Polinomi u Z[x] i Q[x]

Bolješić, Luka

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:514084

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science







Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Luka Bolješić

Polinomi u $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$

Diplomski rad

Osijek, 2018.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Luka Bolješić

Polinomi u $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2018.

Sadržaj

Uvod **i**

1 Polinomi u $\mathbb{Q}[x]$ **1**
1.1 Gaussova lema 1
1.2 Provjera ireducibilnosti 7
1.3 Polinomi modulo $\boldsymbol{p}$ koji se mogu faktorizirati za svaki prost broj $\boldsymbol{p}$ . . 12

2 Kongruencije i Kineski teorem o ostatcima **15**
2.1 Kongruencija modulo polinom 15
2.2 Kineski teorem o ostatcima 24
2.3 Metoda Lagrangeove interpolacije 25
2.4 Faktoriziranje polinoma u $\mathbb{Z}[x]$ je konačan proces 28

3 Brzo množenje polinoma **31**

Literatura **39**

Sažetak **40**

Summary **41**

Životopis **42**

Uvod

U ovom diplomskom radu bavit ćemo se faktorizacijom polinoma u $\mathbb{Q}[x]$ i Kineskim teoremom o ostatcima za polinome. Za polinom s koeficijentima iz polja kažemo da je ireducibilan ako se ne može prikazati kao umnožak polinoma stupnja većeg ili jednakog 1. Inače kažemo da je reducibilan. U radu ćemo pokazati dva načina kako provjeriti je li polinom ireducibilan u $\mathbb{Q}[x]$. U jednom načinu na polinome ćemo djelovati s modulo p, gdje je p prost broj, a u drugom načinu koristimo Eisensteinov kriterij. Nećemo promatrati polinome iz $\mathbb{C}[x]$ jer je polje $\mathbb{C}$ algebarski zatvoreno pa je svaki nekonstantan polinom reducibilan i nećemo promatrati polinome u $\mathbb{R}[x]$ jer ih je teže faktorizirati nego polinome u $\mathbb{Q}[x]$. Vidjet ćemo da polinomi iz $\mathbb{Q}[x]$ imaju jednaku faktorizaciju do na invertibilni element kao polinomi iz $\mathbb{Z}[x]$, te ćemo dokazati Gaussovu lemu koja omogućava da kod faktorizacije polinoma s cjelobrojnim koeficijentima možemo pretpostaviti da faktori imaju cjelobrojne koeficijente. Zbog toga su u primjerima pretežito korišteni polinomi iz $\mathbb{Z}[x]$. Na kraju prvog poglavlja dat ćemo primjere polinoma modulo p koji su reducibilni za svaki prost broj p u $\mathbb{Z}_p[x]$.

U drugom poglavlju definirat ćemo kongruenciju modulo polinom i vidjet ćemo da su svojstva kongruencija za polinome identična svojstvima za cijele brojeve. Kako su svojstva kongruencija identična, vidjet ćemo da Kineski teorem o ostatcima vrijedi i za polinome i dokazat ćemo taj teorem. Kineski teorem o ostatcima nam osigurava jedinstvenost polinoma dobivenog Lagrangeovom metodom interpolacije stupnja manjeg ili jednakog d koji prolazi kroz $d+1$ danih točaka, te ćemo Lagrangeov interpolacioni polinom koristiti za traženje faktorizacije polinoma iz $\mathbb{Z}[x]$. Vidjet ćemo da je faktoriziranje polinoma u $\mathbb{Z}[x]$ konačan proces jer racionalna nultočka polinoma u $\mathbb{Z}[x]$ ovisi o djeliteljima slobodnog i vodećeg koeficijenta kojih ima konačno mnogo. U trećem poglavlju navest ćemo i opisati metodu od 3 koraka za brzo množenje polinoma koja je učinkovitija od klasične metode. Metoda od 3 koraka je učinkovitija u smislu da je za izračunavanje produkta dva polinoma potrebno manje množenja nego kod klasične metode.

1 Polinomi u $\mathbb{Q}[x]$

U ovom poglavlju razmatrat ćemo kako faktorizirati polinome s racionalnim koeficijentima.

Ovdje je situacija dosta drugačija nego kod polinoma s koeficijentima u $\mathbb{R}$ ili $\mathbb{C}$. Nad poljem $\mathbb{Q}$ imamo mnogo ireducibilnih polinoma svakog stupnja i provjeravanje ireducibilnosti polinoma je teško u odnosu na polinome nad $\mathbb{R}$ ili $\mathbb{C}$. S druge strane, traženje nultočki (odnosno ireducibilnih faktora stupnja 1) polinoma u $\mathbb{Q}[x]$ je lagano i mi ćemo navesti dvije različite procedure za traženje faktorizacije polinoma bilo kojeg stupnja s racionalnim koeficijentima u konačno mnogo koraka.

Polazište za sve rezultate u $\mathbb{Q}[x]$ je činjenica da je faktoriziranje u $\mathbb{Q}[x]$ "jednako" faktoriziranju u $\mathbb{Z}[x]$. Prvi dio ovog poglavlja posvećen je objašnjavanju te činjenice.

1.1 Gaussova lema

Podsjetimo se da ako su $f(x)$ i $g(x)$ dva polinoma s koeficijentima u polju F i ako postoji ne-nul element $c \in F$ takav da je $f(x) = cg(x)$, onda su polinomi $f(x)$ i $g(x)$ asocirani. Asocirani polinomi imaju jednaku faktorizaciju u obliku produkta ireducibilnih polinoma do na invertibilni element i poredak faktora.

Ako je $f(x) = a_n x^n + \ldots + a_1 x + a_0$ polinom s racionalnim koeficijentima, onda možemo pomnožiti $f(x)$ s najmanjim zajedničkim višekratnikom nazivnika koeficijenata, nazovimo taj broj sa s. Množenjem dobivamo polinom $g(x) = sf(x)$ kojemu su koeficijenti cijeli brojevi i koji je asociran s polinomom $f(x)$ u $\mathbb{Q}[x]$. Ako imamo faktorizaciju od $f(x)$, množenjem jednog od faktora sa s dobit ćemo faktorizaciju polinoma $g(x)$. Direktno slijedi da polinomi $g(x)$ i $f(x)$ imaju jednake faktorizacije u $\mathbb{Q}[x]$ do na invertibilni element s. Dakle, kada promatramo faktorizaciju polinoma iz $\mathbb{Q}[x]$ uvijek možemo pretpostaviti da polinom ima cjelobrojne koeficijente, to neće utjecati na faktorizaciju.

Definicija. Kažemo da je polinom $f(x)$ iz $\mathbb{Q}[x]$ primitivan ako ima cjelobrojne koeficijente i najveći zajednički djelitelj tih koeficijenata je 1.

Svaki polinom $f(x)$ s cjelobrojnim koeficijentima asociran je s nekim primitivnim polinomom: jednostavno podijelimo $f(x)$ s najvećim zajedničkim djeliteljem njegovih koeficijenata, dobiveni polinom je primitivan i asociran je s $f(x)$. Za-

ključujemo da je svaki polinom u $\mathbb{Q}[x]$ asociran s primitivnim polinomom. Primjerice, polinom koji je primitivan i asociran s $3x^3 + \frac{7}{2}x + \frac{4}{3}$ je

$$18x^3 + 21x + 8 = 6\left(3x^3 + \frac{7}{2}x + \frac{4}{3}\right).$$

Pogodan način za određivanje primitivnih polinoma je djelovanje na njih modulo p.

