SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mia Matić

ALGORITMI ZA FAKTORIZACIJU POLINOMA

Diplomski rad

Voditelj rada:
prof.dr.sc Andrej Dujella

Zagreb, rujan, 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Najljepša hvala prof. dr. sc. Andreju Dujelli na svestranoj pomoći i strpljivosti tijekom pisanja ovog diplomskog rada.

Zahvaljujem se svojoj obitelji i prijateljima koji su bili uz mene tijekom studija.

Ovaj diplomski rad posvećujem svojoj majci, Ljiljani Matić.

Sadržaj

Uvod

Cilj ovog diplomskog rada je opisati tri osnovna algoritma za faktorizaciju cjelobrojnih polinoma s jednom varijablom. Jedan od njih je klasičan, a ostala dva su moderna. Diplomski rad se sastoji od četiri poglavlja. Prvo poglavlje čine osnovni teoremi i svojstva za polinome pisani prema [3]. U drugom poglavlju prema [1] i [4] opisan je Kroneckerov algoritam, ujedno i prvi algoritam za faktorizaciju polinoma. Osmislio ga je F. T. Schubert 1793. godine, a doradio L. Kronecker 1882. godine. Treće poglavlje posvećeno je Berlekampovom algoritmu te je pisano prema [4]. Berlekampov algoritam je nastao 1969. godine, a zasluge pripadaju matematičarima E. R. Berlekampu i H. Zassenhausu. Algoritam, kojeg su 1982. godine otkrili A. K. Lenstra, H. W. Lenstra i L. Lovász naziva se LLL-algoritam i opisan je u četvrtom poglavlju prema [2] i [5]. Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Polinomi

1.1 Osnovno o polinomima

Definicija 1.1.1. *Funkcija $f : \mathbb{R} \to \mathbb{R}$, kojoj je domena i kodomena $\mathbb{R}$, zadana formulom*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \tag{1.1}$$

gdje su $a_0, a_1, .., a_n$ realni brojevi, $a_n \neq 0$, n prirodni broj, zove se polinom n-tog stupnja. Brojevi $a_0, a_1, .., a_n$ zovu se koeficijenti polinoma f. Prirodni broj n zove se stupanj polinoma f. Koeficijent a_n zove se vodeći ili najstariji koeficijent polinoma f, a koeficijent a_0 zove se slobodni član polinoma f. Ako je $a_n = 1$, kažemo da je f normiran polinom. Zapis (1.1) zove se kanonski zapis polinoma f. Ako je $a_0 = a_1 = ... = a_n = 0$, onda se f zove nulpolinom. Nulpolinom je jedini polinom za koji se stupanj ne definira i pišemo $f = 0$. Polinom f, zadan formulom $f(x) = a, a \in \mathbb{R} \setminus \{0\}$, zove se konstantni polinom ili kraće konstanta.

Teorem 1.1.2. *Polinomi*

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

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0,$$

pri čemu su $a_n \neq 0$, $b_m \neq 0$, su jednaki ako i samo ako vrijedi: $m = n$ i $a_i = b_i$,
$i = 0, 1, \ldots, n$.
(dokaz [3, str. 9])

Definicija 1.1.3. *Neka su f i g dva polinoma iz $\mathbb{R}[x]$, $f \neq 0$, $g \neq 0$. Polinom h zove se zajednički djelitelj polinoma f i g ako su f i g djeljivi sa h. Za zajednički djelitelj d polinoma f i g kažemo da je najveći zajednički djelitelj od f i g ako je d djeljiv sa svakim zajedničkim djeliteljem od f i g.*

Definicija 1.1.4. *Jednadžba oblika*

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0, \tag{1.2}$$

pri čemu su $a_n \neq 0$, $a_i \in \mathbb{C}$, zove se algebarska jednadžba n-tog stupnja. Brojevi $a_0, a_1, \ldots, a_n$ zovu se koeficijenti jednadžbe, a_n se zove najstariji koeficijent, a a_0 slobodni član te jednadžbe. Ako je $a_n = 1$, onda za jednadžbu (1.2) kažemo da je normirana. Jednadžbi (1.2) možemo pridružiti polinom

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

Svaki korijen jednadžbe (1.2) je nultočka polinoma f i obrnuto, k-struku nultočku polinoma f nazivamo k-strukim korijenom pripadne algebarske jednadžbe.

Teorem 1.1.5. *Ako je $\alpha = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0, \gcd(p, q) = 1$ racionalan korijen jednadžbe s cjelobrojnim koeficijentima*

$$a_n x^n + a_{n-1} x^{n-1} + +a_1 + a_0 = 0,$$

pri čemu je $a_n \neq 0$, onda je p djelitelj slobodnog člana a_0 i q je djelitelj vodećeg koeficijenta a_n. (dokaz [3, str. 47])

1.2 Egzistencija algoritma za faktorizaciju polinoma

Kao što je naglašeno u uvodu, ovaj diplomski rad odnosit će se na polinome s cjelobrojnim koeficijentima s jednom varijablom. Prije nego što objasnimo koja svojstva polinomi moraju imati da bi na njih primijenili algoritme, potrebno je definirati visinu polinoma, Mahlerovu mjeru i iskazati Mahlerovu lemu.

Definicija 1.2.1. *Neka je polinom f oblika*

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

Tada je

$$H(f) = \max(|a_n|, |a_{n-1}|, ..., |a_0|)$$

visina polinoma f.

Definicija 1.2.2. *Ako je visina $H(P)$ polinoma P s kompleksnim koeficijentima*

$$P(x) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 = a_n (X - \alpha_1)...(X - \alpha_n)$$

različita od nule, tada definiramo Mahlerovu mjeru polinoma P kao

$$M(P) = |a_n| \prod_{i=1}^{n} \{\max 1, |\alpha_i|\}.$$

Lema 1.2.3. *Neka je P nenul polinom s kompleksnim koeficijentima stupnja n. Tada vrijedi:*

$$\binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} H(P) \leq M(P) \leq \sqrt{n+1} \cdot H(P), \tag{1.3}$$

pri čemu je H(P) visina polinoma P, a M(P) Mahlerova mjera polinoma P.

Neka je F polinom s cjelobrojnim koeficijentima stupnja $d \geq 2$ i neka je H visina polinoma F. Polinom F je oblika

$$F(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0,$$

pri čemu su $a_n, a_{n-1}, ..., a_0$ relativno prosti. Ako je polinom F reducibilan nad $\mathbb{Z}$, tada postoji polinom $G \in \mathbb{Z}[x]$, pri čemu je G stupnja d' tako da vrijedi $0 < d' \leq d/2$ i polinom G dijeli polinom F. Neka je $F = G \cdot J$. Iz nejednakosti $2^{d'} > \binom{d'}{\lfloor \frac{d'}{2} \rfloor}$, nejednakosti (1.3) te multiplikativnosti Mahlerove mjere slijedi:

$$2^{-d'} \cdot H(G) \leq \binom{d'}{\lfloor \frac{d'}{2} \rfloor}^{-1} \cdot H(G) \leq M(G) \leq M(G) \cdot M(J) \leq M(F) \leq \sqrt{d+1} \cdot H(F).$$

Dakle, imamo

$$H(G) \leq \sqrt{d+1} \cdot 2^{d'} \cdot H(F) \leq \sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F). \tag{1.4}$$

Kako bi pronašli faktor G moramo provjeriti sve polinome koji imaju stupanj najviše $\frac{d}{2}$ i čija je visina omeđena sa $\sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F)$. Koeficijenata polinoma ima približno $\frac{d}{2}$. Budući da je visina polinoma G nije veća od $\sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F)$ to znači da najveća apsolutna vrijednost koeficijenata polinoma od G jednaka $\sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F)$. Kada uzmemo u obzir sve negativne i pozitivne brojeve čija apsolutna vrijednost ne prelazi $\sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F)$, dobivamo da svaki od $\frac{d}{2}$ koeficijenata može poprimiti $2 \cdot \sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F)$. Iz ovog slijedi da je ukupan broj mogućnosti jednak

$$2 \cdot \sqrt{d+1} \cdot 2^{\frac{d}{2}} \cdot H(F)^{\frac{d}{2}} = (2H(F))^{\frac{d}{2}} \cdot (d+1)^{\frac{d}{4}} \cdot 2^{\frac{d}{4}}.$$

Možemo primijetiti da takvih polinoma ima mnogo te da algoritam prestaje biti praktičan za npr. $d \geq 6$.

