Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Mirna Repić

Faktorizacija u $\mathbb{Z}[x]$

Završni rad

Osijek, 2019.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Mirna Repić

Faktorizacija u $\mathbb{Z}[x]$

Završni rad

Voditelj: Izv. prof. dr. sc. Ivan Matić

Osijek, 2019.

Sažetak

Tema ovog rada je faktorizacija polinoma u $\mathbb{Z}[x]$. Polinomi su matematički izrazi koji sadrže varijable i konstante povezane računskim operacijama zbrajanja, oduzimanja i množenja, te nenegativnih cijelobrojnih potencija. Pokazat ćemo da postupak faktorizacije u $\mathbb{Q}[x]$ polinoma iz $\mathbb{Z}[x]$ završava u konačno mnogo koraka, kao i dokaz da je polinom ireducibilan u $\mathbb{Q}[x]$. Iznijet ćemo dvije ideje koje će nam pomoći učiniti postupak faktorizacije polinoma izvedivijim. Najprije ćemo uvesti pojam granične vrijednosti za koeficijente koji su djelitelji danog polinoma kojeg želimo faktorizirati. U postupcima traženja graničnih vrijednosti za korijene i koeficijente koristit ćemo metodu bisekcije i Newtonovu metodu. Potom ćemo naći učinkoviti način faktorizacije polinoma modulo M, gdje je M dovoljno velik modul. Pri tom ćemo koristiti Berlekampov algoritam faktorizacije i Henselovu metodu faktorizacije.

Ključne riječi: polinom, faktorizacija polinoma, granična vrijednost, ireducibilan polinom, stupanj polinoma

Abstract

The theme of this paper is the factorization of polynomials in $\mathbb{Z}[x]$. In mathematics, a polynomial is an expression consisting of variables and coefficients, that involves only the operations of addition, subtraction, multiplication, and non-negative integer exponents of variables. We will show that finding a factorization in $\mathbb{Q}[x]$ of a monic polynomial of degree n in $\mathbb{Z}[x]$, or showing that polynomial is irreducible in $\mathbb{Q}[x]$, takes finitely many steps. We will present two ideas that will make factoring process more feasible. Foremost, we will introduce the concept of bound for the coefficients of polynomials of a given polynomial. Thereat we will use the method of bisection and Newton's method. Thus, we will find an efficient way to factor a polynomial modulo M for M a suitably large modulus. For that process we will use Berlekamp's Factoring Algorithm and the Hensel Factorization Method.

Key words: polynomial, factorization of polynomial, bound on the coefficients, irreducible polynomial, degree of a polynomial

Sadržaj

1. Faktorizacija polinoma u $\mathbb{Z}[x]$

Za dani polinom $f(x)$ u $\mathbb{C}[x]$ postoji realan broj $B > 0$ takav da za svaki kompleksni broj z za koji vrijedi $|z| > B$ slijedi i $|f(z)| > 0$. Iz toga zaključujemo da ukoliko je r korijen od $f(x)$, tada je $|r| \leqslant B$, odnosno da postoji granična vrijednost za korijene polinoma $f(x)$. Iz granične vrijednosti korijena $f(x)$ postavljamo graničnu vrijednost za koeficijente bilo kojeg polinoma iz $\mathbb{C}[x]$ koji dijeli polinom $f(x)$.

Propozicija 1.1 *Neka je $f(x)$ u $\mathbb{C}[x]$ normirani polinom stupnja n i neka je $B > 0$ realan broj takav da za svaki r iz $\mathbb{C}$ koji je korijen od $f(x)$ vrijedi $|r| \leq B$. Nadalje, neka je*

$$g(x) = x^d + b_1 x^{d-1} + \ldots + b_{d-1}x + b_d$$

faktor stupnja d od $f(x)$. Tada za svaki k, $1 \leq k \leq d$, vrijedi

$$|b_k| \leq \binom{d}{k} B^k$$

Teorem 1.1 *Ako je $f(x)$ polinom s koeficijentima iz polja $\mathbb{C}[x]$ i a element polja $\mathbb{C}[x]$, onda je $f(a) = 0$ ako i samo ako $x - a$ dijeli $f(x)$.*

Dokaz Propozicije 1.1. Ako su $r_1, \ldots, r_d$ kompleksni korijeni od $g(x)$, tada

$$g(x) = (x - r_1)(x - r_2)\cdots(x - r_n).$$

Kada raspišemo desni dio prethodne jednadžbe i promotrimo koeficijente uz potencije od x vidimo da je, do na predznak, koeficijent b_k suma produkata k korijena od $r_1, \ldots, r_d$. Na primjer,

$$\begin{aligned} -b_1 &= r_1 + r_2 + \ldots + r_d, \\ b_2 &= r_1 r_2 + r_1 r_3 + r_2 r_3 + r_1 r_4 + \cdots + r_{d-1} r_d, \\ &\vdots \\ (-1)^d b_d &= r_1 r_2 r_3 \cdots r_d. \end{aligned}$$

Općenito, za svaki k, $1 \leq k \leq d$ vrijedi

$$(-1)^k b_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq d} r_{i_1} r_{i_2} \cdots r_{i_k}.$$

Uzimajući apsolutne vrijednosti obje strane jednakosti i primjenom nejednakosti trokuta dobivamo:

$$|b_k| \leq \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq d} |r_{i_1} r_{i_2} \cdots r_{i_k}|. \tag{1.1}$$

Svaki korijen ima apsolutnu vrijednost manju ili jednaku B, pa posljedično za svaki produkt iz prethodne nejednakosti vrijedi da je manji ili jednak B^k. Kako postoji $\binom{d}{k}$ načina na koji možemo odabrati k rješenja medu svim rješenjima $r_1, r_2, \ldots, r_d$, suma iz nejednadžbe (1.1) sadrži $\binom{d}{k}$ faktora. Sada očito slijedi

$$|b_k| \leq \binom{d}{k} B^k$$

za svaki k.

Teorem 1.2 *Postupak faktorizacije u $\mathbb{Q}[x]$ normiranog polinoma $f(x)$ stupnja n iz $\mathbb{Z}[x]$, kao i dokaz da je $f(x)$ ireducibilan u $\mathbb{Q}[x]$, završava u konačno mnogo koraka.*

Dokaz. Neka je $f(x)$ normirani polinom stupnja n u $\mathbb{Z}[x]$ i neka je B granična vrijednost za korijene polinoma $f(x)$. Ako $f(x)$ ima faktorizaciju u $\mathbb{Q}[x]$, tada je jedan od faktora od $f(x)$ normirani ireducibilni polinom $g(x) \in \mathbb{Z}[x]$ stupnja d, gdje je $d \leq n/2$ iz $\mathbb{Z}[x]$. Za svaki d, $1 \leq d \leq n/2$, i svaki k, $1 \leq k \leq d$, postoji konačno mnogo cijelih brojeva b_k za koje vrijedi

$$|b_k| \leq \binom{d}{k} B^k.$$

Odnosno, za svaki d postoji konačno mnogo normiranih polinoma

$$g(x) = x^d + b_1 x^{d-1} + \ldots + b_{d-1}x + b_d$$

u $\mathbb{Z}[x]$ takvih da za svaki k, $1 \leq k \leq d-1$ vrijedi

$$|b_k| \leq \binom{d}{k} B^k.$$

Prema tome, za svaki d, $1 \leq d \leq n/2$, samo konačno mnogo normiranih polinoma stupnja d mogu biti faktori polinoma $f(x)$. Za bilo koji takav $g(x)$ koji dijeli $f(x)$ možemo pisati $f(x) = g(x)h(x)$ i time smo faktorizirali polinom $f(x)$. Ukoliko niti jedan od kandidata za faktore polinoma ne dijeli $f(x)$ niti za jedan $d \leq n/2$, tada kažemo da je polinom $f(x)$ ireducibilan. Kako je svaki od brojeva d i n prirodan, ovaj postupak završava u konačno mnogo koraka.

Primijetimo da smo u prethodnom dokazu pretpostavili da je naš polinom normiran polinom s koeficijentima iz skupa cijelih brojeva. Od ranije znamo da za bilo koji dani polinom iz $\mathbb{Q}[x]$ množenjem polinoma nekim racionalnim brojem možemo dobiti polinom u $\mathbb{Z}[x]$ koji je prost, odnosno polinom čiji je najveći zajednički djelitelj svih koeficijenata jednak 1. Iz toga ne slijedi nužno da je novi dobiveni polinom normiran, no ako je

$$h(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

polinom s cjelobrojnim koeficijentima, tada je

$$g(y) = a_0^{n-1} h \frac{y}{a_0} = y^n + a_1 y^{n-1} + a_2 a_0 y^{n-2} + \ldots + a_0^{n-2} a_{n-1} y + a_0^{n-1} a_n$$

normirani polinom s cjelobrojnim koeficijentima i $h(x)$ faktorizira naš polinom na isti način kao i $g(y)$. Dakle, ako možemo faktorizirati svaki normirani polinom iz $\mathbb{Z}[x]$ u konačno mnogo koraka, isto slijedi i za svaki polinom iz $\mathbb{Q}[x]$.