Neka je p prost broj. Ako imamo polinom $f(x)$ s cjelobrojnim koeficijentima lako možemo dobiti polinom s koeficijentima iz $\mathbb{Z}/p\mathbb{Z}$ tako da zamijenimo koeficijente od $f(x)$ s klasama kongurencije tih koeficijenata modulo p. Neka je γ_p preslikavanje koje prebacuje koeficijente iz $\mathbb{Z}$ u koeficijente iz $\mathbb{Z}/p\mathbb{Z}$. Ako imamo polinom

$$a_n x^n + \ldots + a_1 x + a_0$$

s cjelobrojnim koeficijentima, onda je

$$\gamma_p(a_n x^n + \ldots + a_1 x + a_0) = [a_n]x^n + \cdots + [a_1]x + [a_0],$$

gdje je $[a_i] = \{a_i + kp : k \in \mathbb{Z}\}$, $i = 0, \ldots, n$. Polinom $f(x)$ u $\mathbb{Z}[x]$ je primitivan ako i samo ako ne postoji prost broj koji dijeli sve njegove koeficijente, odnosno ako i samo ako za svaki prost broj p vrijedi $\gamma_p(f(x)) \neq 0$. Pogledajmo kako djeluje preslikavanje γ_3,

$$\gamma_3(18x^3 + 21x + 8) = [2]_3.$$

Primijetimo da je preslikavanje $\gamma_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ homomorfizam, jer vrijedi

$$\gamma_p(f(x)g(x)) = \gamma_p(f(x)) \cdot \gamma_p(g(x))$$

za sve polinome $f(x)$, $g(x)$ iz $\mathbb{Z}[x]$.

Korištenjem preslikavanja γ_p lako dokazujemo:

Propozicija 1. *Produkt dva primitivna polinoma je primitivan polinom.*

Dokaz. Neka su $f(x)$ i $g(x)$ primitivni. Tada je za svaki prost broj p, $\gamma_p(f(x)) \neq 0$ i $\gamma_p(g(x)) \neq 0$. Kako je $\mathbb{Z}_p$ polje, onda $\mathbb{Z}_p[x]$ nema djelitelje nule. Slijedi da je $\gamma_p(f(x)g(x)) = \gamma_p(f(x)) \cdot \gamma_p(g(x)) \neq 0$. Kako to vrijedi za svaki prost broj p, polinom $f(x)g(x)$ je primitivan. □

Dokazat ćemo lemu koja će nam trebati:

Lema 2. *Neka je $g(x)$ primitivan, $f(x)$ polinom u $\mathbb{Z}[x]$ i $f(x) = ag(x)$ za neki racionalan broj a. Tada je $a \in \mathbb{Z}$ i ako je $f(x)$ također primitivan, onda je $a = 1$ ili -1.*

Dokaz. Neka je $a = \frac{r}{s}$, te za r i s vrijedi $(r, s) = 1$. Tada je

$$sf(x) = rg(x).$$

Kako su r i s relativno prosti, s dijeli sve koeficijente od $g(x)$. Međutim, kako je $g(x)$ primitivan slijedi da je $s = 1$ ili -1, odnosno $a \in \mathbb{Z}$. Ako je $f(x)$ primitivan, isto kao i za s, slijedi da je $r = 1$ ili -1, pa je $a = 1$ ili -1. □

Sada možemo pokazati glavni rezultat ovog poglavlja:

Teorem 3 (Gaussova lema)**.** *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima i $f(x) = a(x)b(x)$, gdje su $a(x)$, $b(x) \in \mathbb{Q}[x]$. Tada postoje polinomi $a_1(x)$, $b_1(x) \in \mathbb{Z}[x]$ koji su asocirani s polinomima $a(x)$ i $b(x)$ takvi da $f(x) = a_1(x)b_1(x)$.*

Ukoliko tražimo faktorizaciju polinoma s cjelobrojnim koeficijentima, Gaussova lema nam omogućava da možemo tražiti samo faktore s cjelobrojnim koeficijentima. Prije dokaza promotrit ćemo primjer.

Primjer 1. Promotrimo polinom

$$x^4 - 2x^2 + x + 3.$$

Tražimo faktorizaciju tog polinoma takvu da su faktori polinomi drugog stupnja:

$$x^4 - 2x^2 + x + 3 = (x^2 + ax + b)(x^2 + cx + d).$$

Ako postoji takva faktorizacija u $\mathbb{Q}[x]$, onda prema Gaussovoj lemi postoji faktorizacija u kojoj su koeficijenti a, b, c, d cijeli brojevi. Množenjem desne strane dobivamo:

$$x^4 - 2x^2 + x + 3 = x^4 + (c + a)x^3 + (b + d + ac)x^2 + (ad + cb)x + bd.$$

Izjednačavajući koeficijente uz x^3 dobivamo $c = -a$. Ako to iskoristimo i izjednačimo koeficijente uz ostale odgovarajuće potencije od x dobivamo:

$$\begin{aligned} -2 &= b + d - a^2, \\ 1 &= ad - ab = a(d - b), \\ 3 &= bd. \end{aligned}$$

Kako su a, b i d cijeli brojevi, iz druge jednadžbe dobivamo $d - b = 1$ ili -1, odnosno d i b se razlikuju za 1; dok iz treće jednadžbe dobivamo $b = \pm 1, d = \pm 3$ ili $b = \pm 3, d = \pm 1$. Time smo dobili kontradikciju jer se b i d ne razlikuju za 1, pa ne postoji tražena faktorizacija danog polinoma.

Da nismo mogli pretpostaviti da su a, b i d cijeli brojevi, imali bismo beskonačno mogućnosti za a, b i d, te bi pokazivanje da sustav jednadžbi nemaju rješenje za sve moguće a, b i d bilo znatno teže.

Dokaz Gaussove leme. Neka je $f(x) \in \mathbb{Z}[x]$ i pretpostavimo da je $f(x) = a(x)b(x)$, gdje su $a(x), b(x) \in \mathbb{Q}[x]$. Neka su $a_1(x), b_1(x) \in \mathbb{Z}[x]$ primitivni polinomi koji su asocirani s $a(x), b(x)$. Imamo

$$a(x) = ca_1(x),\ b(x) = db_1(x),$$

gdje su $c, d \in \mathbb{Q}$. Tada je

$$f(x) = cda_1(x)b_1(x).$$

Prema Propoziciji 1, $a_1(x)b_1(x)$ je primitivan polinom, a prema Lemi 2 je $cd \in \mathbb{Z}$. Zapišimo preglednije

$$f(x) = (cda_1(x))b_1(x).$$

Vidimo da smo dobili faktorizaciju u $\mathbb{Z}[x]$ u kojoj je polinom $cda_1(x)$ asociran s $a(x)$, a polinom $b_1(x)$ je asociran s $b(x)$. Time smo dobili traženu tvrdnju. □

Korolar 4. *Neka je $f(x) \in \mathbb{Z}[x]$ i $f(x) = g(x)h(x)$, gdje su $g(x), h(x) \in \mathbb{Q}[x]$ i $g(x)$ je primitivan, onda je $h(x) \in \mathbb{Z}[x]$.*

Dokaz. Prema Gaussovoj lemi imamo $f(x) = cg(x)dh(x)$, gdje su $c, d \in \mathbb{Q}$ takvi da $cd = 1$ i $cg(x), dh(x) \in \mathbb{Z}[x]$. No, kako je $cg(x) \in \mathbb{Z}[x]$ i $g(x)$ primitivan, tada je po Lemi 2, $c \in \mathbb{Z}$. Slijedi $h(x) = cdh(x) = c(dh(x)) \in \mathbb{Z}[x]$. □

Koristeći Korolar 4 dokazat ćemo poznati Descartesov kriterij za određivanje nultočki polinoma s cjelobrojnim koeficijentima.