Poglavlje 2

Kroneckerov algoritam

Kao što je naglašeno u uvodu, u ovom diplomskom radu bavit ćemo se polinomima s cjelobrojnim koeficijentima s jednom varijablom. Kroneckerov algoritam se bazira na činjenici da za bilo koji cijeli broj a , vrijednost $G(a)$ dijeli broj $F(a)$, pri čemu je G bilo koji faktor polinoma F. Budući da $\frac{d}{2} + 1 = \frac{d+2}{2}$ vrijednosti određuju polinom G stupnja najviše $\frac{d}{2}$, slijedi da trebamo izabrati n cijelih brojeva a , pri čemu je vrijednost broja $n \in \mathbb{N}$ najbliža vrijednosti $\frac{d+2}{2}$.

Primjer 2.0.1. *U ovom primjeru ćemo faktorizirati polinom*

$$F(x) = x^5 + 6x^4 + 10x^3 + 4x^2 + x - 1.$$

Prema teoremu 1.1.5 kandidati za nultočke su: ± 1. *Kako je*

$$F(1) = 21, F(-1) = -3,$$

slijedi da polinom nema racionalnih nultočaka odnosno da nema ni cjelobrojnih nultočaka. Ako je F stupnja $d = 5$ reducibilan, tada postoji polinom G stupnja $d' \leq \frac{d}{2}$. Iz ovog slijedi da je polinom G stupnja 2. Bez smanjenja općenitosti, možemo pretpostaviti da djelitelj G ima pozitivan vodeći koeficijent tj. G je oblika

$$G(x) = X^2 + aX + b,$$

gdje su a i b cijeli brojevi. Kako je $F(0) = -1$ po Kroneckeru slijedi da je $G(0) = b = \pm 1$.

$$F(-1) = -3 \Rightarrow G(-1) = -a + b + 1 \in \{\pm 1, \pm 3\}$$
$$F(1) = 21 \Rightarrow G(1) = a + b + 1 \in \{\pm 1, \pm 3, \pm 7, \pm 21\}$$

Iz prethodnih jednakosti imamo sustav jednadžbi:

$$a = -G(-1) + b + 1$$

$$a = G(1) - b - 1.$$

Kada prvu jednadžbu pomnožimo s (-1) i dodamo drugoj imamo:

$$2b = G(-1) + G(1) - 2.$$

Kako je $b = \pm 1$*, očito je da* $G(1) \notin \pm 21$*. Imamo 2 slučaja.*

1. slučaj:

Neka je

$$b = 1 \Rightarrow 2 = G(-1) + G(1) - 2 \Rightarrow G(-1) + G(1) = 4,$$

pri čemu je

$$G(-1) \in \{\pm 1, \pm 3\}$$
$$G(1) = a + b + 1 \in \{\pm 1, \pm 3, \pm 7\}.$$

Primijetimo da u obzir dolaze samo 3 podslučaja:

1.1. $G(1) = 1, G(-1) = 3 \Rightarrow 2 = 1 + 3 - 2 = 2 \Rightarrow a = -1$

1.2. $G(1) = 3, G(-1) = 1 \Rightarrow 2 = -3 + 1 - 2 = 2 \Rightarrow a = 1$

1.3. $G(1) = 7, G(-1) = -3 \Rightarrow 2 = 7 - 3 - 2 = 2 \Rightarrow a = 5$

2. slučaj:

Neka je

$$b = -1 \Rightarrow -2 = G(-1) + G(1) - 2 \Rightarrow G(-1) + G(1) = 0,$$

pri čemu je

$$G(-1) \in \{\pm 1, \pm 3\}$$
$$G(1) = a + b + 1 \in \{\pm 1, \pm 3, \pm 7\}.$$

Uočimo da u obzir dolaze samo 4 podslučaja:

2.1. $G(1) = 1, G(-1) = -1 \Rightarrow -2 = 1 - 1 - 2 = -2 \Rightarrow a = -1$

2.2. $G(1) = -1, G(-1) = 1 - 2 = -1 + 1 - 2 = -2 \Rightarrow a = -1$

2.3. $G(1) = 3, G(-1) = -3 - 2 = 3 - 3 - 2 = -2 = 3$

2.4. $G(1) = -3, G(-1) = 3 \Rightarrow -2 = -3 + 3 - 2 = -2 \Rightarrow a = -3$

Dakle, imamo 7 mogućnosti:

1) $b = 1$ *za* $G(1) = 1$, $G(-1) = 3$, *pri čemu je* $a = -1$

2) $b = 1$ *za* $G(1) = 3$, $G(-1) = 1$, *pri čemu je* $a = 1$

3) $b = 1$ *za* $G(1) = 7$, $G(-1) = -3$, *pri čemu je* $a = 5$

4) $b = -1$ *za* $G(1) = 1$, $G(-1) = -1$, *pri čemu je* $a = 1$

5) $b = -1$ *za* $G(1) = -1$, $G(-1) = 1$, *pri čemu je* $a = -1$

6) $b = -1$ *za* $G(1) = 3$, $G(-1) = -3$, *pri čemu je* $a = 3$

7) $b = -1$ *za* $G(1) = -3$, $G(-1) = 3$, *pri čemu je* $a = -3$

Iz $F(-2) = -3$ *slijedi* $G(-2) = 4 - 2a + b \in \{\pm 1, \pm 3\}$. *Za sve mogućnosti izračunajmo* $G(-2)$*:*

1) $G(-2) = 7$

2) $G(-2) = 3$

3) $G(-2) = -5$

4) $G(-2) = 1$

5) $G(-2) = 5$

6) $G(-2) = -3$

7) $G(-2) = 9$

Primijetimo da vrijednost $G(-2)$ *dobivena pod 2), 4) i 6) pripada skupu* $\{\pm 1, \pm 3\}$ *iz čega slijedi da imamo tri kandidata za polinom* G*:*

2) $G(x) = x^2 + x + 1$

4) $G(x) = x^2 + x - 1$

6) $G(x) = x^2 + 3x - 1$

Kada podijelimo polinom F *polinomima pod 2), 4), 6) dobijemo da jedino polinom* $G(x) = x^2 + 3x - 1$ *dijeli polinom* F*. Dakle,*

$$F(x) = (x^2 + 3x - 1) \cdot (x^3 - 2x^2 + 3x + 1).$$

Poglavlje 3

Berlekampov algoritam

3.1 Uvod u Berlekampov algoritam

Kako bi objasnili Berlekampov algoritam potrebno je prvo definirati kvadratno slobodan polinom, iskazati Henselovu lemu, definirati rezultantu dvaju polinoma te iskazati Hadamardovu nejednakost.

Definicija 3.1.1. *Za polinom $f \in \mathbb{F}[x]$ kažemo da je kvadratno slobodan ako i samo ako vrijedi da je* $\gcd(f, f') = 1$*, pri čemu je f' derivacija polinoma f.*

Neka su f i g dva polinoma s jednom varijablom i koeficijentima iz polja $\mathbb{F}$. Kada f i g imaju netrivijalni zajednički faktor h tako da $f = f_1 h$, $g = g_1 h$, onda jednadžba

$$uf + vg = 0, \tag{3.1}$$

pri čemu je

$$\deg(u) < \deg(g)$$

$$\deg(v) < \deg(f)$$

ima rješenja $u = g_1$ i $v = -f_1$. Pišemo:

$$f(X) = \sum_{i=0}^{m} a_i X^i$$

$$g(X) \sum_{j=0}^{n} b_j X^j.$$

Tada je jednadžba (3.1) ekvivalentna homogenom linearnom sustavu od $n+m$ jednadžbi sa $n+m$ nepoznanica. Nepoznanice su nam koeficijenti polinoma u i v. Neka je

$$u(X) = \sum_{k=0}^{n-1} u_k X^k$$

$$v(X) = \sum_{l=0}^{m-1} v_l X^l.$$

Tada imamo $uf + vg = 0$ odnosno

$$a_m u_{n-1} X^{m+n-1} + a_m u_{n-2} X^{m+n-2} + ... + a_m u_0 X^m + ... + a_{0un-1} X^{n-1} + a_0 u_{n-2} X^{n-2} + ... + a_0 u_0 +$$
$$+ b_n v_{m-1} X^{n+m-1} + b_n v_{m-2} X^{n+m-2} + ... + b_n v_0 X^n + ... + b_0 v_{m-1} X^{m-1} + b_0 v_{m-2} X^{m-2} + ... + b_0 v_1 X + b_0 v_0 = 0$$

Izlučimo koeficijente uz iste potencije.

$$(a_m u_{n-1} + b_n v_{m-1}) X^{m+n-1} + (a_{m-1} u_{n-1} + a_m u_{n-2} + b_{n-1} v_{m-1} + b_n v_{m-2}) X^{m+n-2} + ... + a_0 u_0 + b_0 v_0 = 0$$

