kako je n broj koji faktoriziramo složen, to $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ nije polje nego je prsten.

Faktorizaciju provodimo tako da prvo na slučajan način izaberemo eliptičku krivulju $E(\mathbb{Z}_n)$ zadanu jednadžbom $y^2 = x^3 + ax + b$, gdje je $\operatorname{nzd}(n, 6) = 1$. To možemo jednostavno napraviti tako da na slučajan način odaberemo $a, x, y \in \mathbb{Z}_n$, a zatim izračunamo $b = (y^2 - x^3 - ax) \pmod n$. Neka je

$$d = \operatorname{nzd}(4a^3 + 27b^2, n).$$

U ovisnosti od vrijednosti d imamo tri slučaja.

1. Ako je $1 < d < n$, d je netrivijalni faktor od n.
2. Ako je $d = n$, biramo novu eliptičku krivulju.
3. Ako je $d = 1$, dobro smo odabrali eliptičku krivulju $E(\mathbb{Z}_n)$ i biramo točku P na njoj, te možemo nastaviti dalje s algoritmom.

Nakon toga biramo granicu B i računamo k kao produkt svih potencija prostih brojeva koje su manje ili jednake B.

Sada računamo $[k]P$. Ako prilikom računanja ne možemo odrediti multiplikativni inverz modulo n nekog nazivnika, onda računamo najveći zajednički djelitelj tog nazivnika i broja n. Ako je taj najveći zajednički djelitelj različit od n, on predstavlja netrivijalni faktor broja n.

U slučaju neuspjeha biramo novu eliptičku krivulju ili povećavamo granicu B.

Primjer 4. *Faktorizirati broj* $n = 247$.

Rješenje. Odaberimo krivulju $E(\mathbb{Z}_{247})$ zadanu jednadžbom

$$y^2 = x^3 + 5x + 2.$$

Tada je

$$d = \text{nzd}\,(4 \cdot 5^3 + 27 \cdot 2^2, 247) = \text{nzd}\,(608, 247) = 19.$$

Kako je $1 < d = 19 < 247 = n$, to je $d = 19$ netrivijalni faktor od $n = 247$ i vrijedi

$$247 = 19 \cdot 13.$$

♢

Primjer 5. *Faktorizirati broj* $n = 187$.

Rješenje. Odaberimo krivulju $E(\mathbb{Z}_{187})$ zadanu jednadžbom

$$y^2 = x^3 + 10x + 5.$$

Tada je

$$d = \text{nzd}\,(4 \cdot 10^3 + 27 \cdot 5^2, 187) = \text{nzd}\,(4675, 187) = 187.$$

Kako je $d = 187 = n$, moramo birati novu eliptičku krivulju.

Odaberimo sada krivulju $E(\mathbb{Z}_{187})$ zadanu jednadžbom

$$y^2 = x^3 + 7x + 2.$$

Tada je

$$d = \text{nzd}\,(4 \cdot 7^3 + 27 \cdot 2^2, 187) = \text{nzd}\,(1480, 187) = 1.$$

Kako je $d = 1$, biramo točku $P \in E(\mathbb{Z}_{187})$ i nastavljamo dalje s algoritmom. Neka je $P = (8, 3) \in E(\mathbb{Z}_{187})$ i izaberimo granicu B. Neka je $B = 6$. Tada imamo

$$2^2 \leq B < 2^3, \quad 3^1 \leq B < 3^2, \quad 5^1 \leq B < 5^2, \quad 7 > B$$

$$\Longrightarrow k = 2^2 \cdot 3^1 \cdot 5^1 = 60,$$

pa trebamo izračunati $[k]P = [60](8, 3)$. Koristit ćemo binarnu metodu.

$$60 = (111100)_2.$$

i	$Q = [2]Q$	k_i	$Q = Q + P$
	$\mathcal{O}$		
5	$\mathcal{O}$	1	$\mathcal{O} + (8, 3) = (8, 3)$
4	$[2](8, 3) = (175, 37)$	1	$(175, 37) + (8, 3) = (106, 14)$
3	$[2](106, 14) = (85, 74)$	1	$(85, 74) + (8, 3) = \quad \Rightarrow\Leftarrow$