Prethodni teorem pokazuje da je faktorizacija u $\mathbb{Z}[x]$ postupak koji završava u konačno mnogo koraka. Iz toga ne slijedi da je uvijek moguće provesti postupak faktorizacije. U teoriji, postupak faktorizacije je gotovo nemoguće dugačak postupak s obzirom na to da postoji vrlo mnogo polinoma koji su mogući faktori. Pokušat ćemo taj postupak učiniti nešto izvedivijim koristeći dvije ideje. Prva je da pokušamo naći bolju graničnu vrijednost za koeficijente polinoma koji su djelitelji danog polinoma. Druga je naći učinkovit način faktorizacije polinoma modulo M, gdje je M dovoljno velik modul. Kako bismo stekli dojam što ove ideje predstavljaju, pogledajmo sljedeći primjer.

Primjer 1.1 *Pretpostavimo da je*

$$f(x) = x^6 - 7x^5 + 16x^4 + 143x^3 - 939x^2 + 786x - 144.$$

Možemo vidjeti da je $B = 339$ *granična vrijednost za koeficijente svakog polinoma trećeg stupnja koji je faktor polinoma* $f(x)$. *Dodatno, možemo zaključiti da je* $f(x)$ *produkt dva polinoma koji su oba ireducibilna modulo* 5, *odnosno*

$$f(x) \equiv (x^3 + 2x + 1)(x^3 + 3x^2 + 4x + 1) \pmod 5.$$

Vidimo da ukoliko $f(x)$ *ima faktorizaciju u* $\mathbb{Z}[x]$, *njegovi faktori moraju biti ireducibilni polinomi trećeg stupnja. Ako je* $g(x) = x^3 + ax^2 + bx + c$ *faktor polinoma* $f(x)$ *u* $\mathbb{Z}[x]$ *i* $g(x) \equiv x^3 + 2x + 1 \pmod 5$, *onda znamo da su apsolutne vrijednosti svih koeficijenata* a, b *i* c *manje od* 339, *odnosno* $|a| \leq 339$, $|b| \leq 339$ *i* $|c| \leq 339$. *Kako* $335/5 = 67$, *zaključujemo da postoji* 135 *različitih brojeva* a *takvih da je* $a \equiv 0 \pmod 5$ *i* $|a| \leq 339$. *Analogno dobivamo i za koeficijente* b *i* c *pa vidimo da postoji približno* $135^3 = 2460375$ *mogućnosti za faktore polinoma* $f(x)$ *u* $\mathbb{Z}[x]$. *Očito bi postupak faktorizacije bio dug i kompliciran proces, pa nas zanima postoji li drugi način koji bi nas lakše doveo do rješenja.*
Pretpostavimo da je

$$f(x) \equiv (x^3 + 660x + 6)(x^3 + 676x^2 + 399x + 659) \pmod{683}$$

produkt ireducibilnih polinoma modulo 683, *prvog prostog broja većeg od* $2 \cdot 339$. *Ako* $f(x)$ *ima faktorizaciju u* $\mathbb{Z}[x]$, *onda znamo da* $f(x)$ *mora biti produkt dva ireducibilna polinoma stupnja* 3 *pri čemu za jedan od njih mora vrijediti*

$$g(x) \equiv x^3 + 660x + 6 \pmod{683}.$$

No, ukoliko je $g(x) = x^3 + ax^2 + bx + c$*, tada znamo da je i apsolutna vrijednost svih koeficijenata* a*,* b *i* c *manja ili jednaka* 339*. Jedini polinom* $g(x)$ *u* $\mathbb{Z}[x]$ *koji zadovoljava oba prethodna uvjeta je polinom*

$$g(x) = x^3 + (660 - 683)x + 6 = x^3 - 23x + 6.$$

Sada dijeljenjem polinoma $f(x)$ *polinomom* $g(x)$ *dobivamo i drugi faktor potreban za faktorizaciju:*

$$f(x) = (x^3 - 23x + 6)(x^3 - 7x^2 + 39x - 24).$$

Primjer 1.2 *Promotrimo polinom*

$$f(x) = x^6 - 31x^5 - 105x^4 + 757x^3 + 790x^2 - 176x + 97.$$

Taj polinom možemo zapisati kao umnožak dva polinoma koja su ireducibilna modulo 2*,*

$$f(x) \equiv (x^2 + x + 1)(x^4 + x + 1) \pmod 2.$$

Ukoliko $f(x)$ *ima faktorizaciju u* $\mathbb{Z}[x]$*, njegovi faktori moraju biti ireducibilni polinomi stupnja* 2 *i* 4*. Granična vrijednost za polinom drugog stupnja je* $B = 2236$*. Kao u prethodnom primjeru, ponovno želimo faktorizirati* $f(x)$ *modulo prvi prost broj veći od* $2B$*:*

$$f(x) \equiv (x^4 + 371x^3 + 559x + 706)(x^2 + 1608x + 1285) \pmod{4513}.$$

Ako je $g(x)$ *ireducibilan polinom drugog stupnja u* $\mathbb{Z}[x]$ *koji je faktor od* $f(x)$*, onda vrijedi*

$$g(x) \equiv x^2 + 1608x + 1285 \pmod{4513}.$$

Kako su koeficijenti polinoma $g(x)$ *manji od* 2236*, jedina mogućnost za* $g(x)$ *u* $\mathbb{Z}[x]$ *je* $g(x) = x^2 + 1608x + 1285$*. No, polinom* $f(x)$ *nije djeljiv polinomom* $g(x)$ *pa zaključujemo da polinom* $f(x)$ *nema ireducibilan faktor drugog stupnja te je i sam ireducibilan u* $\mathbb{Z}[x]$*.*

2. Postavljanje graničnih vrijednosti za korijene i koeficijente faktora

Neka je

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_0$$

normirani polinom s cjelobrojnim koeficijentima. Zanima nas kako dobiti graničnu vrijednost za koeficijente bilo kojeg normiranog faktora $g(x)$ polinoma $f(x)$ u $\mathbb{Z}[x]$. Jedan od načina traženja gornje granične vrijednosti je najprije pronaći gornju među za norme kompleksnih korijena polinoma $f(x)$, što smo spomenuli već u prvom poglavlju u Propoziciji 1.1. Znamo da je

$$B_0 = 1 + |a_1| + \ldots + |a_n|$$

gornja međa za korijene polinoma $f(x)$. Ipak, pokušat ćemo naći precizniju ocjenu gornje međe te naći graničnu vrijednost za koeficijente koristeći Mignotteovu teoriju iz 1974. godine te usporediti njegovu među s međom dobivene iz granične vrijednosti korijena.

Propozicija 2.1 *Neka je*

$$p(x) = x^n - (p_1 x^{n-1} + \ldots + p_{n-1}x + p_n)$$

polinom iz $\mathbb{R}[x]$ *pri čemu su svi* $p_1, p_2, \ldots, p_n \geq 0$ *te barem jedan* $p_j > 0$ *za* $1 \leq j \leq n$. *Tada za* $p(x)$ *postoji jedinstveni pozitivni realni korijen* r.
Dodatno, $p(x) < 0$ *za* $0 < x < r$ *i* $p(x) > 0$ *za* $x > r$.

Dokaz. Uzmimo da je

$$h(x) = \frac{p(x)}{x^n} = 1 - q(x)$$

gdje je $q(x) = \frac{p_1}{x} + \frac{p_2}{x^2} + \ldots + \frac{p_{n-1}}{x^{n-1}} + \frac{p_n}{x^n}$. Kako su svi $p_1, \ldots, p_n$ nenegativni i $q(x) \neq 0$, očito je da za dovoljno mali nenegativni x, $q(x)$ teži u $+\infty$, dok za dovoljno veliki x, $q(x)$ teži u 0. Dodatno, za $x > 0$ derivacija od $q(x)$,

$$q'(x) = -\left(\frac{p_1}{x^2} + 2\frac{p_2}{x^3} + \ldots + (n-1)\frac{p_{n-1}}{x^n} + n\frac{p_n}{x^{n+1}}\right)$$

je negativna suma članova većih ili jednakih 0 pa je očito za svaki $x > 0$ uvijek negativna. Prema tome, $q(x)$ monotono pada dok x raste na intervalu od 0 do $+\infty$. Tada je $h(x) = 1 - q(x)$ monotono rastući i negativan za svaki x blizu 0. Kada x pustimo u beskonačnost, $h(x)$ teži prema 1. Dakle, $h(x)$ ima jedinstveni pozitivni realni korijen koji možemo označiti s c. Tada je c i jedinstveni pozitivni realni korijen polinoma $p(x) = x^n h(x)$. Nadalje, $h(x)$ je manji od 0 za svaki x za koji je $0 < x < r$ i veći od 0 za svaki $x > r$. Zbog veze polinoma $h(x)$ i $p(x)$ isto vrijedi i za $p(x)$.