Prema teoremu 1.1.2. imamo sustav jednadžbi:

$$a_m u_{n-1} + b_n v_{m-1} = 0$$
$$a_{m-1} u_{n-1} + a_m u_{n-2} + b_{n-1} v_{m-1} + b_n v_{m-2} = 0$$
$$...$$
$$a_0 u_0 + b_0 v_0 = 0$$

Znamo da sustav ima netrivijalno rješenje ako i samo ako mu je determinanta jednaka nuli. Determinanta sustava je jednaka

$$\begin{vmatrix} a_m & a_{m-1} & \dots & a_1 & a_0 & 0 & \dots & 0 & \\ 0 & a_m & a_{m-1} & \dots & a_1 & a_0 & \dots & 0 & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ b_n & b_{n-1} & \dots & b_1 & b_0 & 0 & \dots 0 & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & \dots & \dots & 0 & b_n & b_{n-1} & \dots & b_1 & b_0 \end{vmatrix}$$

Preciznije, koeficijenti matrice su dani formulama:

$$c_{i,j} = a_{m-j+i}, 1 \leq i \leq n$$
$$c_{n+i,j} = b_{n-j+i}, 1 \leq i \leq m,$$

gdje je $a_i = 0$, $i \notin \{0, 1, \ldots, m\}$ i $b_j = 0$, $j \notin \{0, 1, \ldots, n\}$.
Ovako definiranu determinantu nazivamo rezultanta polinoma f i g i pišemo $Res(f, g)$.
Diskriminantu polinoma f stupnja m i korijena $\alpha_1, \alpha_2, \ldots$ računamo formulom

$$Discr(f) = a_m^{2m-2} \prod_{i=1}^{m} \prod_{j=1; j\neq i}^{m} (\alpha_i - \alpha_j),$$

pri čemu je a_m vodeći koeficijent polinoma f, a α_i su korijeni polinoma f.

Teorem 3.1.2. *(Hadamardova nejednakost) Neka su $b_1, b_2, \ldots, b_n$, $n \in \mathbb{N}$ nenul vektori euklidskog prostora $\mathbb{R}^n$, tada vrijedi nejednakost:*

$$|\det(b_1, b_2, ..., b_n)| \leq |b_1| \cdot |b_2| \cdot ... \cdot |b_n|.$$

(dokaz [2, str. 82])

Neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ polinom iz $\mathbb{Z}[X]$ stupnja n. Tada vrijedi

$$Res(f, f') = (-1)^{\frac{n(n-1)}{2}} a_n \cdot Discr(f). \tag{3.2}$$

Lema 3.1.3. *(Henselova lema) Neka je p prost broj te neka su f, h_0, g_0 polinomi u Z[X] za koje vrijedi:*

a) g_0 je normiran i $\deg(g_0) + \deg(h_0) = \deg(f)$
b) $f(X) - g_0(X)h_0(X) \equiv 0 (\mathrm{mod}\ p^{1+2k})$, gdje $p^k || Res(g_0, h_0)$, pri čemu $||$ označava da p^k dijeli $Res(g_0, h_0)$, a p^{k+1} ne dijeli $Res(g_0, h_0)$.

Tada za bilo koji $n \geq 0$, postoje polinomi h_n i g_n s cjelobrojnim koeficijentima tako da imamo:
1) g_n je normiran i $\deg(g_n) + \deg(h_n) = \deg(f)$
2) $g_n \equiv g_0 (\mathrm{mod}\ p^{k+1})$, $h_n \equiv h_0 (\mathrm{mod}\ p^{k+1})$
3) $f \equiv g_n h_n (\mathrm{mod}\ p^{n+2k+1})$

Dokaz. Lemu ćemo dokazati matematičkom indukcijom po n.

Baza:
Za $n = 0$, moramo dokazati:
1) g_0 je normiran i $\deg(g_0) + \deg(h_0) = \deg(f)$
2) $g_0 \equiv g_0 (\text{mod } p^{k+1}), \quad h_0 \equiv h_0 (\text{mod } p^{k+1})$
3) $f \equiv g_0 h_0 (\text{mod } p^{2k+1})$
Iz pretpostavke leme, slijedi da ove tvrdnje vrijede, odnosno da baza indukcije vrijedi.

Pretpostavka:
Pretpostavimo da za neki $n - 1 \in \mathbb{N}$ vrijedi:
1) g_{n-1} je normiran i $\deg(g_{n-1}) + \deg(h_{n-1}) = \deg(f)$
2) $g_{n-1} \equiv g_0 \text{ mod } (p^{k+1}), \quad h_{n-1} \equiv h_0 (\text{mod } p^{k+1})$
3) $f \equiv g_{n-1} h_{n-1} (\text{mod } p^{n+2k+1})$

Korak:
Provjerimo vrijedi li lema i za $n \in \mathbb{N}$. Tvrdnje pod 1) i 2) su očite. Moramo još provjeriti tvrdnju pod 3). Tražimo polinome g_n i h_n koji su zadani kao:

$$g_n = g_{n-1} + p^{n+k} g_n^*$$

$$h_n = h_{n-1} + p^{n+k} h_n^* \tag{3.3}$$

te vrijedi da je

$$\deg(g_n^*) \leq \deg(g_0) - 1$$

$$\deg(h_n^*) \leq \deg(h_0).$$

Za ovako definirane g_n i h_n tvrdnje 1) i 2) su zadovoljene. Potrebno je dokazati tvrdnju pod 3) odnosno da vrijedi

$$f \equiv g_n h_n (\text{mod } p^{n+2k+1}).$$

Iz ovog slijedi da je

$$f - g_n h_n \equiv 0 (\text{mod } p^{n+2k+1}).$$

$$f - g_n h_n = f - (g_{n-1} + p^{n+k} g_n^*)(h_{n-1} + p^{n+k} h_n^*) = f - g_{n-1} h_{n-1} - p^{n+k}(g_n^* h_{n-1} + g_{n-1} h_n^*) - g_n^* h_n^* p^{2(n+k)}$$

Slijedi

$$f - g_{n-1} h_{n-1} - p^{n+k}(g_i^* h_{n-1} + g_{n-1} h_n^*) \equiv 0 (\text{mod } p^{n+2k+1}).$$

Iz

$$f(X) - g_{n-1}(X) h_{n-1}(X) = p^{n+2k} r_{n-1}(X) \tag{3.4}$$

slijedi

$$g_{n-1}(X)h_n^*(X) + h_{n-1}(X)g_n^*(X) \equiv p^k r_{n-1}(x) (\mathrm{mod}\ p^{k+1}). \tag{3.5}$$

Kongruencija (3.2) je ekvivalentna linearnom sustavu gdje su nepoznanice koeficijenti polinoma g_n^* i h_n^*. Neka je d stupanj polinoma f. Broj nepoznanica linearnog sustava jednak je broju koeficijenata polinoma g_n^* i h_n^*. Sada imamo

$$\deg(h_n^*) + 1 + \deg(g_n^*) + 1 = \deg(h_0) + 1 + \deg(g_0) = d + 1$$

Primijetimo da je broj koeficijenata nekog polinoma za jedan veći od stupnja tog polinoma. Iz ovog slijedi da je broj nepoznanica linearnog sustava jednak broju koeficijenata polinoma f odnosno da je broj nepoznanica jednak broju jednadžbi linearnog sustava. Determinanta ovog sustava je zapravo rezultanta polinoma g_{n-1} i h_{n-1} iz čega, po pretpostavci, slijedi da je determinanta ovog sustava djeljiva s p^k, ali nije djeljiva s p^{k+1} prema pretpostavci leme. Prema Cramerovom pravilu slijedi da sustav (3.2) ima rješenje (g_n^*, h_n^*) u polju racionalnih brojeva te da zajednički nazivnik a polinoma g_n^* i h_n^* nije djeljiv s p. Ako je u cijeli broj tako da vrijedi:

$$ua \equiv 1 (\mathrm{mod}\ p^{k+1}),$$

tada, kada rješenje (g_n^*, h_n^*) pomnožimo s ua dobivamo dva polinoma s cjelobrojnim koeficijentima čija redukcija p^k zadovoljava kongruenciju (3.2). Budući da baza indukcije vrijedi, te iz prepostavke da tvrdnje 1), 2), 3) vrijede za neki $n - 1 \in \mathbb{N}$ slijedi da vrijede i za $n \in \mathbb{N}$, prema aksiomu matematičke indukcije možemo zaključiti da tvrdnje 1), 2), 3) vrijede za svaki $n \in \mathbb{N}$. Ovime je dokaz gotov. □

3.2 Berlekampov algoritam

Neka je $F \in \mathbb{Z}[x]$ kvadratno slobodan polinom stupnja d i visine H. Pretpostavimo da je F normiran. Berlekampova metoda se sastoji od ovih koraka:

1) Trebamo odabrati prosti broj p koji ne dijeli diskriminantu polinoma F.