Teorem 5. *Neka je*

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

polinom iz $\mathbb{Z}[x]$. Ako je $\frac{r}{s}$ racionalna nultočka od $f(x)$, gdje su $r, s \in \mathbb{Z}$ takvi da $(r, s) = 1$, onda s dijeli a_n, a r dijeli a_0.

Dokaz. Kako je $\frac{r}{s}$ nultočka polinoma, možemo pisati $f(x) = (sx - r)g(x)$ gdje je

$$g(x) = b_{n-1}x^{n-1} + \ldots + b_1x + b_0$$

polinom u $\mathbb{Q}[x]$. Kako je $sx - r$ primitivan polinom, po Korolaru 4, vrijedi $g(x) \in \mathbb{Z}[x]$. Iz $f(x) = (sx - r)g(x)$ slijedi $b_{n-1}s = a_n$ i $(-b_0)r = a_0$, odnosno s dijeli a_n i r djeli a_0. □

Pokažimo još jedan dokaz:

Dokaz. Pošto je $\frac{r}{s}$ nultočka polinoma $f(x)$, vrijedi

$$0 = f\left(\frac{r}{s}\right) = a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\frac{r}{s} + a_0.$$

Množenjem prethodne jednakosti sa s^n dobivamo

$$0 = s^n f\left(\frac{r}{s}\right) = a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n.$$

Iz jednakosti

$$-(a_{n-1}r^{n-1} + \cdots + a_0 s^{n-1})s = a_n r^n$$

slijedi da s dijeli $a_n r^n$, no kako su r i s relativno prosti, s dijeli a_n. Dok iz jednakosti

$$-(a_n r^{n-1} + \cdots + a_1 s^{n-1})r = a_0 s^n$$

slijedi da r dijeli $a_0 s^n$, te kako su r i s relativno prosti, r dijeli a_0. □

Kako a_n i a_0 imaju konačan broj djelitelja, prethodni teorem kaže da je traženje racionalnih nultočki polinoma s cjelobrojnim koeficijentima reducirano na testiranje konačnog skupa racionalnih brojeva $\frac{r}{s}$ koji ovise o a_n i a_0.

Primjer 2. Jedine moguće nultočke polinoma

$$x^3 - 7x^2 + 8x + 3$$

su $x = 1, -1, 3$ i -3, četiri djelitelja broja 3.

Primjer 3. Promotrimo polinom

$$g(x) = x^5 + x^4 - 3x^3 + 141x^2 - x + 5040.$$

Kako je $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, broj 5040 ima 120 djelitelja. Descartesov kriterij kaže da imamo 120 potencijalnih nultočki polinoma $g(x)$, što je još uvijek puno. U [2] možemo pronaći kako smanjiti broj potencijalnih nultočki.

Sljedeći primjer pokazuje kako možemo poboljšati Descartesov kriterij.

Primjer 4. Promotrimo koliko je potencijalnih nultočaka polinoma

$$f(x) = x^4 + x^3 - 5x^2 - 2x + 8.$$

Kako broj 8 ima 8 djelitelja imamo 8 potencijalnih nultočaka polinoma $f(x)$. Primijetimo da $f(1) = 3$ ima samo 4 djelitelja. Ako je x_0 nultočka polinoma $f(x)$, onda je $x_0 \in \mathbb{Z}$ jer je polinom normiran. Znamo da $x - x_0$ dijeli $f(x)$ u $\mathbb{Z}[x]$, pa vrijedi

$$1 - x_0 \text{ dijeli } f(1) = 3.$$

Potencijalna nultočka x_0 od $f(x)$ mora zadovoljavati

$$\begin{aligned} 1 - x_0 &= 1, \text{ ili} \\ 1 - x_0 &= -1, \text{ ili} \\ 1 - x_0 &= 3, \text{ ili} \\ 1 - x_0 &= -3. \end{aligned}$$

Slijedi da je $x_0 \in \{0, 2, -2, 4\}$. Direktnom provjerom dobivamo $f(-2) = 0$.

Prije nego što prijeđemo na sljedeće potpoglavlje, primijetimo da se faktorizacija polinoma iz $\mathbb{Q}[x]$ može svesti na faktorizaciju normiranog polinoma s cjelobrojnim koeficijentima. Neka je dan polinom

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

s cjelobrojnim koeficijentima. Ako stavimo $x = \frac{y}{a_n}$, dobivamo

$$g(y) = a_n \frac{y^n}{a_n^n} + a_{n-1} \frac{y^{n-1}}{a_n^{n-1}} + \cdots + a_1 \frac{y}{a_n} + a_0.$$

Množenjem $g(y)$ s a_n^{n-1} dobivamo

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

gdje je $h(y)$ normirani polinom s cjelobrojnim koeficijentima. Ako je $y = y_0$ nultočka polinoma $h(y)$, onda je $x = \frac{y_0}{a_n}$ nultočka polinoma $f(x)$.

1.2 Provjera ireducibilnosti

U ovom potpoglavlju pokazat ćemo dva načina kako provjeriti ireducibilnost polinoma $f(x) \in \mathbb{Q}[x]$ stupnja $d > 1$.

Jedan od načina provjere ireducibilnosti je da na polinom djelujemo s modulo m, gdje je $m > 1$.

Neka je $\gamma_m : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ homomorfizam koji mijenja koeficijente od $f(x)$ s klasama kongruencije tih koeficijenata modulo m. Ako je vodeći koeficijent invertibilan modulo m, onda je polinom $\gamma_m(f(x))$ isto stupnja d.

Neka je $f(x) = a(x)b(x)$, gdje su $a(x)$ i $b(x)$ stupnja r i s, redom, takvi da $r + s = d$ i vodeći koeficijent od $f(x)$ je invertibilan modulo m. Tada su vodeći koeficijenti od $a(x)$ i $b(x)$ također invertibilni modulo m, pa vrijedi

$$\gamma_m(f(x)) = \gamma_m(a(x)b(x)) = \gamma_m(a(x))\gamma_m(b(x)).$$

Dobili smo faktorizaciju polinoma $f(x)$ modulo m u obliku produkta polinoma stupnja r i s. Ovo razmatranje dovodi nas do sljedećeg rezultata.

Propozicija 6. *Neka je $f(x) \in \mathbb{Z}[x]$. Ako je vodeći koeficijent polinoma $f(x)$ invertibilan modulo m, za neki $m \geq 2$ i ako je $\gamma_m(f(x))$ ireducibilan, onda je $f(x)$ ireducibilan.*

Posebno, Propozicija 6 vrijedi kad je polinom $f(x)$ normiran.

Primjer 5. Neka je $f(x) = x^5-4x^4+2x^3+x^2+18x+3$. Tada je $\gamma_2(f(x)) = x^5+x^2+1$ ireducibilan polinom u $\mathbb{Z}_2[x]$, pa je $f(x)$ ireducibilan u $\mathbb{Q}[x]$.

Primjer 6. Neka je $f(x) = x^5+4x^4+2x^3+3x^2-5+11$. Tada $\gamma_2(f(x)) = x^5+x^2+x+1$ nije ireducibilan jer je $1 \in \mathbb{Z}_2$ nultočka polinoma $\gamma_2(f(x))$. Međutim, $\gamma_3(f(x)) = x^5+x^4+2x^3+2x+2$ je ireducibilan polinom u $\mathbb{Z}_3[x]$, pa je $f(x)$ ireducibilan polinom u $\mathbb{Q}[x]$.