Sada to možemo proširiti na cijeli $\mathbb{C}[x]$.

Propozicija 2.2 *Neka je*

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

polinom u $\mathbb{C}[x]$. *Nadalje, neka je* $p_1 = |a_1|, \ldots, p_n = |a_n|$ *i neka je*

$$p(x) = x^n - (p_1x^{n-1} + \ldots + p_{n-1}x + p_n).$$

Ako je c *jedinstveni pozitivni realni korijen od* $p(x)$, *tada za svaki kompleksni korijen* α *od* $f(x)$ *vrijedi* $|\alpha| \leq c$.

Dokaz. Pretpostavimo da je $f(\alpha) = 0$. Tada je

$$\alpha^n = -(a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n),$$

pa po nejednakosti trokuta slijedi

$$\begin{aligned} |\alpha|^n = |\alpha^n| &= |a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n| \\ &\leq |a_1||\alpha^{n-1}| + \ldots + |a_{n-1}||\alpha| + |a_n| \\ &= p_1|\alpha|^{n-1} + \ldots + p_{n-1}|\alpha| + p_n. \end{aligned}$$

Uzmemo li $|\alpha| = r$, dobivamo

$$r^n \leq p_1r^{n-1} + \ldots + p_{n-1}r + p_n,$$

stoga je $p(r) \leq 0$ pa prema prethodnoj propoziciji dobivamo $|\alpha| = r \leq c$.

Iz prethodne dvije propozicije možemo dobiti nekoliko granica za norme kompleksnog korijena polinoma

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n :$$

$$\begin{aligned} B_1 &= \max_{1\leq k\leq n} \left(\frac{2^n - 1}{\binom{n}{k}}|a_k|\right)^{\frac{1}{k}}, \\ B_2 &= \max_{1\leq k\leq n} (2(|a_k|)^{\frac{1}{k}}), \\ B_3 &= \max_{1\leq k\leq n} ((n|a_k|)^{\frac{1}{k}}). \end{aligned}$$

Za B_1, B_2 i B_3 može se pokazati da su granice tako da pokažemo da su veće od jedinstvenog pozitivnog korijena c danog realnog polinoma $p(x)$ iz prethodne propozicije.

Propozicija 2.3 *Neka su dani* $f(x)$ *i* $p(x)$ *kao u Propoziciji* 2.2 *i* $B_2 = \max_{1\leq k\leq n}(2(|a_k|)^{\frac{1}{k}})$. *Tada je* $B_2 \geq c$, *pri čemu je* c *jedinstveni pozitivni korijen polinoma* $p(x)$.

Dokaz. Uzmemo li $B_2 = b$, imamo $b \geq 2|a_k|^{1/k}$ za svaki k pa slijedi

$$|a_k| \leq \frac{b^k}{2^k}.$$

Iz tog dobivamo

$$\begin{aligned} p(b) &= b^n - (|a_1|b^{n-1} + |a_2|b^{n-2} + \ldots + |a_k|b^{n-k} + \ldots + |a_n|) \\ &\geq b^n - \left(\frac{b}{2}b^{n-1} + \ldots + \frac{b^k}{2^k}b^{n-k} + \ldots + \frac{b^n}{2^n}\right) \\ &= b^n\left(1 - \frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^n}\right) > 0. \end{aligned}$$

Dakle, $B_2 = b > c$ po Propoziciji 2.1.

Za bilo koji dani polinom $f(x)$ možemo koristiti jedinstveni pozitivni korijen c od $p(x)$ kao graničnu vrijednost za norme korijena polinoma $f(x)$. Da bismo našli c možemo koristiti metodu bisekcije na $p(x)$ ili Newtonovu metodu na funkciji $h(x) = p(x)/x^n$.

Metoda bisekcije. Za metodu bisekcije potrebno je naći a_0 i b_0 sa svojstvom da je $p(a_0) < 0$ i $p(b_0) > 0$ te zatim promatrati $p((a_0 + b_0)/2)$. Ukoliko je $p((a_0 + b_0)/2) > 0$, postavljamo $a_1 = a_0$ i $b_1 = (a_0 + b_0)/2$ te ponavljamo postupak. U slučaju da je $p((a_0 + b_0)/2) < 0$, $a_1 = (a_0 + b_0)/2$ i $b_1 = b_0$ te ponovno ponavljamo postupak.

Newtonova metoda. Newtonovu metodu počinjemo s x_0, $h(x_0) = p(x_0)/x_0^n < 0$. U sljedećem koraku uzimamo $x_1 = x_0 - h(x_0)/h'(x_0)$ i ponavljamo postupak. Može se pokazati da uzimajući bilo koji x_0, $0 < x_0 \leq c$, kao početni ulaz za Newtonovu metodu dobivamo niz aproksimacija za (x_n) koji konvergira prema c.

Primjer 2.1 *Neka je*

$$f(x) = x^6 - 7x^5 + 16x^4 + 143x^3 - 939x^2 + 786x - 144.$$

Tada je

$$h(x) = 1 - \left(\frac{7}{x} + \frac{16}{x^2} + \frac{143}{x^3} + \frac{939}{x^4} + \frac{786}{x^5} + \frac{144}{x^6}\right)$$

i $h(1) < 0$. *Nakon* 14 *iteracija Newtone metode počevši s* $x_0 = 1$, *dobivamo*

$$c = 10.62080617.$$

Za usporedbu, koeficijenti od $f(x)$ *zadovoljavaju*

$$\begin{aligned} |a_1| &= 7, \\ |a_2|^{1/2} &= |16|^{1/2} = 4, \\ |a_3|^{1/3} &= |143|^{1/3} = 5.22, \\ |a_4|^{1/4} &= |939|^{1/4} = 5.54, \\ |a_5|^{1/5} &= |786|^{1/5} = 3.79, \\ |a_6|^{1/6} &= |144|^{1/6} = 2.29, \end{aligned}$$

pa su B_1, B_2, B_3

$$B_1 = \max_{1\le k\le n}\Big(\frac{2^n-1}{\binom{n}{k}}|a_k|\Big)^{\frac{1}{k}} = 73.5,$$
$$B_2 = \max_{1\le k\le n}(2(|a_k|)^{\frac{1}{k}}) = 14,$$
$$B_3 = \max_{1\le k\le n}((n|a_k|)^{\frac{1}{k}}) = 42.$$

Za $B_0 = 1 + |a_1| + \ldots + |a_n|$ *dobivamo* $B_0 = 1+7+16+143+939+786+144 = 2036$

U prethodnom primjeru nam je najbolja granična vrijednost od B_0, B_1, B_2, B_3 bila $B_2 = \max_{1\le k\le n}(2(|a_k|)^{\frac{1}{k}})$. Iz iskustva možemo zaključiti da je B_2 dobra međa za svaki polinom.

Propozicija 2.4 *Neka je*

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

polinom u $\mathbb{C}[x]$. *Neka je* $p_1 = |a_1|, p_2 = |a_2|, \ldots, p_n = |a_n|$ *i neka je*

$$p(x) = x^n - (p_1x^{n-1} + \ldots + p_{n-1}x + p_n).$$

Nadalje, neka je c *jedinstveni pozitivni realni korijen od* $p(x)$. *Tada*

$$B_2 = \max_{1\le k\le n}(2(|a_k|)^{\frac{1}{k}}) \le 2c.$$

Promatramo li primjer 2.1, imamo $c = 10.62080617$ i $B_2 = 14 < 2c$.

Dokaz. Neka je $B_2 = 2|a_l|^{1/l} = 2p_l^{1/l}$. Tada je $p_l = \frac{B_2^l}{2^l}$. Sada imamo

$$\begin{aligned} 0 = p(c) &= c^n - p_1c^{n-1} - p_2c^{n-2} - \ldots - p_lc^{n-l} - \ldots - p_n \\ &\le c^n - p_lc^{n-l} \\ &= c^{n-l}(c^l - p_l) \\ &= c^{n-l}\Big(c^l - \frac{B_2^l}{2^l}\Big). \end{aligned}$$

Dakle, $2^lc^l - B_2^l \ge 0$, odnosno $B_2 \le 2c$.

Ograničavanje korijena. Granična vrijednost B_2 ili međa c mogu nadopuniti Decartesov teorem o racionalnim korijenima tako da ograniče broj mogućnosti cjelobrojnih korijena normiranog polinoma s cjelobrojnim koeficijentima.