2) Faktorizirati polinom $f \in \mathbb{Z}_p[x]$, gdje je f slika polinoma F modulo p. Neka su $P_1, P_2, \ldots, P_k$ ireducibilni faktori od $f \in \mathbb{Z}_p[x]$.

3) Ako je $k = 1$, tada F nije reducibilan i na ovom mjestu procedura staje.

4) Ako je $k > 1$, izaberemo bilo koju particiju skupa $\{1, 2, 3, \ldots, k\}$ u dva neprazna skupa S i T i označimo:

$$g_0 = \prod_{i \in S} P_i$$

$$h_0 = \prod_{i \in T} P_i$$

tako da vrijedi $F \equiv g_0 h_0 (\text{mod } p)$, pri čemu je $Res(g_0, h_0) \not\equiv 0 (\text{mod } p)$, uz pretpostavku da su g_0 i h_0 polinomi s cjelobrojnim koeficijentima.

5) Primijenimo Henselovu lemu: $F \equiv gh (\text{mod } p^n)$, $p^n \geq B$, pri čemu je B izabrana granica, a polinomi g i h imaju koeficijente koji su između $-p^{\frac{n}{2}}$ i $p^{\frac{n}{2}}$.

6) Provjerimo dijeli li polinom g polinom F u prstenu $\mathbb{Z}[x]$. Imamo tri mogućnosti:

6.1) Polinom g dijeli F. Dakle, pronašli smo netrivijalni faktor polinoma F. Tada, možemo primijeniti cijeli postupak na faktore g i F/g polinoma F.

6.2) Polinom g ne dijeli F, ali postoji barem jedna particija skupa $\{1, 2, 3, \ldots, k\}$ koja nije provjerena. Tada, pokušamo s tom particijom i vratimo se na korak 4.

6.3) Sve particije su provjerene. Postupak zaustavljamo i zaključujemo da je polinom F ireducibilan nad cijelim brojevima.

3.3 Analiza Berlekampovog algoritma

Ako pogledamo korake Berlekampovog algoritma, primijetit ćemo da nam se prirodno postavljaju pitanja: kako odabrati prosti broj u prvom koraku te kako odabrati granicu B u petom koraku. Prije nego što odgovorimo na ta pitanja, analizirajmo prvi korak. Da bi mogli primijeniti Berlekampov algoritam na polinom F, polinom F mora biti kvadratno slobodan. Je li polinom F kvadratno slobodan provjeravamo na način da nađemo najveći zajednički djelitelj polinoma F i njegove derivacije F'. Vrijedi da je F kvadratno slobodan u $\mathbb{Z}_p[X]$ ako i samo ako je $\gcd(F, F') = 1$ odnosno ako i samo ako

$$Res(F, F') = (-1)^{\frac{n(n-1)}{2}} a_n \cdot Discr(f) \neq 0.$$

Iz ovoga slijedi, F je kvadratno slobodan ako i samo ako p ne dijeli diskriminantu od F.

Odabir prostog broja p

Odgovorimo sada na naše prvo postavljeno pitanje: kako odabrati prost broj p u prvom koraku. Ideja leži u tom da odredimo maksimalnu vrijednost diskriminante polinoma F

te odredimo koliko ima prostih djelitelja. Kada pronađemo broj prostih djelitelja diskriminante, dokazali smo da postoji prost broj koji ne dijeli diskriminantu jer prostih brojeva ima beskonačno mnogo. Nakon raznih transformacija, dobivamo da je

$$p = O(d \cdot \ln d + d \cdot \ln H),$$

pri čemu je O sljedeća oznaka:
$f(x) = O(g(x))$ ako postoji konstanta C takva da je $|f(x)| \leq Cg(x)$ za sve x. (dokaz, [3, str. 319])

Odabir granice B

Neka je G djelitelj polinoma $F \in \mathbb{Z}[X]$ tako da

$$G(X) = b_m X^m + b_{m-1} X^{m-1} + ... + b_1 x + b_0,$$

pri čemu je m stupanj polinoma G. Kako vrijedi

$$2^m > \binom{m}{\lfloor \frac{m}{2} \rfloor}$$

$$H(G) \leq M(G) \cdot \binom{m}{\lfloor \frac{m}{2} \rfloor}$$

slijedi

$$H(G) \leq M(G) \cdot \binom{m}{\lfloor \frac{m}{2} \rfloor} \leq 2^m \cdot M(F).$$

Iz leme 1.2.2 slijedi

$$H(G) \leq M(F) \cdot 2^m \leq 2^m \cdot \sqrt{d+1} \cdot H(F).$$

Kada faktoriziramo polinom F modulo p^n, koeficijente faktora biramo iz intervala $[-\frac{p^n-1}{2}, \frac{p^n-1}{2}]$ i biramo eksponent n koji je dovoljno velik da vrijedi $p^n \geq 2H(G)$, pri čemu je polinom G bilo koji djelitelj polinoma F stupnja najviše $\frac{d}{2}$. Ako uzmemo

$$p^n \geq 2^{1+\frac{d}{2}} \cdot (d+1)^{1/2} \cdot H(F),$$

zbog nejednakosti (1.4) slijedi da je

$$p^n \geq 2^{1+\frac{d}{2}} \cdot (d+1)^{1/2} \cdot H(F) \geq 2 \cdot H(G).$$

Dakle, dovoljno je uzeti

$$B = 2^{1+\frac{d}{2}} \cdot (d+1)^{\frac{1}{2}} \cdot H(F). \tag{3.6}$$

Sada kada znamo odabrati p i B, riješimo primjer.

Primjer 3.3.1. *Faktorizirajmo polinom*

$$F(x) = x^3 - 3x^2 - x + 3.$$

Primijetimo da je vodeći član polinoma jednak 1*, a stupanj polinoma jednak* $d = 3$*. Prije prvog koraka, provjerimo je li F kvadratno slobodan. Derivacija polinoma F je*

$$F'(x) = 3x^2 - 6x - 1.$$

Primijenimo Euklidov algoritam:

$$x^3 - 3x^2 - x + 3 = \left(3x^2 - 6x - 1\right)\left(\frac{1}{3}x - \frac{1}{3}\right) - \frac{8}{3}x + \frac{8}{3}$$

$$3x^2 - 6x - 1 = \left(\frac{-8}{3}x + \frac{8}{3}\right)\left(\frac{-9}{8}x + \frac{12}{8}\right) - 5$$

Očito je da je $gcd(F, F') = 1$ *iz čega slijedi da je F kvadratno slobodan.*

1) Odaberimo prosti broj p koji ne dijeli diskriminantu polinoma P. Rezultanta polinoma F i F' *je:*

$$\begin{vmatrix} 1 & -3 & -1 & 3 & 0 \\ 0 & 1 & -3 & -1 & 3 \\ 3 & -6 & -1 & 0 & 0 \\ 0 & 3 & -6 & -1 & 0 \\ 0 & 0 & 3 & -6 & -1 \end{vmatrix} = -256.$$

Iz (3.2) slijedi da je $Discr(F) = 256$*. Dakle, možemo uzeti* $p = 3$ *jer 3 ne dijeli 256.*

2) Odredimo polinom $f \in \mathbb{Z}_3[x]$*.*

$$x^3 - 3x^2 - x + 3 \equiv x^3 - x \pmod 3$$

Iz ovoga slijedi da je

$$f(x) = x^3 - x.$$

Faktorizrajmo polinom f:

$$f(x) = x^3 - x = x(x-1)(x+1),$$

pri čemu je $P_1 = x$*,* $P_2 = x - 1$*,* $P_3 = x + 1$*. Dakle,* $k = 3$*. Kako je* $k > 1$*, idemo na četvrti korak.*

4) Trebamo izabrati g_0 i h_0 tako da $F \equiv g_0 h_0 (\mathrm{mod}\ 3)$ i broj 3 ne dijeli $Res(g_0, h_0)$. Ako uzmemo $g_0(x) = x$ i $h_0(x) = x^2 - 1$, tada vrijedi da je $F \equiv g_0 h_0 (\mathrm{mod}\ 3)$ jer

$$x^3 - 3x^2 - x + 3 \equiv x^3 - x (\mathrm{mod}\ 3)$$

$$\Leftrightarrow x^3 - 3x^2 - x + 3 - x^3 + x \equiv 0 (\mathrm{mod}\ 3)$$

$$\Leftrightarrow -3x^2 + 3 \equiv 0 (\mathrm{mod}\ 3).$$

Provjerimo dijeli li prost broj 3 rezultantu polinoma h_0 i g_0.

$$Res(g_0, h_0) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{vmatrix} = -1$$

Budući da 3 ne dijeli $Res(g_0, h_0)$ te vrijedi $F \equiv g_0 h_0 (\mathrm{mod}\ 3)$, g_0 i h_0 su dobro odabrani.