Iz prethodnog primjera vidimo da ireducibilan polinom u $\mathbb{Q}[x]$ ne mora biti ireducibilan u $\mathbb{Z}_n[x]$ za svaki $n \in \mathbb{N}$.

Primjer 7. Neka je $f(x) = 3x^4 + 6x^3 + 12x^2 + 13x + 25$. Vidimo da je $\gamma_3(f(x)) = x + 1$. Dobili smo polinom stupnja manjeg od 4 i ne možemo ništa zaključiti o ireducibilnosti $f(x)$. Ako pak djelujemo s γ_2, dobivamo $\gamma_2(f(x)) = x^4 + x + 1$ što je ireducibilan polinom stupnja 4 u $\mathbb{Z}_2$. Slijedi da je $f(x)$ ireducibilan u $\mathbb{Q}[x]$.

Primjer 8. Neka je $f(x) = (2x-1)(x^2-x+1) = 2x^3-3x^2+3x-1$. $f(x)$ očito nije ireducibilan u $\mathbb{Q}[x]$, ali $\gamma_2(f(x)) = x^2+x+1$ je ireducibilan u $\mathbb{Z}_2[x]$. Ovaj primjer nam pokazuje da je uvjet na vodeći koeficijent u Propoziciji 6 nužan.

Propozicija 6 pokazuje da ako za neki d i m postoji ireducibilan polinom $h(x)$ stupnja d s koeficijentima iz $\mathbb{Z}_m$, onda postoji beskonačno mnogo primitivnih polinoma stupnja d s koeficijentima iz $\mathbb{Z}$ koji su ireducibilni u $\mathbb{Q}[x]$. Primjerice, svi polinomi stupnja d iz $\mathbb{Z}[x]$ na koje kad djelujemo s modulo m dobivamo $h(x)$.

Poznato je (vidjeti u [2]) da postoje ireducibilni polinomi bilo kojeg stupnja $d > 0$ iz $\mathbb{Z}_p[x]$ za svaki prost broj p. Time slijedi da za bilo koji stupanj $d > 0$ postoji beskonačno mnogo ireducibilnih polinoma u $\mathbb{Q}[x]$. Tu činjenicu možemo pokazati i pomoću sljedećeg teorema:

Teorem 7 (Eisensteinov kriterij)**.** *Neka je $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ i neka postoji prost broj p takav da p ne dijeli a_n, p dijeli $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ i p^2 ne dijeli a_0. Tada je $f(x)$ ireducibilan u $\mathbb{Q}[x]$.*

Dokaz. Neka je $n \geq 2$ i $\gamma_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ preslikavanje koje zamjenjuje koeficijente s kongruentnim klasama modulo p tih koeficijenata. Tada je $\gamma_p(f(x)) = [a_n]x^n$, gdje je $[a_n] \neq 0$ u $\mathbb{Z}_p$. Pretpostavimo da je $f(x) = g(x)h(x)$, gdje je $\deg g(x) = r \geq 1$, $\deg h(x) = s \geq 1$ i $r+s = n$. Tada je $\gamma_p(f(x)) = \gamma_p(g(x))\gamma_p(h(x))$ u $\mathbb{Z}_p[x]$. Kako je $\mathbb{Z}_p[x]$ domena jedinstvene faktorizacije, imamo $\gamma_p(g(x)) = [b]x^r$ i $\gamma_p(h(x)) = [c]x^s$, gdje je $bc \equiv a_n \pmod{p}$. Iz $\gamma_p(g(0)) = \gamma_p(h(0)) = 0$ slijedi $g(0) \equiv 0 \pmod{p}$ i $h(0) \equiv 0 \pmod{p}$. Odnosno, p dijeli $g(0)$ i $h(0)$. Slijedi da p^2 dijeli $g(0)h(0) = f(0) = a_0$, što je kontradikcija s pretpostavkom na a_0. $f(x)$ je ireducibilan. □

Primjer 9. Korištenjem Eisensteinovog kriterija možemo lagano konstruirati ireducibilne polinome. Primjerice, to su polinomi oblika

$$x^n - b$$

gdje je b djeljiv s nekim prostim brojem p, ali nije djeljiv s p^2, kao

$$x^5 - 14$$

ili

$$x^4 - 6.$$

Primjer 10. Neka je p neparan prost broj i

$$\Phi(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Stavimo $x = y + 1$ i definiramo

$$\begin{aligned} q(y) = \Phi(y+1) &= \frac{(y+1)^p - 1}{y} = \frac{1}{y}\left(\sum_{k=0}^{p} \binom{p}{k} y^{p-k} - 1\right) \\ &= y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \ldots + \binom{p}{p-2} y + \binom{p}{p-1}. \end{aligned}$$

Po Eisensteinovom kriteriju $g(y)$ je ireducibilan jer znamo da p dijeli $\binom{p}{k}$ za svaki k takav da $1 \leq k \leq p-1$, a $\binom{p}{p-1} = p$ nije djeljiv s p^2. Time slijedi da je i $\Phi(x)$ ireducibilan.

Primijetimo da su nultočke polinoma $\Phi(x)$ p-ti korijeni broja 1, osim broja 1. Kako je $\Phi(x)$ ireducibilan, $\Phi(x)$ je polinom najmanjeg stupnja čije su nultočke p-ti korijeni jedinice.

Čebiševljevi polinomi. Za svaki $n \geq 1$, Čebiševljev polinom $T_n(x)$ definiran je s $T_n(\cos\theta) = \cos(n\theta)$. Na primjer,

$$\begin{aligned} &T_1(x) = x && \text{jer je } \cos(\theta) = \cos(\theta), \\ &T_2(x) = 2x^2 - 1 && \text{jer je } 2\cos^2(\theta) - 1 = \cos(2\theta), \\ &T_3(x) = 4x^3 - 3x && \text{jer je } 4\cos^3(\theta) - 3\cos(\theta) = \cos(3\theta). \end{aligned}$$

Čebiševljevi polinomi su polinomi iz $\mathbb{Z}[x]$.

Koristeći Eisensteinov kriterij, za neki prost broj p možemo pokazati da je $T_p(x) = xQ(x)$ gdje je $Q(x)$ ireducibilan polinom u $\mathbb{Q}[x]$.

Kako bismo to pokazali, prvo ćemo pronaći formulu za $T_n(x)$ koristeći DeMoivreovu formulu

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta).$$

Ako uvrstimo $-\theta$ u prethodnu formulu dobivamo

$$(\cos(-\theta) + i\sin(-\theta))^n = \cos(-n\theta) + i\sin(-n\theta)$$

što je

$$(\cos(\theta) - i\sin(\theta))^n = \cos(n\theta) - i\sin(n\theta).$$

Zbrajanjem DeMoivreovih jednadžbi za θ i $-\theta$ dobivamo

$$2\cos(n\theta) = (\cos(\theta) + i\sin(\theta))^n + (\cos(\theta) - i\sin(\theta))^n.$$

Ako stavimo $x = \cos(\theta)$, onda je

$$i\sin(\theta) = \sqrt{\cos^2(\theta) - 1} = \sqrt{x^2 - 1}$$

za $-1 \leq x \leq 1$. Supstitucijom dobivamo

$$T_n(x) = \frac{(x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n}{2}.$$

Ovu formulu za $T_n(x)$ koristimo za dokazivanje sljedećeg teorema.