Primjer 2.2 *Neka je*

$$f(x) = x^6 - 7x^5 + 16x^4 + 143x^3 - 939x^2 + 786x - 144$$

polinom iz primjera 2.1. *Decartesov teorem govori da bilo koji cjelobrojni korijen od* $f(x)$ *mora dijeliti* 144, *no istovremeno svaki korijen od* $f(x)$ *mora imati normu manju ili jednaku* c *pri čemu je* $c = 10.62080617$. *Sada su mogućnosti za cjelobrojne korijene od* $d(x)$ *redom brojevi* $1, 2, 3, 4, 6, 8$ *i* 9 *te isti pomnoženi s* -1. *Time smo smanjili broj mogućih korijena s* 30 *na* 14.

Primjer 2.3 *Uzmimo sada da je*

$$f(x) = x^{18} + 5x^{10} + 2^9 3^9 5^9.$$

Za graničnu vrijednost B_2 *dobivamo* $B_2 = 2(2^9 3^9 5^9)^{1/18} = 2\sqrt{30} < 11$. *Sada nam Decartesov teorem smanjuje broj mogućnosti za korijene polinoma* $f(x)$ *s* 2000 *(broj djelitelja od* $2^9 3^9 5^9$*) na* 18 *cijelih brojeva čija je apsolutna vrijednost manja od* 11 *(*-1, -2, -3, -4, -5, -6, -8, -9, -10, 1, 2, 3, 4, 5, 6, 8, 9 *i* 10*).*

Ograničavanje koeficijenata. Iz granične vrijednosti B za korijene polinoma $f(x)$ dobivamo graničnu vrijednost za koeficijente svakog polinoma koji dijeli $f(x)$ u $\mathbb{C}[x]$ iz Propozicije 1.1. Naime, ako je

$$g(x) = x^d + b_1 x^{d-1} + \ldots + b_{d-1}x + b_d$$

normirani polinom stupnja d koji je faktor polinoma $f(x)$, onda za svaki k, $1 \leq k \leq d$, slijedi

$$|b_k| \leq \binom{d}{k} B^k.$$

Mignotte je pokazao da se granična vrijednost za koeficijente polinoma iz faktorizacije od $f(x)$ može dobiti i bez upotrebe granične vrijednosti za korijene kao u Propoziciji 1.1. Za polinom

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

s cjelobrojnim koeficijentima definiramo normu $||f|| = (|a_0|^2 + |a_1|^2 + \ldots + |a_n|^2)^{1/2}$, kao duljinu vektora čije su komponente koeficijenti $(a_0, a_1, \ldots, a_n)$ iz $\mathbb{C}^{d+1}$. Mignotte je ustvrdio da ako je

$$g(x) = b_0 x^d + b_1 x^{d-1} + \ldots + b_{d-1}x + b_d$$

iz $\mathbb{Z}[x]$ faktor polinoma $f(x)$, takav da je $g(x)g_1(x) = f(x)$ za $g_1(x)$ iz $\mathbb{Z}[x]$, onda za svaki k, $0 \leq k \leq d$, vrijedi

$$|b_k| \leq \binom{d}{k} ||f||.$$

Primjer 2.4 *Neka je*

$$f(x) = x^{10} + 4x^7 - 2x^3 + 5x - 1.$$

Tada je

$$||f|| = (1 + 16 + 4 + 25 + 1)^{1/2} = \sqrt{47}.$$

Uzmemo li da je $f(x) = g(x)g_1(x)$ *u* $\mathbb{Z}[x]$ *pri čemu je*

$$g(x) = b_0x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

iz $\mathbb{Z}[x]$*, možemo pretpostaviti da su* $g(x)$ *i* $g_0(x)$ *normirani, odnosno da je* $b_0 = 1$ *i* $b_5 = 1$ *ili* -1*. Tada Mignotteova granica implicira da ostali koeficijenti polinoma* $g(x)$ *moraju zadovoljavati*

$$|b_1| \leq \binom{5}{1}\sqrt{47} < 35,$$

$$|b_2| \leq \binom{5}{2}\sqrt{47} < 69,$$

$$|b_3| \leq \binom{5}{3}\sqrt{47} < 69,$$

$$|b_4| \leq \binom{5}{4}\sqrt{47} < 35.$$

Za usporedbu, jedinstveni pozitivni korijen c *odgovarajućeg polinoma* $h(x)$ *je* $c = 1.7966$ *pa ćemo za normirani faktor stupnja* 5 *polinoma* $f(x)$ *imati*

$$|b_1| \leq \binom{5}{1}c < 9,$$

$$|b_2| \leq \binom{5}{2}c^2 < 33,$$

$$|b_3| \leq \binom{5}{3}c^3 < 58,$$

$$|b_4| \leq \binom{5}{4}c^4 < 52.$$

Primjer 2.5 *Neka je*

$$f(x) = x^6 - 7x^5 + 16x^4 + 143x^3 - 939x^2 + 786x - 144$$

Tada je

$$||f|| = (1 + 7^2 + 16^2 + 143^3 + 939^2 + 786^2 + 144^2)^{1/2} = \sqrt{15410087} = 1241.4.$$

U Primjeru 1.1. *pokazali smo da je granična vrijednost za apsolutne vrijednosti korijena od* f *jednaka* $c = 10.62$*. Pretpostavimo da tražimo faktor od* $f(x)$ *u obliku*

$$g(x) = x^3 + b_1x^2 + b_2x + b_3.$$

Promotrimo granične vrijednosti za koeficijente dobivene preko graničnih vrijednosti za korijene

$$|b_k| < \binom{3}{k}||f||,$$

odnosno konkretnije

$$|b_1| < 3725, |b_2| < 3725, |b_3| < 1242.$$

Sada promotrimo granične vrijednosti za koeficijente dobivene Mignotteovom normom:

$$|b_k| < \binom{3}{k}c^k,$$

odnosno konkretnije

$$|b_1| < 32, |b_2| < 339, |b_3| < 1198.$$

Možemo primijetiti da je prvi pristup bolji za ograničavanje koeficijenata viših potencija od x u faktoru $g(x)$ od $f(x)$, dok je Mignotteov pristup bolji za ograničavanje nižih potencija od x. Mignotteov pristup pronalaska međe daje brzu i uniformnu među za sve koeficijente faktora $g(x)$ stupnja d. Najveći binommni koeficijent $\binom{d}{k}$ javlja se za $k = d/2$ ili $k = (d-1)/2$. Tada za $g(x)$ čiji je stupanj paran, Mignotteova međa daje uniformnu graničnu vrijednost za sve koeficijente polinoma $g(x)$, odnosno

$$|b_k| < \binom{d}{d/2}||f||$$

za sve $k = 1, \ldots, d$. Primjenom Stirlingove formule možemo izraz $\binom{d}{d/2}$ zamijeniti s nešto većom aproksimacijom $\frac{2^d}{\sqrt{(d/2)\pi}}$ pa dobivamo

$$B_u = \frac{2^d}{\sqrt{(d/2)\pi}}||f||$$

što je uniformna granična vrijednost za koeficijente faktora stupnja d polinoma $f(x)$ u $\mathbb{Z}[x]$ kada je d paran broj. Analogno dobivamo kada je d neparan.

3. Berlekampov algoritam faktorizacije

U prvom poglavlju smo pokazali da možemo ili faktorizirati bilo koji normirani polinom f iz $\mathbb{Z}[x]$ ili pokazati da je f ireducibilan odabirući dovoljno velik M i faktorizirajući modulo M. U drugom poglavlju postavili smo graničnu vrijednost B na koeficijente faktora polinoma f takvu da ukoliko faktoriziramo f modulo M, pri čemu je $M > 2B$, onda faktorizacija modulo M daje najviše jednu moguću faktorizaciju od f u $\mathbb{Z}[x]$ pa se problem faktorizacije svodi na faktorizaciju polinoma f modulo M.
Sada ćemo pokazati kako faktorizirati polinom modulo p kada je p prost broj. Algoritam koji ćemo koristiti osmislio je američki matematičar Elwyn Ralph Berlekamp 1967. godine. Njegov algoritam kombinacija je Fermatovog teorema i elementarne linearne algebre.

Neka je p prost broj i označimo s $\mathbb{F}_p$ polje od p elemenata koji su predstavnici klasa kongruencija modulo p. Elementima polja $\mathbb{F}_p$ pridružit ćemo redom brojeve $0, 1, \ldots, p-1$ koje ćemo koristiti u daljnjem tekstu kao reprezentate klasa kongruencija, odnosno ostatke dijeljenja koeficijenata početnog polinoma s p. Sada će polinom $x^3 + 2x^2 + x + 2$ iz $\mathbb{F}_3$ poprimiti oblik $[1]_3x^3 + [2]_3x^2 + [1]_3x + [2]_3$.

Pretpostavimo da želimo faktorizirati polinom $f(x)$ stupnja d u $\mathbb{F}_p[x]$. Slično kao i brojeve, polinom $f(x)$ možemo faktorizirati jednostavnom provjerom djeljivosti polinoma $f(x)$ svim polinomima stupnja najviše $d/2$ u $\mathbb{F}_p[x]$ (jer ih postoji konačno mnogo). S obzirom na nepraktičnost tog postupka i u vremenskom i u tehničkom smislu, odlučujemo primijeniti Berlekampov algoritam faktorizacije koji tvrdi da ukoliko možemo pronaći neki nekonstantni polinom $h(x)$ stupnja manjeg ili jednakog d takav da $f(x)$ dijeli $h(x)^p - h(x)$, onda dobivamo i faktorizaciju od $f(x)$.