5) U ovom koraku trebamo primijeniti Henselovu lemu: $F \equiv gh (\mathrm{mod}\ p^n)$, $p^n \geq B$, pri čemu je B izabrana granica, a polinomi g i h imaju koeficijente koji su između $\frac{-p^n}{2}$ i $\frac{p^n}{2}$. Iz (3.6) slijedi da je $B \approx 33.94$ odnosno da je $n = 4$. Koeficijenti polinoma g i h moraju biti unutar intervala $[-40, 40]$.

Trebamo pronaći polinome g i h tako da $F \equiv gh (\mathrm{mod}\ 81)$. Budući da $F \not\equiv g_0 h_0 (\mathrm{mod}\ 81)$, pokušajmo s g_1 i h_1. Prema (3.3) slijedi

$$g_1 = g_0 + 3g_1^*$$

$$h_1 = h_0 + 3h_1^*, \tag{3.7}$$

pri čemu je $n = 1$ i $p = 3$. Kako 3 ne dijeli rezultantu, $k = 0$.

Kako bi iz kongruencije (3.5) odredili $g_1(x)^*$ i $h_1(x)^*$, potrebno je pronaći $r_0(x)$ iz jednakosti (3.4).

$$F(x) - g_0(x)h_0(x) = 3r_0(x)$$

$$x^3 - 3x^2 - x + 3 - x^3 + x = 3r_0(x)$$

$$-3x^2 + 3 = 3 \cdot r_0(x)$$

$$r_0(x) = -x^2 + 1$$

Iz kongruencije (3.5) slijedi

$$x \cdot h_1(x)^* + (x^2 - 1) \cdot g_1(x)^* \equiv (-x^2 + 1) (\mathrm{mod}\ 3).$$

Primijetimo da ako uzmemo da je $h_1(x)^* = 0$ i $g_1(x)^* = -1$, kongruencija vrijedi. Tada iz (3.7) slijedi

$$g_1 = x - 3$$

$$h_1 = x^2 - 1.$$

Provjerimo vrijedi li $F \equiv g_1 h_1 (\mathrm{mod}\ 81)$.

$$F - g_1 h_1 \equiv 0 (\mathrm{mod}\ 81)$$

$$\Leftrightarrow x^3 - 3x^2 - x + 3 = (x-3)\cdot(x^2-1)$$

$$\Leftrightarrow 0 \equiv 0 (\mathrm{mod}\ 81)$$

Dakle, vrijedi da je $F \equiv g_1 h_1 (\mathrm{mod}\ 81)$. *Sada možemo zaključiti da je* $g(x) = x - 3$, *a* $h(x) = x^2 - 1$. *Možemo primijetiti da je* $F - gh = 0$ *iz čega slijedi da je* $F = gh$. *Kako je* g *ireducibilan te je očito da je* $h(x) = (x-1)\cdot(x+1)$, *faktorizacija završava. Dakle,*

$$F(x) = x^3 - 3x^2 - x + 3 = (x-3)\cdot(x-1)\cdot(x+1).$$

Primjer 3.3.2. *Faktorizirajmo polinom*

$$F(x) = x^4 + 3x^3 + 11x^2 + 15x + 18.$$

Provjerimo je li F *kvadratno slobodan Euklidovim algoritmom.*

$$F'(x) = 4x^3 + 9x^2 + 22x + 15$$

$$x^4 + 3x^3 + 11x^2 + 15x + 18 = (4x^3 + 9x^2 + 22x + 15)\cdot\left(\frac{1}{4}x + \frac{3}{16}\right) + \frac{61}{16}x^2 + \frac{57}{8}x + \frac{243}{16}$$

$$4x^3 + 9x^2 + 22x + 15 = \left(\frac{61}{16}x^2 + \frac{57}{8}x + \frac{243}{16}\right)\cdot\left(\frac{64}{61}x + \frac{1488}{3721}\right) + \frac{11968}{3721}x + \frac{33216}{3721}$$

$$\frac{61}{16}x^2 + \frac{57}{8}x + \frac{243}{16} = \left(\frac{11968}{3721}x + \frac{33216}{3721}\right)\cdot\left(\frac{226981}{191488}x - \frac{53729}{50000}\right) + \frac{6932223}{279752}$$

Možemo uočiti da je $\gcd(F, F') = 1$ *odnosno da je* F *kvadratno slobodan. Sada možemo primijeniti Berlekampov algoritam na polinom* F.

1) Trebamo odrediti prost broj p *koji ne dijeli diskriminantu polinoma* f.

$$Res(F, F') = \begin{vmatrix} 1 & 3 & 11 & 15 & 18 & 0 & 0 \\ 0 & 1 & 3 & 11 & 15 & 18 & 0 \\ 0 & 0 & 1 & 3 & 11 & 15 & 18 \\ 4 & 9 & 22 & 15 & 0 & 0 & 0 \\ 0 & 4 & 9 & 22 & 15 & 0 & 0 \\ 0 & 0 & 4 & 9 & 22 & 15 & 0 \\ 0 & 0 & 0 & 4 & 9 & 22 & 15 \end{vmatrix} = 59616.$$

Uočimo da je vodeći koeficijent polinoma F jednak 1 *te da je stupanj polinoma F jednak* 4. *Tada iz (3.2) slijedi $Res(F, F') = Discr(F)$. Budući da je* 5 *najmanji prost broj koji ne dijeli diskriminantu polinoma F, uzmimo da je $p = 5$.*

2) Trebamo faktorizirati polinom $f \in \mathbb{Z}_5[x]$, gdje je f slika polinoma F modulo 5. *Neka su $P_1, P_2, ..., P_k$ ireducibilni faktori od $f \in \mathbb{Z}_5[x]$.*

$$f(x) = x^4 + 3x^3 + x^2 + 3 \equiv x^4 + 3x^3 + 6x^2 + 5x + 3 (\text{mod } 5)$$

$$\begin{aligned} x^4 + 3x^3 + 6x^2 + 5x + 3 &= x^4 + 2x^3 + x^3 + 3x^2 + 2x^2 + x^2 + 2x + 3x + 3 \\ &= x^2(x^2 + x + 1) + 2x(x^2 + x + 1) + 3(x^2 + x + 1) \\ &= (x^2 + x + 1) \cdot (x^2 + 2x + 3) \end{aligned}$$

Dakle, imamo

$$f(x) = (x^2 + x + 1) \cdot (x^2 + 2x + 3), f \in \mathbb{Z}_5[x].$$

$$P_1(x) = x^2 + x + 1$$

$$P_2(x) = x^2 + 2x + 3.$$

Iz ovog slijedi da je $k = 2$ te idemo na četvrti korak.

4) Moramo izabrati g_0 i h_0 tako da je $F \equiv g_0 h_0 (\text{mod } 5)$ i $Res(g_0, h_0) \not\equiv 0 (\text{mod } 5)$. Provjerimo možemo li uzeti da je

$$g_0 = x^2 + x + 1$$

$$h_0 = x^2 + 2x + 3.$$

$$\begin{aligned} & F \equiv g_0 h_0 (\text{mod } 5) \\ \Leftrightarrow\ & F - g_0 h_0 (\text{mod } 5) \\ \Leftrightarrow\ & x^4 + 3x^3 + 11x^2 + 15x + 18 - x^4 - 3x^3 - 6x^2 - 5x - 3 \equiv 0 (\text{mod } 5) \\ \Leftrightarrow\ & 5x^2 + 10x + 15 \equiv 0 (\text{mod } 5). \end{aligned} \tag{3.8}$$

Kako zadnja kongruencija vrijedi, slijedi da vrijedi i $F \equiv g_0 h_0 (\text{mod } 5)$. Još treba provjeriti dijeli li $Res(g_0, h_0)$.

$$Res(g_0, h_0) = \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{vmatrix} = 3$$