Teorem 8. *Neka je n neparan broj i $T_n(x)$ Čebiševljev polinom. Tada je*

(i) $T_n(0) = 0$;

(ii) Vodeći koeficijent polinoma $T_n(x)$ je 2^{n-1};

(iii) Koeficijent uz x u $T_n(x)$ je $(-1)^{\frac{n-1}{2}} n$;

(iv) Ako je p neparan prost broj, onda je $T_p(x) \equiv x^p \pmod{p}$.

Dokaz. Koristeći Binomni teorem dobivamo

$$\begin{aligned} T_n(x) &= \frac{(x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n}{2} \\ &= \frac{1}{2}\left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k}(\sqrt{x^2-1})^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k}(-1)^k(\sqrt{x^2-1})^k\right). \end{aligned}$$

Kad je k neparan izrazi se krate pa dobivamo

$$T_n(x) = \sum_{l=0}^{(n-1)/2} \binom{n}{2l} x^{n-2l}(x^2-1)^l.$$

Kako je $n - 2l$ neparan za sve l, dobivamo $T_n(0) = 0$. Time smo dokazali *(i)*.

Koeficijent uz x^n je

$$\sum_{l=0}^{\frac{n-1}{2}} \binom{n}{2l}.$$

Kako je n nepran, onda je

$$\begin{aligned} 2\sum_{l=0}^{\frac{n-1}{2}} \binom{n}{2l} &= \sum_{l=0}^{\frac{n-1}{2}} \binom{n}{2l} + \sum_{l=0}^{\frac{n-1}{2}} \binom{n}{n-2l} \\ &= \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n. \end{aligned}$$

Slijedi da je koeficijent uz x^n u $T_n(x)$ jednak 2^{n-1}. Time smo dokazali *(ii)*.

Koeficijent uz x postiže se jedino za $l = \frac{n-1}{2}$, pa je taj koeficijent jednak

$$\binom{n}{n-1}(-1)^{\frac{n-1}{2}} = (-1)^{\frac{n-1}{2}} n,$$

čime smo dokazali *(iii)*.

Ako je $n = p$ neparan prost broj, onda je $\binom{p}{2l} \equiv 0 \pmod{p}$ za sve $l > 0$, pa imamo

$$\begin{aligned} T_p(x) &= \sum_{l=0}^{\frac{p-1}{2}} \binom{p}{2l} x^{p-2l}(x^2-1)^l \\ &\equiv x^p \pmod{p}, \end{aligned}$$

čime smo dokazali *(iv)*.

□

Sad ćemo dokazati spomenuti rezultat:

Teorem 9. *Za svaki neparan prost broj p vrijedi $T_p(x) = xQ_p(x)$, gdje je $Q_p(x)$ ireducibilan u $\mathbb{Q}[x]$.*

Dokaz. Kako je $T_p(0) = 0$, slijedi $T_p(x) = xQ_p(x)$. Znamo da je $T_p(x) \equiv x^p \pmod{p}$, te iz toga slijedi $Q_p(x) \equiv x^{p-1} \pmod{p}$. To znači da neparan prost broj p dijeli sve koeficijente polinoma $Q_p(x)$ osim vodećeg. Iz dijela *(iii)* prethodnog teorema, slijedi da je konstantan dio polinoma $Q_p(x)$ jednak $(-1)^{\frac{p-1}{2}} p$. Koristeći Eisensteinov kriterij slijedi da je polinom Q_p ireducibilan. □

U [2] možemo pronaći dva načina kako možemo pronaći faktorizaciju polinoma $f(x)$ u $\mathbb{Q}[x]$. U jednom načinu koristi se analogon Kineskog teorema o ostatcima za polinome, a u drugom se koristi faktoriziranje polinoma $f(x)$ modulo m.

1.3 Polinomi modulo p koji se mogu faktorizirati za svaki prost broj p

U ovom potpoglavlju pokazat ćemo primjere polinoma u $\mathbb{Z}[x]$ koji se mogu faktorizirati u $\mathbb{Z}_p$ nakon što na njih djelujemo modulo p, za svaki prost broj p, ali su ireducibilni u $\mathbb{Q}[x]$. Naši primjeri bit će polinomi oblika $x^4 + ax^2 + b^2$, gdje su $a, b \in \mathbb{Z}$.

Prvo ćemo pokazati da se ti polinomi mogu faktorizirati nakon djelovanja modulo p, za svaki prost broj p, onda ćemo pronaći uvjete na a i b takve da polinomi oblika $x^4 + ax^2 + b^2$ budu ireducibilni u $\mathbb{Q}[x]$.

Propozicija 10. *Polinom $f(x) = x^4 + ax^2 + b^2$ modulo p može se faktorizirati za sve $a, b \in \mathbb{Z}$ i za svaki prost broj p.*

Dokaz. Ako je $p = 2$, onda je $f(x)$ modulo 2 kongruentno jednom od ovih polinoma:

$$\begin{aligned} &x^4 + x^2 + 1 = (x^2 + x + 1)^2 \\ &x^4 + 1 = (x^2 + 1)^2 \\ &x^4 + x^2 = x^2(x^2 + 1) = (x^2 + x)^2 \\ &x^4. \end{aligned}$$

Vidimo da navedeni polinomi nisu ireducibilni.

Neka je p neparan prost broj. Možemo izabrati s takav da je $a \equiv 2s \pmod{p}$. Tada je

$$f(x) \equiv x^4 + 2sx^2 + b^2 \pmod{p},$$

dobiveni polinom možemo zapisati na tri različita načina:

$$\begin{aligned} x^4 + 2sx^2 + b^2 &= (x^2 + s)^2 - (s^2 - b^2) \\ &= (x^2 + b)^2 - (2b - 2s)x^2 \\ &= (x^2 - b)^2 - (-2b - 2s)x^2. \end{aligned}$$

Kada bi $f(x)$ bio razlika dva kvadrata modulo p, onda bismo $f(x)$ mogli faktorizirati. Trebamo provjeriti je li neki od izraza $s^2 - b^2$, $2b - 2s$ ili $-2b - 2s$ potpun kvadrat modulo p.

Znamo da je u grupi $\mathbb{Z}_p^*$ produkt dva elementa koja nisu potpuni kvadrati potpun kvadrat. Ako $2b - 2s$ i $-2b - 2s$ nisu potpuni kvadrati modulo p, onda je njihov produkt potpun kvadrat, a on je jednak $(2s)^2 - (2b)^2 = 4(s^2 - b^2)$. Kako je 4

potpun kvadrat, slijedi da je i $s^2 - b^2$ potpun kvadrat modulo p pa se $f(x)$ modulo p može faktorizirati. □

Propozicija 11. *Za $a, b \in \mathbb{Z}$,*

$$f(x) = x^4 + ax^2 + b^2$$

može se faktorizirati u $\mathbb{Q}[x]$ ako i samo ako je barem jedan od izraza $a^2 - 4b^2$, $2b - a$ ili $-2b - a$ potpun kvadrat u $\mathbb{Z}$.