Teorem 3.1 *Neka je dan polinom $f(x)$ iz $\mathbb{F}_p[x]$ stupnja $d > 1$ i neka je $h(x)$ iz $\mathbb{F}_p[x]$ polinom stupnja barem 1 i najviše d takav da $f(x)$ dijeli $h(x)^p - h(x)$. Tada je*

$$f(x) = (f(x), h(x)) \cdot (f(x), h(x) - 1) \cdots (f(x), h(x) - (p-1))$$

netrivijalna faktorizacija polinoma $f(x)$ u $\mathbb{F}_p[x]$.

Definicija 3.1 *Neka je $\mathbb{F}$ polje te f i g polinomi stupnja barem 1 s koeficijentima iz $\mathbb{F}$. Polinomi f i g su relativno prosti ako postoje polinomi r i s čiji su koeficijenti iz $\mathbb{F}$ takvi da vrijedi*

$$rf + sg = 1.$$

Dokaz Teorema 3.1. Pretpostavimo da $f(x)$ dijeli $h(x)^p - h(x)$. Prema Fermatovom teoremu, polinom $u^p - u$ ima p korijena u $\mathbb{F}_p[x]$ pri čemu je $u = 0, 1, 2, \ldots, p-1$. Teorem 1.1 možemo primijeniti i u slučaju polja $\mathbb{F}_p[x]$ pa slijedi da $u^p - u$ ima faktorizaciju u $\mathbb{F}_p[x]$:

$$u^p - u = u(u-1)(u-2)\cdots(u-(p-1)).$$

Ukoliko uzmemo da je $u = h(x)$, dobivamo

$$h(x)^p - h(x) = h(x)(h(x)-1)(h(x)-2)\cdots(h(x)-(p-1))$$

u $\mathbb{F}_p[x]$ pri čemu su faktori s desne strane jednadžbe u parovima relativno prosti polinomi iz $\mathbb{F}_p[x]$. Nadalje, ako su a i b relativno prosti polinomi iz $\mathbb{F}[x]$ i $\mathbb{F}$ je polje, onda za svaki polinom f u $\mathbb{F}[x]$ vrijedi

$$(f, ab) = (f, a) \cdot (f, b).$$

Induktivno, dobivamo najveći zajednički djelitelj polinoma f i barem dva u parovima relativno prosta faktora. Kako $f(x)$ dijeli $h(x)^p - h(x)$ slijedi

$$f(x) = (f(x), h(x)^p - h(x)).$$

Iz činjenice da su $h(x) - r$ i $h(x) - s$ relativno prosti za $r \neq s$ slijedi

$$\begin{aligned} f(x) &= (f(x), h(x)^p - h(x)) \\ &= (f(x), h(x)(h(x)-1)\cdots(h(x)-(p-1))) \\ &= (f(x), h(x)) \cdot (f(x), h(x)-1)\cdots(f(x), h(x)-(p-1)). \end{aligned}$$

Kako je stupanj od $h(x) - s$ manji od stupnja polinoma $f(x)$, najveći zajednički djelitelj od $f(x)$ i $h(x) - s$ ne može biti $f(x)$ niti za jedan s pa faktorizacija

$$f(x) = (f(x), h(x)) \cdot (f(x), h(x)-1)\cdots(f(x), h(x)-(p-1))$$

mora sadržavati samo polinome stupnja manjeg ili jednakog $d = deg f(x)$. Slijedi da je faktorizacija od f nužno netrivijalna.

Primjer 3.1 *Neka je $f(x) = x^5+x+1$ polinom iz $\mathbb{F}_2[x]$. Slijedi da za $h(x) = x^4+x^3+x$ $f(x)$ dijeli $(h(x))^2 - h(x) = x^8 + x^6 + x^4 + x^3 + x^2$, tj.*

$$f(x) = (f(x), h(x)) \cdot (f(x), h(x)-1)$$

što ćemo i pokazati.
Da bismo pronašli najveća dva zajednička djelitelja, koristimo Euklidov algoritam. Najprije saznajemo da je $(f(x), h(x)-1) = x^2 + x + 1$

$$x^5 + x + 1 = (x^4 + x^3 + x + 1)(x + 1) + (x^3 + x^2 + x),$$

$$x^4 + x^3 + x + 1 = (x^3 + x^2 + x)x + (x^2 + x + 1),$$

$$x^3 + x^2 + x = (x^2 + x + 1)x.$$

Pa slijedi $(x^5 + x + 1, x^4 + x^3 + x + 1) = x^2 + x + 1$. *Faktorizacija polinoma* $f(x)$ *je dakle*

$$x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1).$$

Kako bismo mogli primijeniti prethodni teorem, moramo naći polinom $h(x)$ *stupnja* e, $1 \leq e \leq d$, *takav da* $f(x)$ *dijeli* $h(x)^p - h(x)$. *Do njega dolazimo postavljajući i rješavajući sustav linearnih jednadžbi za koeficijente od* $h(x)$. *Neka je*

$$h(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{d-1} x^{d-1}$$

pri čemu su $b_0, \ldots, b_{d-1}$ *iz* $\mathbb{F}_p$ *koeficijenti koje želimo odrediti. Također vrijedi*

$$h(x)^p = b_0^p + b_1^p x^p + b_2^p x^{2p} + \ldots + b_{d-1}^p x^{p(d-1)}.$$

Iz Fermatovog teorema slijedi $b^p = b$ *za sve* b *iz* $\mathbb{F}_p$ *te*

$$h(x)^p = b_0 + b_1 x^p + b_2 x^{2p} + \ldots + b_{d-1} x^{p(d-1)} = g(x^p).$$

Da bismo našli ostatak pri dijeljenju polinoma $f(x)$ *polinomom* $h(x)^p$, *pronalazimo* $x^{ip} \pmod{f(x)}$ *za* $i = 0, 1, \ldots, d-1$. *Pišemo*

$$x^{ip} = f(x) q_i(x) + r_i(x)$$

i vrijedi $\deg r_i(x) < d = \deg f(x)$. *Iz toga dobivamo*

$$x^{ip} = r_i(x) \pmod{f(x)}$$

pa uvrštavajući u

$$h(x)^p = b_0 + b_1 x^p + b_2 x^{2p} + \ldots + b_{d-1} x^{p(d-1)} = g(x^p)$$

slijedi

$$h(x)^p = (b_0 r_0(x) + b_1 r_1(x) + \ldots + b_{d-1} r_{d-1}(x)) \mod f(x).$$

Tada $f(x)$ *dijeli* $h(x)^p - h(x)$ *ako i samo ako* $f(x)$ *dijeli polinom*

$$b_0 r_0(x) + b_1 r_1(x) + \ldots + b_{d-1} r_{d-1}(x) - [b_0 + b_1 x + \ldots + b_{d-1} x^{d-1}]. \tag{3.2}$$

No, taj polinom je stupnja manjeg ili jednakog $d-1$ *pa je djeljiv polinomom* $f(x)$ *ako i samo ako nulpolinom u* $\mathbb{F}_p[x]$. *To nam je potreban uvjet za odredivanje koeficijenata* $b_0, \ldots, b_{d-1}$ *polinoma* $h(x)$. *Koeficijenti* $b_0, \ldots, b_{d-1}$ *moraju zadovoljavati*

$$b_0 r_0(x) + b_1 r_1(x) + \ldots + b_{d-1} r_{d-1}(x) - [b_0 + b_1 x + \ldots + b_{d-1} x^{d-1}] = 0.$$

Uzmemo li koeficijente uz sve $1, x, x^2, \ldots, x^{d-1}$ (3.2), *dobivamo* d *linearnih jednadžbi s* d *nepoznanica* $b_0, \ldots, b_{d-1}$ *gdje su koeficijenti uz* $b_j, 0 \leq j \leq d-1$ *koeficijenti uz polinome* $r_j(x)$. *Rješavanjem sustava dobivamo tražene koeficijente polinoma* $h(x)$.