Budući da 5 *ne dijeli* $Res(g_0, h_0)$*, dobro smo odabrali* g_0 *i* h_0*.*

5) U ovom koraku trebamo primijeniti Henselovu lemu $F \equiv gh(\text{mod } p^n)$*,* $p^n \geq B$*, a polinomi g i h imaju koeficijente između* $\frac{-p^n}{2}$ *i* $\frac{p^n}{2}$*. Iz (3.6) slijedi da je* $B \approx 321.99$*. Sada možemo zaključiti da je* $n = 4$ *odnosno moramo pronaći polinome g i h tako da je* $F \equiv gh(\text{ mod } 625)$*, pri čemu polinomi g i h imaju koeficijente koji su između* -312 *i* 312*. Iz (3.8) vidimo da za polinome* g_0 *i* h_0 *ne vrijedi* $F \equiv g_0h_0(\text{mod } 625)$*. Provjerimo vrijedi li ova kongruencija za polinome* g_1 *i* h_1*. Iz (3.3) slijedi*

$$g_1 = g_0 + 5g_1^*$$

$$h_1 = h_0 + 5h_1^*. \tag{3.9}$$

Kako bi mogli izračunati g_1^* *i* h_1^* *iz kongruencije (3.5) moramo najprije izračunati* $r_0(x)$ *iz jednakosti (3.4).*

$$F(x) - g_0h_0 = 5r_0(x)$$

$$5x^2 + 10x + 5 = 5r_0(x)$$

$$r_0(x) = x^2 + 2x + 3$$

Prema (3.5) imamo

$$(x^2 + x + 1) \cdot h_1^*(x) + (x^2 + 2x + 3) \cdot g_1^*(x) \equiv x^2 + 2x + 3(\text{mod } 5).$$

Primijetimo da ako je $h_1^*(x) = 0$ *i* $g_1^*(x) = 1$*, tada konvergencija vrijedi. Iz (3.9) slijedi*

$$g_1(x) = x^2 + x + 6$$

$$h_1(x) = x^2 + 2x + 3.$$

Provjerimo vrijedi li $F \equiv g_1h_1(\text{mod } 625)$*.*

$$F - g_1h_1 \equiv 0(\text{mod } 625)$$

$$\Leftrightarrow x^4 + 3x^3 + 11x^2 + 15x + 18 - (x^2 + x + 6) \cdot (x^2 + 2x + 3) \equiv 0(\text{mod } 625)$$

$$\Leftrightarrow 0 \equiv 0(\text{mod } 625)$$

Iz posljednje kongruencije slijedi da smo pronašli g i h tako da vrijedi $F \equiv gh(\text{mod } 625)$*, pri čemu je*

$$g(x) = x^2 + x + 6$$

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

Uočimo da, kada pomnožimo g i h, dobijemo upravo F. Kako su g i h ireducibilni, ovdje faktorizacija završava. Dakle,

$$F(x) = x^4 + 3x^3 + 11x^2 + 15x + 18 = (x^2 + x + 6) \cdot (x^2 + 2x + 3).$$

3.4 Složenost

Budući da je složenost prva tri koraka prema [4] iznosi

$$O(d^3 \cdot p(\ln p)^2).$$

Možemo pretpostaviti da je

$$p = O(d \cdot \ln(dH)).$$

Stoga, vrijeme izvršavanja prva tri koraka je najviše

$$O(d^4 \cdot (\ln d \cdot H)^2).$$

Za bilo koji izbor particije S, vrijeme izvršavanja je

$$C = (d^2(d + \ln H)^2).$$

Primijetimo da moramo provjeriti najviše 2^{k-1} mogućih particija S i tada je vrijeme izvršavanja od 4-6 koraka ekvivalentno $2^{k-1}C$. Kako imamo $k \leq 2\ln d$ slijedi

$$2^k < d^{\frac{3}{2}}.$$

Iz svega slijedi da je složenost Berlekampovog algoritma

$$O((\ln d)^2 \cdot d^4 \cdot (\ln d \cdot H)^2).$$

Poglavlje 4

LLL algoritam

4.1 Uvod u LLL algoritam

Ovaj algoritam dobio je ime po trima matematičarima koji su zaslužni za njegovo otkriće. To su: Arjen Lenstra, Hendrik Lenstra i László Lovász. Naziva se još i L^3 algoritam. Bazira se na Berlekampovu algoritmu za konačna polja te Henselovoj lemi. Ideja algoritma je da za polinom F s cjelobrojnim koeficijentima treba pronaći odgovarajući prosti broj p i izračunati ireducibilan polinom G koji dijeli $F(\text{mod } p)$. Također, treba pronaći ireducibilan polinom H koji dijeli polinom F, pri čemu $G(\text{mod } p)$ dijeli polinom H. Prije nego što krenemo na sam LLL-algoritam, definirati ćemo rešetku i reduciranu bazu te se podsjetiti Gram-Schmidtovog postupka ortogonalizacije.

Definicija 4.1.1. *Neka je n prirodan broj i neka je L podskup euklidskog prostora $\mathbb{R}^n$. Ako postoji baza $\{b_1, b_2, \ldots, b_n\}$ prostora $\mathbb{R}^n$ takva da vrijedi*

$$L = \sum_{i=1}^{n} b_i\mathbb{Z} = \{\sum_{i=1}^{n} r_i b_i; r_i \in \mathbb{Z}\},$$

tada je L rešetka.

Neka je $\mathbb{R}^n$ vektorski prostor. Prisjetimo se definicije skalarnog umnoška. Neka su $\vec{a} = (a_1, a_2, ..., a_n)$ i $\vec{b} = (b_1, b_2, ..., b_n)$ vektori iz $\mathbb{R}^n$. Skalarni umnožak vektora $\vec{a}$ i $\vec{b}$ je

$$< a, b >= a_1b_1 + a_2b_2 + ... + a_nb_n.$$

Teorem 4.1.2. *(Gram-Schmidtov postupak ortogonalizacije) Neka je $\{b_1, ..., b_n\}$ baza prostora $\mathbb{R}^n$. Ortogonalnu bazu $\{b_1^*, b_2^*, ..., b_n^*\}$ prostora $\mathbb{R}^n$ računamo na način:*

$$b_1 = b_1^*$$

$$b_2^* = b_2 - \frac{< b_2, b_1^* >}{< b_1^*, b_1^* >} b_1^*$$
$$...$$
$$b_n^* = b_n - \frac{< b_n, b_1^* >}{< b_1^*, b_1^* >} b_1^* - ... - \frac{b_n, b_{n-1}^*}{b_{n-1}^*, b_{n-1}^*} b_{n-1}^*.$$

Definicija 4.1.3. *Ako su vektori $b_1, b_2, ..., b_n$ linearno nezavisni, pišemo:*

$$\mu_{i,j} = \frac{< b_i, b_j^* >}{< b_j^*, b_j^* >},$$

pri čemu vrijedi $i = 1, ..., n,\ j = 1, ..., i-1$. Baza $\{b_1, b_2, \ldots, b_n\}$ rešetke $L \in \mathbb{R}^n$ je reducirana, ako vrijedi:

$$|\mu_{i,j}| \leq \frac{1}{2}, 1 \leq j < i \leq n$$

$$||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \geq \frac{3}{4} ||b_{i-1}^*||^2, 1 < i \leq n.$$

Sada ćemo definirati polinome F, G i H koje sam spomenula na početku poglavlja.

Definicija 4.1.4. *Neka je $p \geq 2$ prost broj, $k \in \mathbb{N} \setminus \{0\}$ te neka su $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ i $\frac{\mathbb{Z}}{p^k\mathbb{Z}}$ kvocijentni prsteni. Reprezentanti elemenata iz $\mathbb{Z}/p^k\mathbb{Z}$ su cijeli brojevi iz intervala $[-p^k/2, p^k/2]$. Neka je $F \in \mathbb{Z}[X]$ stupnja $n \geq 1$, polinom H stupnja $d \leq n$ tako da vrijedi:*

1) Polinom H je normiran.

2) $H(\text{mod } p^k)$ dijeli $F(\text{mod } p^k)$ u $(\mathbb{Z}/p^k\mathbb{Z})[X]$

3) $H(\text{mod } p)$ je ireducibilan u $\mathbb{F}_p[X]$

4) $H(\text{mod } p)^2$ ne dijeli $F(\text{mod } p)$ u $\mathbb{F}_p[X]$

Primijetimo da polinom H koji zadovoljava svojstva 1) - 4), možemo pronaći pomoću Berlekampovog algoritma.