Dokaz. Ako je $a^2 - 4b^2 = c^2$ onda $f(x)$ možemo faktorizirati na sljedeći način

$$f(x) = \left(x^2 + \frac{a}{2}\right)^2 - \left(\frac{c}{2}\right)^2 = \left(x^2 + \frac{a}{2} - \frac{c}{2}\right)\left(x^2 + \frac{a}{2} + \frac{c}{2}\right).$$

Ako je $2b - a = r^2$ onda je

$$f(x) = (x^2 + rx + b)(x^2 - rx + b),$$

te ako je $-2b - a = r^2$ onda je

$$f(x) = (x^2 + rx - b)(x^2 - rx - b).$$

Obratno, ako se $f(x)$ može faktorizirati, onda je barem jedan od izraza $a^2 - 4b^2$, $2b - a$ ili $-2b - a$ potpun kvadrat u $\mathbb{Z}$.

Ako se $f(x)$ faktorizira, onda je jedan od faktora stupnja 1 ili 2. Neka $f(x)$ ima faktor stupnja 1 i neka je m nultočka od $f(x)$.

Ako je $m = 0$ onda je $b = 0$, pa je $a^2 - 4b$ potpun kvadrat.

Ako je $m \neq 0$ i $f(m) = 0$, onda je zbog parnosti $f(x)$, $f(-m) = 0$. Slijedi da $x - m$ i $x + m$ dijele $f(x)$, pa onda i $x^2 - m^2$ dijeli $f(x)$. Dakle, ako $f(x)$ ima faktor stupnja 1 različitog od x, onda $f(x)$ ima faktor stupnja 2.

Faktorizirajmo $f(x)$ u $\mathbb{Z}[x]$:

$$f(x) = (x^2 + rx + s)(x^2 + tx + u),$$

gdje su r, s, t, $u \in \mathbb{Z}$. Izjednačavajući koeficijente uz x^3 slijedi $t = -r$, a izjednačavajući koeficijente uz 1, x, x^2 dobivamo sustav:

$$\begin{aligned} us &= b^2, \\ r(u - s) &= 0, \\ s + u &= r^2 + a. \end{aligned}$$

Ako je $r = 0$, onda je $a^2 - 4b^2 = (s+u)^2 - 4su = (s-u)^2$ potpun kvadrat. Ako je $r \neq 0$, onda je $u = s$ i $s^2 = b^2$. Ako je $u = s = b$, onda je $2b - a = r^2$ potpun kvadrat, te ako je $u = s = -b$, slijedi da je $-2b - a = r^2$ potpun kvadrat. Iz svake faktorizacije od $f(x)$ slijedi da je jedan od izraza $a^2 - 4b^2$, $2b - a$ ili $-2b - a$ potpun kvadrat. □

Korolar 12. *Neka je $2b > a > 0$. Tada je $f(x) = x^4 + ax^2 + b^2$ ireducibilan u $\mathbb{Q}[x]$ ako i samo ako $2b - a$ nije potpun kvadrat u $\mathbb{Z}$.*

Dokaz. Ako je $2b > a > 0$, onda $a^2 - 4b^2 < 0$ i $-2b - a < 0$ ne mogu biti potpuni kvadrati u $\mathbb{Z}$. Tvrdnja slijedi direktno iz prethodnog teorema. □

Ako stavimo $2b - a = c$ onda prethodni korolar možemo zapisati ovako:

Korolar 13. *Neka je $0 < c < 2b$. Tada se $f(x) = x^4 + (2b - c)x^2 + b^2$ može faktorizirati u $\mathbb{Q}[x]$ ako i samo ako je c potpun kvadrat u $\mathbb{Z}$.*

Koristeći prethodni korolar lako pronalazimo ireducibilne polinome oblika $x^4 + ax^2 + b^2$. Ako stavimo $b = 10$, onda je

$$f(x) = x^4 + (20 - c)^2 + 100$$

ireducibilan u $\mathbb{Q}[x]$ za sve c takve da $0 < c < 20$, osim za $c = 1, 4, 6$ i 16.

2 Kongruencije i Kineski teorem o ostatcima

U ovom poglavlju pokazat ćemo kako se definira kongruencija za polinome s koeficijentima iz polja, te ćemo iskazati i dokazati Kineski teorem o ostatcima za polinome. Vidjet ćemo neke bitne posljedice tog teorema.

2.1 Kongruencija modulo polinom

Definirajmo kongruenciju za polinome.

Definicija. Neka je F polje i m polinom s koeficijentima iz F. Za f i g iz $F[x]$ kažemo da su kongruentni modulo m i pišemo

$$f \equiv g \pmod{m},$$

ako m dijeli $f - g$, odnosno ako je $f = g + hm$ za neki polinom h iz $F[x]$.

Osnovna svojstva. Kongruencija modulo m u $F[x]$ ima identična svojstva kongruenciji modulo m za cijele brojeve. Posebno, za aritmetička svojstva kongruencije polinoma vrijedi:

Propozicija 1. *Za $f, f_1, f_2, g, g_1, g_2, k$ iz $F[x]$ vrijedi:*

Ako je $f \equiv g \pmod{m}$, onda je $kf \equiv kg \pmod{m}$;

Ako je $f_1 \equiv g_1 \pmod{m}$ i $f_2 \equiv g_2 \pmod{m}$, onda je $f_1 + f_2 \equiv g_1 + g_2 \pmod{m}$ i $f_1 f_2 \equiv g_1 g_2 \pmod{m}$;

Ako je $f \equiv g \pmod{m}$, onda je $f^n \equiv g^n \pmod{m}$ za svaki $n \geq 0$.

Dokaz. Dokazi su identični kao za cijele brojeve. Mi ćemo dokazati svojstvo multiplikativnosti.

Ako je $f_1 \equiv g_1 \pmod{m}$, onda postoji polinom h_1 takav da $f_1 = g_1 + mh_1$. Isto tako, ako je $f_2 \equiv g_2 \pmod{m}$, onda postoji h_2 takav da $f_2 = g_2 + mh_2$. Dobivamo

$$\begin{aligned} f_1 f_2 &= (g_1 + mh_1)(g_2 + mh_2) \\ &= g_1 g_2 + m(h_1 g_2 + g_1 h_2 + mh_1 h_2). \end{aligned}$$

Slijedi

$$f_1 f_2 \equiv g_1 g_2 \pmod{m}.$$

□

Biti kongruentan modulo m za polinome je relacija ekvivalencije, kao i za cijele brojeve. Za sve $f, g, h \in F[x]$ vrijedi:

(R) (refleksivnost) $f \equiv f \pmod{m}$,

(S) (simetričnost) Ako je $f \equiv g \pmod{m}$, onda je $g \equiv f \pmod{m}$,

(T) (tranzitivnost) Ako je $f \equiv g \pmod{m}$ i $g \equiv h \pmod{m}$, onda je $f \equiv h \pmod{m}$.

S ovim svojstvima relacija biti kongruentan nalikuje na relaciju jednako.

Kod cijelih brojeva razlika između relacije biti kongruentan i jednako je u skraćivanju:

ako je $ra = rb$ i $r \neq 0$, onda je $a = b$,

dok kod relacije biti kongruentan vrijedi:

ako je $ra \equiv rb \pmod{m}$, gdje su r i m relativno prosti, onda je $a \equiv b \pmod{m}$.