Primjer 3.2 *Neka je* $f(x) = x^5 + x + 1$ *polinom iz* $\mathbb{F}_2[x]$. *Pronađimo polinome* $r_i(x)$ *koji su ostatci dijeljenja polinoma* $f(x)$ *s* x^{2i} *za* $i = 0, 1, \ldots, 4$.

$$r_0(x) = 1$$

$$r_1(x) = x^2$$

$$r_2(x) = x^4$$

Za $r_3(x) : x^6 = xf(x) + (x^2 + x)$, *pa je* $r_3(x) = x^2 + x$. *Isto tako, za* $r_4(x) : x^8 = x^3 f(x) + (x^4 + x^3)$, *pa je* $r_4(x) = x^4 + x^3$. *Tada jednadžba* (3.2) *postaje*

$$0 = b_0 + b_1x^2 + b_2x^4 + b_3(x^2 + x) + b_4(x^4 + x^3) - (b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4).$$

Uzimajući koeficijente uz sve $1, x, x^2, x^3, x^4$ *dobivamo redom:*

$$\begin{aligned} 0 &= b_0 - b_0 \\ 0 &= b_3 - b_1 \\ 0 &= b_1 + b_3 - b_2 \\ 0 &= b_4 - b_3 \\ 0 &= b_2 + b_4 - b_4. \end{aligned}$$

Sada lako vidimo da je $b_2 = 0$, $b_1 = b_3 = b_4$ *i* b_0 *proizvoljan. Kako bi* $h(x)$ *bio stupnja većeg ili jednakog* 1, *biramo* $b_1 = b_3 = b_4 = 1$. *Tada za* $h(x)$ *imamo dvije opcije, ovisno uzimamo li* $b_0 = 0$ *ili* $b_0 = 1$*:*

$$g_0(x) = x^4 + x^3 + x$$

i

$$g_1(x) = x^4 + x^3 + x + 1 = g_0(x) + 1.$$

Slijedi,

$$\begin{aligned} f(x) &= (f(x), g_0(x)) \cdot (f(x), g_1(x)) \\ &= (x^3 + x^2 + 1)(x^2 + x + 1). \end{aligned}$$

Zgodno je jednadžbu (3.2) *zapisati u obliku matrične forme. Neka je* I *jedinična matrica* $d \times d$ *dimenzije i neka je* $r_i(x) = r_{i,0} + r_{i,1}x + \ldots + r_{i,d-1}x^{d-1}$ *za svaki* i. *Neka je još* Q *matrica dimenzije* $d \times d$ *čiji su redovi koeficijenti polinoma* $r_0, \ldots, r_{d-1}$. *Tada je lako pokazati da komponente vektora* $b = (b_0, b_1, \ldots, b_{d-1})$ *daju rješenje jednadžbe* (3.2) *ako i samo ako*

$$b(Q - I) = 0 = (0, 0, \ldots, 0). \tag{3.3}$$

Primjenom Teorema 1.2 *dobivamo sljedeći teorem.*

Teorem 3.2 (Berlekampov algoritam faktorizacije) *Neka je* $f(x)$ *polinom iz* $\mathbb{F}_p[x]$ *stupnja* d. *Neka je* Q *matrica reda* $d \times d$ *čiji su retci vektori koeficijenata polinoma*

$r_i(x) \equiv x^{pi} \pmod{f(x)}$ *za sve* $i = 0, 1, \ldots, d-1$. *Neka je* $b = (b_0, b_1, \ldots, b_{d-1})$ *rješenje od*

$$b(Q - I) = 0$$

odnosno jednadžbe (3.2) *i neka je*

$$h(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{d-1} x^{d-1}.$$

Ako je $h(x)$ *stupnja barem* 1, *onda za neki* s *iz* $\mathbb{F}_p$, $h(x) - s$ *i* $f(x)$ *imaju zajednički faktor stupnja barem* 1.

Primjer 3.3 *Neka je* $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ *polinom iz* $\mathbb{F}_2[x]$ *stupnja* 6. *Kako bismo našli matricu* Q, *dijelimo polinom* $f(x)$ *s* x^{2i}, *za svaki* $i = 0, 1, \ldots, 5$ *da bismo dobili odgovarajući* $r_i(x)$*:*

$$\begin{aligned}
x^0 &= f(x) \cdot 0 + 1 \Rightarrow r_0(x) = 1,\\
x^2 &= f(x) \cdot 0 + x^2 \Rightarrow r_1(x) = x^2,\\
x^4 &= f(x) \cdot 0 + x^4 \Rightarrow r_2(x) = x^4,\\
x^6 &= f(x) \cdot 1 + x^5 + x^4 + x^3 + x^2 + x + 1 \Rightarrow r_3(x) = x^5 + x^4 + x^3 + x^2 + x + 1,\\
x^8 &= f(x)(x^2 + x) + x \Rightarrow r_4(x) = x,\\
x^{10} &= f(x)(x^4 + x^3) + x^3 \Rightarrow r_5(x) = x^3,
\end{aligned}$$

Koeficijenti $r_0(x), \ldots, r_5(x)$ *su retci matrice* Q *koja je sada oblika*

$$Q = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0\\
1 & 1 & 1 & 1 & 1 & 1\\
0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}$$

Da bismo našli

$$h(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 + b_5 x^5,$$

rješavamo

$$b(Q - I) = 0$$

odnosno

$$\begin{aligned}
b_3 &= 0\\
b_1 + b_3 + b_4 &= 0\\
b_1 + b_2 + b_3 &= 0\\
b_5 &= 0\\
b_2 + b_3 + b_4 &= 0\\
b_3 + b_5 &= 0.
\end{aligned}$$

Dobivamo $b_3 = b_5 = 0$ *i* $b_1 = b_2 = b_4$. *Jedina rješenja za koja vrijedi deg* $h(x) \geq 1$ *su* $h(x) = x^4 + x^1 + x + b_0$ *gdje je* b_0 *jednak* 0 *ili* 1. *Bez obzira na izbor* b_0 *dobivamo*

$$h(x)^2 - h(x) = x^8 + x = f(x)(x^2 + x).$$

Dakle,

$$f(x) = (f(x), x^4 + x^1 + x) \cdot (f(x), x^4 + x^1 + x + 1).$$

Primjenom Euklidovog algoritma, za prvi faktor dobivamo $x^3 + x + 1$, *a za desni* $x^3 + x^2 + 1$. *Oba polinoma su ireducibilna pa je faktorizacija od* $f(x)$ *u* $\mathbb{F}_2[x]$*:*

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1).$$

Prebrojavanje ireducibilnih faktora. Neka je $f(x)$ polinom stupnja d i s $V = \mathbb{F}_p^d$ označimo vektorski prostor nad poljem $\mathbb{F}_p$ koji se sastoji od d-torki elemenata iz tog polja. Nadalje, neka je N skup uređenih d-torki $b = (b_0, b_1, \ldots, b_{d-1})$ u prostoru $\mathbb{F}_p^d$ za koji vrijedi $b(Q - I) = 0$. Tada je N jezgra matrice $Q - I$ te potprostor od V. Neka je $\{v_1, v_2, \ldots, v_g\}$ baza od N. Tada je g dimenzija prostora N. Prostor N sadrži vektore $(a, 0, \ldots 0)$ za bilo koji a iz $\mathbb{F}_p$ jer je vektorska reprezentacija konstantnog polinoma $h(x) = a$, a $h(x)^p - h(x) = a^p - a = 0$ za bilo koji a iz $\mathbb{F}_p$ prema Fermatovom teoremu. Prema tome, dimenzija prostora je jednaka barem jedan. Da bismo faktorizirali $f(x)$, moramo naći polinom $h(x)$ stupnja većeg ili jednakog 1. To znači da moramo pronaći vektor $b = (b_1, b_2, \ldots, b_{d-1})$ iz N pri čemu je barem jedan b_i za neki $1 \leq i \leq d - 1$ različit od 0. Ako takav vektor b postoji, tada postoje vektori iz N koji nisu oblika $(a, 0, \ldots, 0)$ pa je dimenzija prostora N barem 2. Iz toga pretpostavljamo da je $f(x)$ produkt različitih ireducibilnih polinoma.

Definicija 3.2 *Za polinom* $f(x)$ *u polju* $\mathbb{F}$ *kažemo da je kvadratno slobodan ako se može zapisati kao umnožak različitih ireducibilnih polinoma iz* $\mathbb{F}$.

Teorem 3.3 *Neka je* $f(x)$ *iz* $\mathbb{F}_p$ *kvadratno slobodan polinom. Tada vrijedi*
a) Dimenzija jezgre od $Q - I$ *jednaka je broju ireducibilnih faktora polinoma* $f(x)$.
b) $f(x)$ *je ireducibilan u* $\mathbb{F}_p$ *ako i samo ako je jezgra* N *od* $Q - I$ *dimenzije jedan.*

Dimenziju jezgre N od $Q - I$ možemo dobiti na sljedeći način. Kako je $Q - I$ matrica dimenzije $d \times d$, dimenzija jezgre jednaka je d umanjeno za rang po retcima ili stupcima od $Q - I$. Rang po stupcima matrice $Q - I$ jednak je broju nenul stupaca nakon izvođenja elementarnih transformacija nad stupcima kako bi poništili međusobno linearno zavisne stupce, a matricu zapisali u obliku nula i jedinica. Analogno vrijedi i za rang po retcima. Postupak možemo ilustrirati na primjeru matrice E od ranije

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Kako matrica E ima četiri nenul stupca, zaključujemo da je dimenzija jezgre jednaka $6-2=4$. Dodatno, jezgru možemo odrediti rješavajući jednadžbu $bE=0$ s obzirom na to da izvođenje elementarnih operacija na stupcima matrice $Q-I$ ne mijenja prostor rješenja jednadžbe $b(Q-I)=0$. Rješenja b jednadžbe $bE=0$ rješenja su jednadžbi

$$\begin{aligned} b_1+b_4&=0,\\ b_2+b_4&=0,\\ b_3&=0,\\ b_5&=0. \end{aligned}$$

Dakle vektor b možemo zapisati u obliku

$$\begin{aligned} b&=(b_0,b_1,b_2,b_3,b_4,b_5)\\ &=(b_0,b_4,b_4,0,b_4,0)\\ &=b_0(1,0,0,0,0,0)+b_4(0,1,1,0,1,0), \end{aligned}$$

pri čemu su b_0 i b_4 proizvoljni.