Dakle, ne možemo zbrojiti točke $[6]P$ i P. Pogledajmo odgovarajući λ kako bismo odredili netrivijalni faktor od 187:

$$\lambda = (3 - 74)(8 - 85)^{-1} \,(\text{mod}\, 187) = -71 \cdot (-77)^{-1} \,(\text{mod}\, 187) = 116 \cdot 110^{-1}.$$

Kako je $\text{nzd}\,(110, 187) = 11$, to 110 nema multiplikativni inverz modulo 187, pa ne možemo odrediti $[7]P$. Međutim broj $\text{nzd}\,(110, 187) = 11$ predstavlja netrivijalni faktor broja 187, pa smo dobili faktorizaciju

$$187 = 11 \cdot 17.$$

♢

Primjer 6. *Faktorizirati broj* $n = 851$.

Rješenje. Odaberimo krivulju $E(\mathbb{Z}_{851})$ zadanu jednadžbom

$$y^2 = x^3 + 3x + 5.$$

Tada je

$$d = \text{nzd}\,(4 \cdot 3^3 + 27 \cdot 5^2, 187) = \text{nzd}\,(3483, 187) = 1.$$

Kako je $d = 1$, to biramo točku P i granicu B, te nastavljamo dalje s algoritmom. Neka je $P = (1,3) \in E(\mathbb{Z}_{187})$ i $B = 6$. Tada imamo, kao u prošlom primjeru,

$$k = 2^2 \cdot 3^1 \cdot 5^1 = 60 = (111100)_2.$$

i	$Q = [2]Q$	k_i	$Q = Q + P$
	$\mathcal{O}$		
5	$\mathcal{O}$	1	$\mathcal{O} + (1,3) = (1,3)$
4	$[2](1,3) = (850,850)$	1	$(850,850) + (1,3) = (4,842)$
3	$[2](4,842) = (591,112)$	1	$(591,112) + (1,3) = (445,515)$
2	$[2](445,515) = (332,667)$	1	$(332,667) + (1,3) = (260,367)$
1	$[2](260,367) = (850,482)$	0	
0	$[2](850,482) = (11,37)$	0	

Vidimo da računajući $[60]P$ nismo uspjeli faktorizirati broj $n = 851$. Možemo odabrati novu krivulju ili povećati granicu B. Povećajmo granicu. Za $B = 10$ imamo

$$2^3 \leq B < 2^4, \quad 3^2 \leq B < 3^3, \quad 5^1 \leq B < 5^2, \quad 7^1 \leq B < 7^2, \quad 11 > B$$
$$\Longrightarrow k = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 2520 = (100111011000)_2.$$

i	$Q = [2]Q$	k_i	$Q = Q + P$
	$\mathcal{O}$		
11	$\mathcal{O}$	1	$\mathcal{O} + (1,3) = (1,3)$
10	$[2](1,3) = (850,850)$	0	
9	$[2](850,850) = (11,37)$	0	
8	$[2](11,37) = \quad \Rightarrow\Leftarrow$	1	

Dobili smo da ne možemo udvostručiti točku $[4]P = (11,37)$.

$$\lambda = (3 \cdot 11^2 + 3)(2 \cdot 37)^{-1} \,(\text{mod}\, 851) = 366 \cdot 74^{-1} \,(\text{mod}\, 851).$$

Kako je $\text{nzd}\,(74, 851) = 37$, to 74 nema multiplikativni inverz modulo 851, pa ne možemo odrediti $[8]P$. Međutim broj $\text{nzd}\,(74, 851) = 37$ predstavlja netrivijalni faktor broja 851, pa smo dobili faktorizaciju

$$851 = 37 \cdot 23. \qquad \diamondsuit$$

Kao što nam je poznato, uspjeh Pollardove $(p-1)$-metode ovisi o glatkoći broja $p-1$, gdje je p prosti faktor od n, tj. poželjno je da su svi prosti faktori od $p-1$ manji od neke granice B. U metodi koja koristi eliptičke krivulje, grupa $\mathbb{F}_p^*$ reda $p-1$ se zamjenjuje grupom $E(\mathbb{F}_p)$, čiji red, prema Hasseovom teoremu, pripada intervalu

$(p+1-2\sqrt{p}, p+1+2\sqrt{p})$, pa je opravdana naša nada da ćemo pronaći eliptičku krivulju nad $\mathbb{F}_p$ dovoljno glatkog reda. Napomenimo da je red eliptičke krivulje, tj. red grupe $E(\mathbb{F})$, u oznaci $|E(\mathbb{F})|$, jednak broju točaka na toj krivulji.