Jednak rezultat imamo kod polinoma:

Propozicija 2. *Neka su f, g, h, m polinomi s koeficijentima iz polja F i $m \neq 0$. Ako je*

$$hf \equiv hg \pmod{m}$$

i h i m su relativno prosti, onda je

$$f \equiv g \pmod{m}.$$

Dokaz. Pretpostavka je ekvivalentna s

$$m \text{ dijeli } h(f - g).$$

Kako je $(m, h) = 1$, slijedi da m dijeli $f - g$. Stoga je

$$f \equiv g \pmod{m}.$$

□

Ostatak najmanjeg stupnja. Znamo da je svaki broj modulo m kongruentan s brojem iz skupa $\{0, 1, \ldots, m-1\}$. Navodimo odgovarajući rezultat za polinome:

Propozicija 3. *Neka je m polinom stupnja većeg ili jednakog 0 i $f \in F[x]$. Tada je f modulo m kongruentno jedinstvenom polinomomu stupnja manjeg od stupnja od m. Taj polinom nazivamo ostatak najmanjeg stupnja modulo m.*

Dokaz. Primijenimo Teorem o dijeljenju s ostatkom za polinome, dobivamo $f = mq + r$, gdje je $\deg(r) < \deg(m)$. Tada je $f \equiv r \pmod{m}$.

Ostatak najmanjeg stupnja r je jedinstven zbog jedinstvenosti ostatka u Teoremu o dijeljenju s ostatkom. □

Propozicija 4. *Dva polinoma a i b su kongruentni modulo m ako i samo ako su njihovi ostatci najmanjeg stupnja modulo m jednaki.*

Dokaz. Koristeći Teorem o dijeljenju s ostatkom za polinome stavimo $a = mq + r$, $b = ms + t$, gdje r i s imaju manji stupanj od stupnja od m.

Ako je $r = t$, onda je $a \equiv mq + r \equiv r \equiv t \equiv b \pmod{m}$.

Obratno, ako je $a \equiv b \pmod{m}$, onda je $r \equiv t \pmod{m}$. Slijedi da m dijeli $r - t$. Kako polinom $r - t$ ima manji stupanj od m, onda je $r - t = 0$, odnosno $r = t$. □

Propozicija 5. *Za bilo koje polje F, bilo koji element $r \in F$ i bilo koji $f(x) \in F[x]$ vrijedi*

$$f(x) \equiv f(r) \pmod{x - r}.$$

Dokaz. Znamo da ako $f(x)$ podijelimo s $(x - r)$ dobivamo ostatak $f(r)$, odnosno

$$f(x) = (x - r)q(x) + f(r),$$

gdje je $q(x)$ kvocijent. Slijedi $f(x) \equiv f(r) \pmod{x - r}$. □

Primjer 1. Neka je $m(x) = x^2 + x + 1 \in \mathbb{Z}_3[x]$. Kada podijelimo $f(x) = x^4 + 2x^2 + x + 1$ s $m(x)$ dobivamo

$$f(x) = m(x)(x^2 - x + 2) + 2.$$

Slijedi da je 2 ostatak najmanjeg stupnja od $f(x)$ modulo $m(x)$.

Još jedan način dokazivanja Propozicije 5 je da koristimo $x - r \equiv 0 \pmod{x - r}$. Tada je

$$x \equiv r \pmod{x - r}.$$

Koristeći svojstvo kongruencije dobivamo

$$x^k \equiv r^k \pmod{x-r}$$

za sve $k > 1$. Sada zamijenimo x^k s r^k kod polinoma

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

i dobivamo

$$f(x) \equiv a_n r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0 \pmod{x-r}.$$

Desna strana je $f(r)$ čime smo dobili traženu tvrdnju. Ova metoda je analogna "istjerivanju" 11 ili 9 kod brojeva. Zamislimo da se broj 366 dobije evaluiranjem polinoma $3x^2 + 6x + 6$ u 10:

$$366 = 3 \cdot 10^2 + 6 \cdot 10 + 6.$$

Kako je $10 \equiv -1 \pmod{11}$, 10^r možemo zamijeniti s $(-1)^r$ modulo 11. Time dobivamo

$$366 \equiv (-1)^2 \cdot 3 + (-1)6 + 6 \equiv 3 - 6 + 6 \equiv 3 \pmod{11}.$$

Ova se ideja koristi i kad je modul nekonstantan polinom.

Primjer 2. Neka je $m(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Tada je svaki polinom $f(x) \in \mathbb{Z}_2[x]$ modulo $m(x)$ kongruentan polinomu stupnja manjeg od 3 po Propoziciji 3. Pronaći ćemo ostatak najmanjeg stupnja za x^n, $n \geq 3$. Kako je

$$x^3 + x^2 + 1 \equiv 0 \pmod{m(x)},$$

imamo

$$\begin{aligned}
x^3 &\equiv -x^2 - 1 \equiv x^2 + 1 \pmod{m(x)},\\
x^4 &\equiv x(x^2+1) \equiv x^2 + x + 1 \pmod{m(x)},\\
x^5 &\equiv x(x^2+x+1) \equiv x + 1 \pmod{m(x)},\\
x^6 &\equiv x(x+1) \equiv x^2 + x \pmod{m(x)},\\
x^7 &\equiv x(x^2+x) \equiv 1 \pmod{m(x)}.
\end{aligned}$$

Stoga za bilo koji n, ako je $n = 7q + r$, onda je $x^n \equiv x^{7q}x^r \equiv x^r \pmod{m(x)}$.

Primjer 3. Neka je $m(x) = x^2 + x + 1 \in \mathbb{Z}_3[x]$. Za svaki n pronađimo ostatak najmanjeg stupnja modulo $m(x)$ od x^n u $\mathbb{Z}_3[x]$. Prvo primijetimo

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

stoga je

$$x^3 \equiv 1 \pmod{m(x)}.$$

Za svaki n vrijedi, ako je $n = 3q + r, r < 3$, onda je

$$x^n = x^{3q}x^r \equiv x^r \pmod{m(x)}.$$

Još znamo da je

$$x^2 \equiv -x - 1 \equiv 2x + 2 \pmod{m(x)}.$$

To ćemo iskoristiti kako bismo našli ostatak najmanjeg stupnja od $f(x) = 2x^6 + x^5 + 2x^3 + x^2 + 1$:

$$\begin{aligned} 2x^6 + x^5 + 2x^3 + x^2 + 1 &\equiv 2 + x^2 + 2 + x^2 + 1 \\ &\equiv 2x^2 + 2 \\ &\equiv 2(-x - 1) + 2 \equiv x \pmod{m(x)}. \end{aligned}$$

Navedimo Bezoutovu lemu koja će nam trebati za rješavanje linearnih kongruencija:

Lema 6 (Bezoutova lema)**.** *Za polinome $f(x)$ i $g(x)$ iz $F[x]$ postoje polinomi $a(x)$ i $b(x)$ iz $F[x]$ takvi da je $(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.*

Linearne kongruencije. Linearne kongruencije modulo polinom možemo riješiti kao što smo to radili s cijelim brojevima. Kako bismo riješili

$$au \equiv b \pmod{m},$$

za neki polinom $u \in F[x]$, pronaći ćemo najveći zajednički djelitelj od a i m. Nazovimo taj polinom s d. Ako d ne dijeli b onda kongruencija nema rješenje, jer ako je u rješenje, onda je

$$au + mv = b$$

za neki polinom v. Vidimo da d mora dijeliti b ako kongruencija ima rješenja.

Ako pak d dijeli b, onda postoji f takav da $b = df$ i po Bezoutovoj lemi možemo pronaći polinome s i t takve da

$$as + mt = d.$$

Množeći obje strane s f dobivamo

$$asf + mtf = df = b,$$

pa je $u = sf$ rješenje kongruencije

$$au \equiv b \pmod{m}.$$

Vidimo da je teorija identična kao za kongruencije u $\mathbb{Z}$.