Dokaz teorema 3.4. Neka je $f(x)$ polinom stupnja d koji se može zapisati kao produkt g različitih ireducibilnih polinoma, odnosno $f(x)=p_1(x)p_2\cdots p_g(x)$, pri čemu je svaki od polinoma p_i ireducibilan. Konstruirajmo polinome $h(x)$ takve da $f(x)$ dijeli $h(x)^p-h(x)$. Za svaki vektor $s=(s_1,s_2,\ldots,s_g)$ čiji su elementi iz $\mathbb{F}_p$ koristimo Teorem o interpolaciji kako bi dobili jedinstveni polinom $h_s(x)$ stupnja manjeg ili jednakog d takav da

$$h_s(x)\equiv s_i \pmod{p_i(x)}$$

za svaki $i=1,2,\ldots,g$. Iz toga slijedi da p_i dijeli $h_s(x)-s_i$ pa $p_i(x)$ dijeli

$$\begin{aligned} &h_s(x)\cdot(h_s(x)-1)\cdots(h_s(x)-(p-1))\\ &=\prod_{r=1}^{g}(h_s(x)-r)=h_s(x)^p-h_s(x). \end{aligned}$$

Dakle, $f(x)$ dijeli $h(x)^p-h(x)$. Definiramo funkciju γ s $\mathbb{F}_p^g$ u skup $\mathcal{P}$ svih polinoma $h(x)$ takvih da $f(x)$ dijeli $h(x)^p-h(x)$. Za dani polinom $h(x)$ iz $\mathcal{P}$ $f(x)$ dijeli $h(x)^p-h(x)$ i za svaki $\leq i\leq g$ ireducibilni faktor $p_i(x)$ polinoma $f(x)$ dijeli

$$h(x)^p-h(x)=h(x)\cdot(h(x)-1)\cdots(h(x)-(p-1)).$$

Kako su polinomi $h(x),h(x)-1,\ldots,h(x)-(p-1)$ u parovima relativno prosti i svaki $p_i(x)$ je ireducibilan, tada svaki $p_i(x)$ dijeli $h(x)-s_i$ za $1\leq s_i\leq p-1$. Osim toga, vektor $s=(s_1,s_2,\ldots,s_g)$ u $\mathbb{F}_p^g$ i za svaki $i=1,\ldots,g$ vrijedi $h(x)\equiv s_i \pmod{p_i(x)}$. Slijedi $h(x)=h_s(x)$ i γ je injektivno preslikavanje. Ako je $h(x)=b_0+b_1x+\ldots+b_{d-1}x^{d-1}$, onda je $h(x)$ u γ ako i samo ako je vektor koeficijenata $(b_0,b_1,\ldots,b_{d-1})$ jezgra N od

$Q - I$. Stoga je kardinalan broj od N jednak kardinalnom broju od γ, odnosno jednak kardinalnom broju od $\mathbb{F}_p^g = p^g$, gdje je g broj različitih ireducibilnih faktora od $f(x)$. Očito je dimenzija od N jednaka g.
Tvrdnja b) slijedi direktno: jezgra N od $Q - I$ je jednodimenzionalna ako i samo ako je $f(x) = p(x)$ ireducibilan polinom.

Primjer 3.4 *Koliko ireducibilnih faktora iz* $\mathbb{F}_3[x]$ *dijeli polinom*

$$f(x) = x^5 + 2x^4 + x^3 + x^2 + 2?$$

Najprije računamo $Q - I$*:*

$$\begin{aligned}
1 &= f(x) \cdot 0 + 1, \\
x^3 &= f(x) \cdot 0 + x^3, \\
x^6 &= f(x)(x+1) + (1 + x + 2x^2 + x^3), \\
x^9 &= f(x)(x^4 + x^3 + x) + x, \\
x^{12} &= f(x)(x^7 + x^6 + x^4) + x^4.
\end{aligned}$$

Ako uzmemo da su koeficijenti uz potencije od x *u rastućem redoslijedu retci matrice* Q*, dobivamo*

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$Q - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Nakon elementarnih transformacija nad retcima i stupcima dobivamo matricu

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Dakle matrica $Q - I = E$ *je ranga* 2*, pa je jezgra od* E *dimenzije* 3*. Slijedi da* $f(x)$ *ima tri različita ireducibilna faktora, a vektori* b *koji zadovoljavaju jednakost* $bE = 0$ *su oblika*

$$b = (b_0, b_1, b_2, b_3, b_4) = (b_0, b_3, 0, b_3, b_4)$$

gdje su b_0*,* b_3 *i* b_4 *proizvoljni. Prema tome* $f(x)$ *dijeli* $h(x)^3 - h(x)$ *pri čemu je* $h(x) = x^4, h(x) = x + x^3, h(x) = 1$ *ili bilo koja* $\mathbb{F}_3$*-linearna kombinacija tih polinoma.*

4. Henselova metoda faktorizacije

Uz danu graničnu vrijednost za koeficijente u faktorima polinoma $f(x)$ iz $\mathbb{Z}[x]$ možemo naći faktorizaciju od $f(x)$ modulo M za $M \geq 2B$. Bilo koji faktor od f modulo M odgovara najviše jednom mogućem faktoru od f iz $\mathbb{Z}[x]$ jer će postojati samo jedan polinom u $\mathbb{Z}[x]$ koji će zadovoljavati graničnu vrijednost za koeficijente i smanjiti na dani faktor od f modulo M.
Želimo naći faktorizaciju od $f \pmod M$ gdje je M velik. Postoji dva načina na koji to možemo provesti. Prvi način je naći sve proste brojeve $p > 2B$ i primijeniti Berlekampov algoritam za faktorizaciju f modulo p. Ukoliko imamo sreće, f će imati samo nekoliko ireducibilnih faktora modulo p pa će biti samo nekoliko opcija za faktorizaciju u $\mathbb{Z}[x]$.
Postoji i alternativna metoda za ponalazak malih prostih brojeva p takvih da $f \mod p$ ima faktorizaciju u nekoliko različitih ireducibilnih faktora. Nakon toga možemo podići faktorizaciju modulo p na jedinstvenu faktorizaciju modulo p^{2^e} za e dovoljno velik da vrijedi $p^{2^e} > 2B$. Tu metodu razvio je njemački matematičar Hans Julius Zassenhaus te ju nazivamo Henselova metoda faktorizacije.

Definicija relativno prostih polinoma s koeficijentima iz komutativnog prstena R analogna je Definiciji 3.1. Ako je $R = \mathbb{Z}/m\mathbb{Z}$ te f i g polinomi s cjelobrojnim koeficijentima, kažemo da su f i g relativno prosti modulo m ako su slike od f i g u $\mathbb{Z}/m\mathbb{Z}[x]$ relativno proste, odnosno, ako postoje polinomi r i s u $\mathbb{Z}[x]$ takvi da $fr + gs \equiv 1 \pmod m$.

Propozicija 4.1 *Neka su g i h normirani relativno prosti polinomi iz $R[x]$. Tada za svaki k iz $R[x]$ postoje polinomi a i b u $R[x]$ takvi da je $ag + bh = k$.*
Ako je $deg(k) < deg(fg)$, onda možemo odabrati a i b takve da $deg(a) < deg(h)$, $deg(b) < deg(g)$.

Dokaz. Kako su g i h relativno prosti, postoje polinomi r i s takvi da $dr + hs = 1$. Iz toga slijedi $grk + hsk = k$. Pretpostavimo da je $deg(k) < deg(fg)$ i da postoje a, b iz $R[x]$ takvi da je $ag + bh = k$ i $deg(b) \geq deg(g)$. Tada je $b = gq + s$ gdje je $deg(s) < deg(g)$ i vrijedi

$$aq + (gq + s)h = k.$$

Za $(a + gh)g + sh = k$ možemo uvesti supstituciju $r = a + gh$ te dobivamo $rg + sh = k$.
Iz $deg(s) < deg(g)$ dobivamo $deg(sh) < deg(gh)$ i $deg(k) < deg(gh)$.
Slijedi $deg(rg) < deg(gh)$, a kako je g normiran, time i $deg(r) < deg(h)$.