Propozicija 4.1.5. *Ako postoji polinom $H \in \mathbb{Z}[X]$ koji zadovoljava svojstva od 1) - 4), tada postoji ireducibilan djelitelj H_0 od F u polju polinoma s cjelobrojnim koeficijentima tako da je $H_0(\text{mod } p)$ djeljivo s $H(\text{mod } p)$, pri čemu je H_0 jedinstveno određen do na predznak. Ako je polinom G djelitelj polinoma F, sljedeće tvrdnje su ekvivalentne:*

1) $H(\text{mod } p)$ *dijeli* $G(\text{mod } p)$ *u* $\mathbb{F}_p[X]$

2) $H(\text{mod } p^k)$ *dijeli* $G(\text{mod } p^k)$ *u* $(\mathbb{Z}/p^k\mathbb{Z}[X])$

3) H_0 *dijeli* G *u* $\mathbb{Z}[X]$
Ako ove tvrdnje vrijede, tada $H(\text{mod } p^k)$ *dijeli* $H_0(\text{mod } p^k)$ *u* $\mathbb{Z}/p^k\mathbb{Z}$.
(dokaz [5, str. 272])

Neka je prirodan broj $m \geq d = \deg(H)$ te

$$L = \{Q \in \mathbb{Z}[X]; \deg(Q) \leq m, H(\text{mod } p^k) \quad \text{dijeli} \quad Q(\text{mod } p^k) \quad \text{u} \quad (\mathbb{Z}/p^k\mathbb{Z})[X]\}.$$

L je podskup $\mathbb{R}$-vektorskog prostora $\sum_{j=0}^{m} \mathbb{R} \cdot X^j$ što poistovjećujemo sa $\mathbb{R}^{m+1}$ relacijom

$$\sum_{i=0}^{m} a_i X^i \to (a_0, a_1, ..., a_m).$$

Tada je L rešetka u $\mathbb{R}^{m+1}$, a baza od L je jednaka:

$$B = \{p^k X^i, 0 \leq i < d\} \cup \{HX^j, 0 \leq j \leq m - d\}.$$

Teorem 4.1.6. *U teoremu se uzimaju u obzir oznake prethodno definirane.*
Ako je $\{b_1, b_2, ..., b_{m+1}\}$ *reducirana baza od L, tada :*

1) Ako vrijedi $\|b_1\| < (p^{kd} \cdot \|F\|^{-m})^{1/n}$, *onda* $\deg(H_0) \leq m$.

2) Ako vrijede nejednakosti:

$$p^{kd} > 2^{mn/2} \cdot \binom{2m}{m}^{n/2} \cdot \|F\|^m \cdot M(F)^n, \tag{4.1}$$

$$\deg(H_0) \leq m,$$

tada

$$\|b_1\| < (p^{kd} \cdot \|F\|^{-m})^{1/n}.$$

Prisjetimo se $M(F)$ *označava Mahlerovu mjeru definiranu pod 1.2.2.*
(dokaz [5, str. 275])

Korolar 4.1.7. *Neka je* $j \in \{1, 2, ..., m + 1\}$ *tako da*

$$\|b_j\| < (p^{kd} \cdot \|F\|^{-m})^{1/n}. \tag{4.2}$$

Neka je t najveći takav j. Tada imamo:

$$\deg(H_0) = m + 1 - t,$$

$$H_0 = \gcd(b_1, b_2, ..., b_t)$$

i nejednakost (4.1.) vrijedi za svaki $j \in \{1, 2, ..., t\}$.

4.2 LLL algoritam

Kako bi mogli provesti LLL algoritam potrebno je definirati algoritam redukcije baze te još dva pomoćna algoritma A i B.

Algoritam redukcije baze

Neka je $\{b_1, b_2, ..., b_n\}$ baza rešetke L. Pomoću Gram-Schmidtovog postupka ortogonalizacije (teorem 4.1.2) izračunajmo b_i^*, za $1 \leq i \leq n$, $\mu_{i,j}$ za $1 \leq j < i \leq n$ te neka je $k \in \{1, 2, ..., n+1\}$. Na početku algoritma je $k = 2$.

Provjerimo jesu li zadovoljeni uvjeti:
1)

$$|\mu_{i,j}| \leq \frac{1}{2}, \text{za} \quad 1 < j < i < k,$$

$$\|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \geq \frac{3}{4}\|b_{i-1}^*\|, \text{za} \quad 1 < i < k.$$

Uvjeti su zadovoljeni za $k = 2$. Ako je $k = n + 1$, algoritam staje jer je baza reducirana. Inače, ako je $k < n + 1$, provjerimo je li zadovoljen uvjet 2.
2)

$$\mu_{k,k-1} \leq \frac{1}{2}, \text{za} \quad k > 1.$$

Ako uvjet 2) nije ispunjen, onda računamo cijeli broj r koji je najbliži broju $\mu_{k,k-1}$ i zamijenimo b_k sa $b_k - rb_{k-1}$, $\mu_{k,j}$, $j < k$ sa $\mu_{k,j} - r\mu_{k-1,j}$, $\mu_{k,k-1}$ sa $\mu_{k,k-1} - r$. Nakon ove promjene, uvjet je zadovoljen. Sada imamo dva slučaja.

1.slučaj:

$$k = 1 \quad \text{ili} \quad \|b_k^* + \mu_{k,k-1} b_{k-1}^*\|^2 \geq \frac{3}{4}\|b_{k-1}^*\|^2$$

U ovom slučaju provjeravamo uvjet:
3)

$$|\mu_{k,j}| \leq \frac{1}{2}, 1 \leq j \leq k - 1.$$

Za $j = k - 1$, uvjet je zadovoljen. Zapravo, tada je uvjet 3) ekvivalentan uvjetu 2). Ako uvjet 3) nije zadovoljen, neka je prirodan broj t najveći indeks za kojeg vrijedi $|\mu_{k,t}| \geq \frac{1}{2}$ i neka je cijeli broj r najbliži broju $\mu_{k,t}$. Zamijenimo b_k sa $b_k - rb_1$, $\mu_{k,t}$ sa $\mu_{k,t} - r$. Sve dok je $j < t$, treba zamijeniti $\mu_{k,j}$ sa $\mu_{k,j} - r\mu_{i,j}$. zamjene se ponavljaju sve dok uvjet 3) nije zadovoljen.

2.slučaj:

$$k \geq 2,$$

$$\|b_k^* + \mu_{k,k-1} b_{k-1}^*\|^2 < \frac{3}{4}\|b_{k-1}^*\|^2.$$

Budući da u ovom slučaju imamo puno zamjena, za njih ćemo napisati formule. Neka su c_i i c_i^* vektori koje ćemo zamijeniti vektorima b_i odnosno b_i^* redom. Neka su $v_{i,j}$ koji će biti zamijenjeni sa $\mu_{i,j}$. Baza $\{c_1, c_2, ..., c_n\}$ je dana sa:

$$c_{k-1} = b_k$$

$$c_k = b_{k-1}$$

$$c_i = b_i, \text{ako} \quad \text{je} \quad i \neq k-1, k.$$

Nakon primjene Gram-Schmidtovog postupka ortogonalizacije dobivamo da je

$$c_i^* = b_i^*.$$

$$v_{k-1,j} = \mu_{k,j}$$

$$v_{i,j} = \mu_{i,j},$$

pri čemu je $1 \leq j < k-1$ te

$$v_{i,j} = \mu_{i,j},$$

pri čemu je $i, j \notin \{k-1, k\}$. (Vidi [5], str. 267)
Još nam samo preostaje napraviti zamjenu k sa $k+1$ te se vratiti na provjeru uvjeta pod 1).

Algoritam *A*

Neka je polinom F polinom s cjelobrojnim koeficijentima stupnja $n \geq 1$, p je prost broj, $k \in \mathbb{N}_0$ te polinom H stupnja d koji zadovoljava svojstva 1-4 iz definicije 4.1.4. Polinom F je primitivan, a koeficijenti polinoma H su reducirani modulo p^k i vrijedi

$$\|H\|^2 < 1 + dp^{2k}.$$

Također, neka je $m \geq d$ broj tako da vrijedi nejednakost (4.1). Tada prema propoziciji 4.1.5 postoji jedinstveni polinom $H_0 \in \mathbb{Z}$ tako da $H(\text{mod } p)$ dijeli $H_0(\text{mod } p)$ u $\mathbb{F}_p[X]$. Algoritam provjerava je li $\deg(H_0) \leq m$ te ako je, vraća kako izgleda H_0. Broj m je određen tako da vrijedi

$$p^{kd} > 2^{mn/2} \cdot \binom{2m}{m}^{n/2} \cdot \|F\|^m \cdot M(F)^n.$$

Koraci algoritma A:
1) Neka je L rešetka baze

$$\{p^k X^i; 0 \leq i < d\} \cup \{HX^j; 0 \leq j < m - d\}.$$

2) Treba izračunati bazu $\{b_1, b_2, ..., b_{m+1}\}$ rešetke L koristeći prethodno opisan algoritam redukcije baze.