I kod ove metode, kao i kod Pollardove $(p-1)$-metode, k bi trebao biti višekratnik reda pripadne grupe. U ovom slučaju bi k trebao biti višekratnik od $|E(\mathbb{F}_p)|$, gdje je p neki prosti faktor od broja n koji faktoriziramo. U tom slučaju će kod računanja $[k]P$ pripadni nazivnik biti djeljiv s p, pa neće biti invertibilan modulo n, jer u $E(\mathbb{F}_p)$ vrijedi da je $[k]P = \mathcal{O}$.

Kod ocjene složenosti ovog algoritma ključno je pitanje kako optimalno odabrati granicu B. Označimo s $\psi(x,y)$ broj prirodnih brojeva iz segmenta $[1,x]$ koji su y-glatki, tj. neka je

$$\psi(x,y) = \#\{1 \leq n \leq x \,:\, n \text{ je } \ y\text{-gladak}\}.$$

Iz činjenice da su redovi $|E(\mathbb{F}_p)|$ skoro uniformirano distribuirani unutar Hasseovog intervala, dobivamo ocjenu vjerojatnosti uspjeha ovog algoritma

$$prob(B) > c \cdot \frac{\psi(p+1+2\sqrt{p}, B) - \psi(p+1-2\sqrt{p}, B)}{\sqrt{p} \cdot \ln p}.$$

Kako je, s druge strane, broj operacija potrebnih za pokušaj faktorizacije pomoću jedne eliptičke krivulje proporcionalan s B, to bismo željeli minimizirati vrijednost $B/prob(B)$. Taj minimum se postiže za

$$B = e^{(\sqrt{2}/p+o(1))\sqrt{\ln p \cdot \ln(\ln p)}},$$

dok je složenost algoritma

$$e^{(\sqrt{2}/p+o(1))\sqrt{\ln p \cdot \ln(\ln p)}}.$$

U najlošijem slučaju, tj. kada je $p = O(\sqrt{n})$, složenost metode faktorizacije pomoću eliptičkih krivulja je

$$e^{O\left(\sqrt{\ln n \cdot \ln(\ln n)}\right)}.$$

Iako postoje metode bolje složenosti, kao što je metoda sita polja brojeva, važno svojstvo ECM je da njena složenost ovisi o najmanjem prostom faktoru broja n, pa je vrlo prikladna za faktorizaciju "slučajnih" brojeva. Kako slučajni brojevi obično imaju neki prosti faktor koji je znatno manji od $\sqrt{n}$, to u takvim slučajevima ECM daje bolje rezultate od ostalih metoda. Također treba naglasiti da i kod primjene asimptotski boljih metoda imamo potrebu, unutar tih algoritama, faktorizirati neke "pomoćne" brojeve, za koje možemo očekivati da se ponašaju kao slučajni brojevi, pa se tu ECM može koristiti kao pomoćna metoda.

Literatura

[1] A. Crnkić, B. Ibrahimpašić, *Opće metode faktorizacije*, MFL 3/ 247 (2012), 177–186.

[2] A. Dujella, *Eliptičke krivulje u kriptografiji*, Skripta, PMF–MO, Zagreb, `http://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf`

[3] B. Ibrahimpašić, *Metode faktorizacije*, MFL 4/ 224 (2006), 233–239.

[4] B. Ibrahimpašić, A. Šehanović, *Eliptičke krivulje*, MAT–KOL Vol XVII (2)(2011), 17–24.

[5] B. Ibrahimpašić, *Uvod u teoriju brojeva*, Pedagoški fakultet, Bihać, 2014.

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