Teorem 4.1 *Neka je f normiran polinom iz $\mathbb{Z}[x]$. Pretpostavimo da postoje normirani polinomi g_1, h_1 u $\mathbb{Z}[x]$ takvi da su g_1 i h_1 relativno prosti modulo m i $f = g_1 h_1 \pmod m$. Tada postoje jedinstveni normirani polinomi g_2 i h_2 takvi da je*

$$g_2 \equiv g_1 \pmod m$$

$$h_2 \equiv h_1 \pmod{m}$$

g_2 i h_2 su relativno prosti modulo m^2 i

$$f \equiv g_2 h_2 \pmod{m^2}.$$

Dokaz. Konstruirajmo g_2 i h_2, neka je

$$g_2 = g_1 + mb$$

i

$$h_2 = h_1 + mc$$

pri čemu su polinomi b i c iz $\mathbb{Z}[x]$ takvi da $deg(b) < deg(g_1), deg(c) < deg(h_1)$, a koje moramo pronaći. Primijetimo da je $f \equiv g_1 h_1 \pmod{m}$, te $f = g_1 h_1 + mk$ za neki polinom k iz $\mathbb{Z}[x]$. Iz normiranosti polinoma f, h_1 i g_1 slijedi $deg(k) < deg(g_1 h_1)$. Tada vrijedi

$$\begin{aligned} g_2 h_2 - f &= (g_1 + mb)(h_1 + mc) - (g_1 h_1 + mk) \\ &= g_1 h_1 + m g_1 c + m h_1 b + m^2 bc - g_1 h_1 - mk. \end{aligned}$$

Da bi lijeva strana bila kongruentna 0 modulo m^2, trebamo

$$m(g_1 c + h_1 b - k) \equiv 0 \pmod{m^2}$$

ili

$$g_1 c + h_1 b - k \equiv 0$$

no, s obzirom da su g_1 i h_1 relativno prosti modulo m, postoje polinomi c i b takvi da

$$g_1 c + h_1 b \equiv k \pmod{m}.$$

Uz uvjet $deg(k) < deg(g_1 h_1)$, možemo odabrati polinome c i b takve da vrijedi $deg(c) < deg(h_1)$ i $deg(b) < deg(g_1)$. Ovisno o odabiru polinoma c i b dobivamo normirane polinome $g_2 = g_1 + mb$ i $h_2 = h_1 + mc$ koji zadovoljavaju $f \equiv g_2 h_2 \pmod{m^2}$.
Još trebamo pokazati da su g_2 i h_2 relativno prosti modulo m^2. Tražimo polinome r_2 i s_2 takve da je $r_2 g_2 + s_2 h_2 \equiv 1 \pmod{m^2}$. Kako su g_1 i h_1 relativno prosti, postoje polinomi r_1 i s_1 takvi da $r_1 g_1 + s_1 h_1 = 1 + mz$ za neki polinom z.
Pišemo $r_2 = r_1 + mw, s_2 = s_1 + my$, pri čemu su w i y nepoznati polinomi iz $\mathbb{Z}[x]$. To sada uvrštavamo u kongruenciju

$$r_2 g_2 + s_2 h_2 \equiv 1 \pmod{m^2}.$$

Dobivamo

$$\begin{aligned} &(r_1 + mw)(g_1 + mb) + (s_1 + my)(h_1 + mc) \\ &\equiv r_1 g_1 + m w g_1 + m r_1 b + s_1 h_1 + m s_1 c + m y h_1 \pmod{m^2} \\ &\equiv 1 + mz + m(w g_1 + r_1 b + s_1 c + y h_1) \pmod{m^2}. \end{aligned}$$

Da bi zadnji izraz bio kongruentan 1 modulo m^2, moramo pronaći polinome w i y takve da

$$wg_1 + yh_1 \equiv -z - r_1 b - s_1 c \pmod{m}.$$

Iz činjenice da su g_1 i h_1 relativno prosti modulo m slijedi da možemo naći takve w i y.
Dakle, postoje $r_2 = r_1 + mw$ i $s_2 = s_1 + my$ za koje vrijedi $r_2 g_2 + s_2 h_2 \equiv 1 \pmod{m^2}$ i prema tome g_2 i h_2 su relativno prosti modulo m^2.

Primjer 4.1 *Neka je* $f(x) = x^4 + 23x^3 - 15x^2 + 17x - 7$. *Tada je*

$$f(x) \equiv x^4 + 2x^3 + 3x^2 + 2x + 2 = (x^2 + 1)(x^2 + 2x + 2) \pmod{3}$$

odnosno, $f(x)$ *se može zapisati kao produkt dva različita polinoma koji su ireducibilni modulo* 3, *a time i relativno prosti modulo* 3. *Sada želimo faktorizirati* $f(x)$ *modulo* 9. *Uvedimo*

$$g_1 = x^2 + 1, h_1 = x^2 + 2x + 2$$

te

$$g_2 = g_1 + 3b = (x^2 + 1) + 3b,$$

$$h_2 = h_1 + 3c = (x^2 + 2x + 2),$$

dok su b *i* c *neki polinomi za koje vrijedi* $deg(c) < deg(h_1), deg(b) < deg(g_1)$. *Tada*

$$g_2 h_2 \equiv (x^2 + 1)(x^2 + 2x + 2) + 3c(x^2 + 1) + 3b(x^2 + 2x + 2) \pmod{9}.$$

Da bismo došli do b *i* c, *postavljamo kongruenciju*

$$f \equiv g_2 h_2 \pmod{9}$$

i metodom supstitucije dolazimo do

$$x^4+23x^3-15x^2+17x-7 \equiv (x^4+2x^3+3x^2+2x+2)+3c(x^2+1)+3b(x^2+2x+2) \pmod{9}$$

ili

$$21x^3 - 18x^2 + 15x - 9 \equiv 3c(x^2 + 1) + 3b(x^2 + 2x + 2) \pmod{9}.$$

Podijelimo li sve s 3, *dobivamo*

$$7x^3 - 6x^2 + 5x - 3 \equiv c(x^2 + 1) + b(x^2 + 2x + 2) \pmod{3}$$

koju znamo da možemo riješiti za polinome b *i* c *(čiji je stupanj manji ili jednak* 2*) s obzirom da su* $x^2 + 1$ *i* $x^2 + 2x + 2$ *relativno prosti modulo* 3. *Neka je* $b = rx + s$ *i* $c = tx + v$. *Tada*

$$7x^3 - 6x^2 + 5x - 3 \equiv (tx + v)(x^2 + 1) + (rx + s)(x^2 + 2x + 2) \pmod{3}.$$

Izjednačavanjem koeficijenata uz iste potencije s obje strane kongruencije, dobivamo

$$\begin{aligned} -3 &\equiv v + 2s \pmod 3 \\ 5 &\equiv t + 2r + 2s \pmod 3 \\ -6 &\equiv v + 2r + s \pmod 3 \\ 7 &\equiv t + r \pmod 3. \end{aligned}$$

Očito je $r = t = 2, s = v = 1$ *jedinstveno rješenje jednadžbe pa dobivamo*

$$b = 2x + 1, c = 2x + 1.$$

Slijedi

$$g_2 = g_1 + 3b \equiv (x^2 + 1) + 3(2x + 1) \equiv x^2 + 6x + 4$$

$$h_2 = h_1 + 3c \equiv (x^2 + 2x + 2) + 3(2x + 1) \equiv x^2 + 8x + 5.$$

Lako je provjeriti da vrijedi

$$\begin{aligned} (x^2 + 6x + 4)(x^2 + 8x + 5) &\equiv x^4 + 14x^3 + 57x^2 + 62x + 20 \\ &\equiv x^4 + 23x^3 - 15x^2 + 17x - 7 \\ &\equiv f(x) \pmod 9. \end{aligned}$$

Na sličan način dolazimo i do faktorizacije modulo $9^2, 81^2$, *itd. dok ne pređemo graničnu vrijednost za koeficijente nekog faktora stupnja* 2 *polinoma* $f(x)$. *U tom trenutku ili nalazimo faktorizaciju od* f *u* $\mathbb{Z}[x]$ *ili pokazujemo da ne postoji.*
Primijetimo da je $||f|| = (1^2+23^2+15^2+17^2+7^2)^{1/2} = \sqrt{1093} = 33.06$ *pa bi korištenjem Mignotteove granice bilo dovoljno naći faktorizaciju* f *modulo* 81 *kako bismo odredili faktorizaciju od* $f(x)$ *ili pokazali da je ireducibilan. U ovom primjeru dobivamo da je* $f(x)$ *ireducibilan modulo* 5 *pa time i ireducibilan u* $\mathbb{Q}[x]$.

Literatura

[1] Lindsay N. Childs, A Concrete Introduction to Higher Algebra, Third Edition, 2009.