3) Ako je

$$\|b_1\| \geq (p^{kd} \cdot \|F\|^{-m})^{1/n},$$

tada je $\deg(H_0) \geq m$ i algoritam staje.

4) Ako

$$\|b_1\| < (p^{kd} \cdot \|F\|^{-m})^{1/n},$$

tada je $\deg(H_0) = m + 1 - t \leq m$ i $H_0 = \gcd(b_1, b_2, ..., b_t)$, pri čemu je t definiran u korolaru 4.1.7.

Algoritam *B*

Neka je dan polinom F s cjelobrojnim koeficijentima stupnja n, prost broj p i polinom H s cjelobrojnim koeficijentima koji ima svojstva 1) - 4) iz definicije 4.1.4 pri čemu je $k = 1$. Pretpostavimo da su koeficijenti od H reducirani modulo p. Algoritam računa ireducibilni djelitelj H_0 polinoma F, pri čemu $H(\mathrm{mod}\ p)$ dijeli $H_0(\mathrm{mod}\ p)$.

Koraci algoritma B:
1) Neka je $d = \deg(H)$. Ako je $d = n$, tada $H_0 = F$. Algoritam staje.
Inače, $d < n$ i algoritam računa najmanji k za kojeg vrijedi

$$p^{kd} \geq 2^{m(n-1)/2} \cdot \binom{2m}{m}^{(n-1)/2} \cdot \|F\|^m \cdot M(F)^{n-1}.$$

2) Koristeći Henselovu lemu, modificiramo H tako da sada u svojstvu 2) u definiciji 4.1.4 broj k predstavlja broj izračunat u prvom koraku. I dalje svojstva pod 1), 3) i 4) moraju biti zadovoljena. Možemo pretpostaviti da koeficijenti polinoma H reducirani modulo p^k.

3) Neka je u, najveći cijeli broj tako da $d \leq (n-1)/2^u$. U ovom koraku algoritam B primjenjuje algoritam A na

$$m = \lfloor (n-1)/2^u \rfloor, \lfloor (n-1)/2^{u-1} \rfloor, ..., \lfloor (n-1)/2 \rfloor, n-1.$$

Algoritam staje kada za neku od ovih vrijednosti m pronađe odgovarajući H_0.

4) Ako za nijednu vrijednost m, odgovarajući H_0 nije pronađen, tada $\deg(H_0) > n - 1$ i $H_0 = F$.

Koraci LLL algoritma

Neka je $F \in \mathbb{Z}[X]$ primitivni polinom stupnja $n \geq 1$. Koraci LLL -algoritma su:

1) Treba izračunati F' te rezultantu polinoma F i F'.

2) Ako je $Res(F, F') = 0$, tada označimo $G = \gcd(F, F')$ i $F_0 = F/G$. Budući da je polinom F_0 kvadratno slobodan u $\mathbb{Z}[X]$, slijedi da $Res(F_0, F_0') \neq 0$ te koristimo algoritam kako bi faktorizirali polinom F_0. Kako svaki ireducibilan djelitelj polinoma G dijeli F_0, možemo završiti faktorizaciju polinoma $F = F_0 \cdot G$ koristeći konačno mnogo dijeljenja.

3) Ako je $Res(F, F') \neq 0$, algoritam računa prost broj p koji ne dijeli rezultantu. Tada $F(\text{mod } p)$ ima stupanj $n = \deg(F)$ i nema više istih djelitelja u $\mathbb{F}_p[X]$. Tada je svojstvo 4) definicije 4.1.4. zadovoljeno s bilo kojim ireducibilnim djeliteljem $H(\text{mod } p)$ polinoma $F(\text{mod } p)$ na $\mathbb{F}_p$.

4) Koristeći Berlekampov algoritam, LLL-algoritam računa faktorizaciju od $F(\text{mod } p)$ u $\mathbb{F}_p[X]$.

5) Pretpostavimo da je moguća trivijalna faktorizacija polinoma F tako da je $F = F_1 F_2$, pri čemu su faktori od F_1 u $\mathbb{Z}[x]$ i faktori od $F_2(\text{mod } p)$ u $\mathbb{F}_p[X]$ poznati.

6) Ako je $F_2 = \pm 1$, tada je $F = \pm F_1$ i algoritam staje. Inače, algoritam računa ireducibilan djelitelj $H(\text{mod } p)$ polinoma $F_2(\text{mod } p)$ u $\mathbb{F}_p[X]$. Možemo pretpostaviti da su koeficijenti polinoma H reducirani modulo p te da je H normirani polinom. Tada možemo primijeniti algoritam B na polinom F_2.

7) Koristeći algoritam B, LLL-algoritam računa ireducibilni djelitelj H_0 polinoma F_2 tako da $H(\text{mod } p)$ dijeli $H_0(\text{mod } p)$.

8) LLL -algoritam u ovom koraku mijenja F_1 sa $F_1 H_0$ i F_2 sa F_2/H_0. Od svih ireducibilnih faktora polinoma $F_2(\text{mod } p)$, algoritam "briše" faktore koji dijele $H_0(\text{mod } p)$. Nakon toga, algoritam se vraća na 6. korak.

4.3 Složenost

Za razliku od Berlekampovog algoritma koji ima eksponencijalnu složenost, LLL-algoritam ima polinomijalnu složenost. Primijetimo da složenost LLL-algoritma ovisi o složenosti algoritma za redukciju baze te o složenosti algoritama A i B. Broj operacija koje se izvršavaju u algoritmu A jednak je $O(m^4 k \log p)$, a cijeli brojevi na kojima se te operacije izvršavaju imaju binarnu duljinu $O(mk \log p)$. Što se tiče algoritma B, najveći broj operacija koje se trebaju izvršiti je

$$O(m_0(n^5 + n^4 \log ||F|| + n^3 \log p)),$$

a cijeli brojevi nad kojima se te operacije izvršavaju imaju binarnu duljinu

$$O(n^3 + n^2 \log ||F|| + n \log p).$$

(vidi [5, str. 280.])

Teorem 4.3.1. *LLL -algoritam za faktorizaciju normiranog polinoma F s cjelobrojnim koeficijentima stupnja n na ireducibilne faktore, treba najviše izvršiti $O(n^6 + n^5 log||F||)$ operacija. Za cijele brojeve nad kojima se te operacije izvode binarna duljina iznosi $O(n^3 + n^2 \log ||F||)$.*
(dokaz [5, str. 281.])

Bibliografija

[1] Y. Bugeaud, *Aproximation by Algebraic Numbers*, Cambridge University Press, Cambridge, 2004.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, Berlin, 1996.

[3] B. Dakić, B. Pavković, *Polinomi*, Školska knjiga, Zagreb, 1989.

[4] M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.

[5] M. Mignotte, D. Stefanescu, *Polynomials. An Algorithmic Approach*, Springer, Singapore, 1999.

Sažetak

Diplomski rad podijeljen je na četiri poglavlja. Prvo poglavlje čine osnovni teoremi i svojstva polinoma koja se koriste u radu. U preostala tri poglavlja su opisana tri osnovna algoritma za faktorizaciju polinoma: Kroneckerov algoritam, Berlekampov algoritam i LLL-algoritam. Svako poglavlje, koje opisuje jedan algoritam, podijeljeno je na tri dijela. Prvi dio se sastoji od teorema koji su nam potrebni za razumijevanje algoritma. U drugom dijelu, algoritam je raspisan po koracima, dok je u trećem dijelu komentirana složenost algoritma.

Summary

This master's thesis consists of four chapters, first of which contains theorems and properties of polynomials being used in it. Remaining three chapters focus on three main algorithms for factorization of polynomials: algorithm of Kronecker, algorithm of Berklamp, and, ultimately, the LLL- algorithm. Every chapter takes one of the mentioned algorithms and breaks it down in three parts. First part introduces all theorems needed for proper understanding of the algorithm itself, while the second part describes the algorithm in question going through it step by step. Finally, third part of every chapter comments on the complexity of the given algorithm.

Životopis

Rođena sam 19.9.1992. godine u Sisku. Godine 2011. završavam srednju školu Gimnazija Sisak s odličnim uspjehom te upisujem sveučilišni preddiplomski studij Matematika; smjer: nastavnički na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu. Pored studija, profesiju nastavnika sam usavršavala putem instrukcija iz matematike i informatike te kao demonstrator iz kolegija "Konstruktivne metode u geometriji". Nakon završetka preddiplomskog studija, 2015. godine upisujem sveučilišni diplomski studij Matematika i informatika. U slobodno vrijeme bavim se latinsko-američkim i standardnim plesovima te 2016. godine postajem članom šire reprezentacije Republike Hrvatske u kombinaciji 10 plesova.