Kao i kod cijelih brojeva, ako možemo pronaći jedno rješenje u_1 od

$$au \equiv b \pmod{m},$$

onda generalno rješenje pronalazimo tako da pronađemo sva rješenja pripadne homogene kongruencije

$$au \equiv 0 \pmod{m}.$$

Ako je u_0 rješenje homogene kongruencije, onda je $u = u_0 + u_1$ rješenje originalne nehomogene kongruencije $au \equiv b \pmod{m}$. Obratno, svako rješenje nehomogene kongruencije ima oblik $u_0 + u_1$ za neko rješenje u_0 homogene kongruencije.

Posebno, kongruencija

$$au \equiv 1 \pmod{m}$$

ima rješenje ako i samo ako su a i m relativno prosti.

Primjer 4. Neka su $m(x) = x^3 + x^2 + 2$ i $f(x) = 2x^2 + x$ iz $\mathbb{Z}_3[x]$. Želimo naći $z(x)$ takav da

$$f(x)z(x) \equiv 1 \pmod{m(x)}.$$

To je ekvivalentno traženju $z(x)$ i $w(x)$ tako da vrijedi

$$f(x)z(x) + m(x)w(x) = 1.$$

$z(x)$ i $w(x)$ ćemo pronaći koristeći Euklidov algoritam:

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

Jedinicu stavimo na lijevu stranu, ostalo na desnu:

$$\begin{aligned}1 &= (2x^2+x)-(2x+2)(x+1)\\ &= (2x^2+x)+2((x^3+x^2+2)-(2x^2+x)(2x+1))(x+1)\\ &= 2(x^3+x^2+2)(x+1)+(2x^2+x)(1+(2x+1)(x+1))\\ &= 2(x^3+x^2+2)(x+1)+(2x^2+x)(2x^2+2).\end{aligned}$$

Slijedi da je $z(x) = 2x^2 + 2$.

Potpun skup reprezentanata. Kao i kod cijelih brojeva $(\mathrm{mod}\ m)$, potpun skup reprezentanata modulo m u $F[x]$ definira se kao skup polinoma sa svojstvom da je svaki polinom iz $F[x]$ modulo m kongruentan točno jednom polinomu iz potpunog skupa reprezentanata.

Ako je polje F beskonačno (kao $\mathbb{Q}$ ili $\mathbb{R}$), onda je za svaki modul m stupnja većeg od 0, potpun skup reprezentanata beskonačan. Ako je pak polje F konačno (kao polje $\mathbb{Z}_p$, gdje je p prost), onda je potpun skup reprezentanata konačan.

Primjer 5. U Primjeru 2 pronašli smo potpun skup reprezentanata modulo $m(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

Taj potpun skup reprezentanata sadrži osam polinoma stupnja manjeg od 3 u $\mathbb{Z}_2[x]$, njegovi elementi su:

$$0, 1, x, x^2, x^2+1, x^2+x+1, x+1, x^2+x.$$

Još smo u Primjeru 2 pronašli ostatke najmanjeg stupnja od potencija od x i dobili smo

$$\begin{aligned}x &\equiv x \pmod{m(x)}\\ x^2 &\equiv x^2 \pmod{m(x)}\\ x^3 &\equiv x^2+1 \pmod{m(x)}\\ x^4 &\equiv x^2+x+1 \pmod{m(x)}\\ x^5 &\equiv x+1 \pmod{m(x)}\\ x^6 &\equiv x^2+x \pmod{m(x)}\\ x^7 &\equiv 1 \pmod{m(x)}.\end{aligned}$$

Vidimo da umjesto ostataka najmanjeg stupnja možemo koristiti sljedeći potpun skup reprezentanata

$$\{0, 1, x, x^2, x^3, x^4, x^5, x^6\}.$$

Prethodni skup pogodan je za množenje. Na primjer,

$$(x^2+x+1)(x+1) \equiv x^4 \cdot x^5 \equiv x^9 \equiv x^7 \cdot x^2 \equiv x^2,$$

ili

$$(x^2+x+1)(x^2+x) \equiv x^4 \cdot x^6 \equiv x^{10} \equiv x^3 \equiv x^2+1.$$

Polinom x je primitivan korijen modulo $x^3+x^2+1 \in \mathbb{Z}_2[x]$.

Primjer 6. Pronađimo potpun skup reprezentanata modulo $m(x) = x^2+x+1$ u $\mathbb{Z}_3[x]$ i produkt svaka dva reprezentanta. Po Teoremu o dijeljenju s ostatkom, potpun skup reprezentanata modulo $m(x)$ sadrži polinome stupnja manjeg od 2, odnosno polinome oblika $ax+b$, gdje su $a, b \in \{0, 1, -1\}$. Imamo devet kombinacija:

$$0, 1, -1, x, x+1, x-1, -x, -x+1, -x-1.$$

Množenje tih polinoma je lakše kad je jedan od polinoma stupnja 0:

$$0 \cdot (ax+b) = 0; \qquad 1 \cdot (ax+b) = ax+b; \qquad -1 \cdot (ax+b) = -ax-b.$$

Ako su oba polinoma stupnja 1, onda je njihov produkt stupnja 2. Mi želimo zamijeniti polinome stupnja 2 kongruentnim polinomima stupnja manjim ili jednakim 1.

Kako je $m(x) = x^2+x+1$, imamo $x^2 \equiv -x-1 \pmod{m(x)}$. Iskoristimo to u sljedećem primjeru:

$$\begin{aligned} x(x-1) = x^2 - x &\equiv (-x-1) - x \\ &\equiv -2x-1 \equiv x-1 \pmod{m(x)}. \end{aligned}$$

U sljedećoj tablici prikazujemo množenje polinoma stupnja 1 modulo $m(x) = x^2 + x + 1$:

$\cdot$	x	$x+1$	$x-1$	$-x$	$-x-1$	$-x+1$
x	$-x-1$	-1	$x-1$	$x+1$	1	$-x+1$
$x+1$	-1	x	$-x+1$	1	$-x$	$x-1$
$x-1$	$x-1$	$-x+1$	0	$-x+1$	$x-1$	0
$-x$	$x+1$	1	$-x+1$	$x-1$	-1	$x-1$
$-x-1$	1	$-x$	$x-1$	-1	x	$-x+1$
$-x+1$	$-x+1$	$x-1$	0	$x-1$	$-x+1$	0

Tablica 1: Množenje polinoma stupnja 1 modulo $m(x)$

Primijetimo da su elementi nasuprot dijagonale jednaki, to je zbog komutativnosti množenja.

Iz tablice vidimo da su polinomi $x, x+1, -x, -x-1, 1, -1$ invertibilni, a polinomi $x-1, -x+1$ su djelitelji nule.

Ako je $f(x)$ invertibilan modulo $m(x)$, onda uvijek možemo riješiti kongruenciju oblika

$$f(x)z(x) \equiv h(x) \pmod{m(x)} \tag{1}$$

za $z(x)$: jednostavno obje strane pomnožimo s inverzom (modulo $m(x)$) od $f(x)$. Na primjer, u $\mathbb{Z}_3[x]$ trebamo pronaći $z(x)$ takav da

$$z(x)(x+1) \equiv x \pmod{x^2+x+1}.$$

Iz Tablice 1 vidimo da je inverz od $x+1$ jednak $-x$, pa obje strane kongruencije pomnožimo s $-x$ i dobivamo

$$z(x) \equiv -x^2 \equiv x+1 \pmod{x^2+x+1}.$$

Ako pak $f(x)$ nije invertibilan onda se može dogoditi da ne možemo riješiti jednadžbu (1). Na primjer jednadžba

$$(-x+1)z(x) \equiv x \pmod{x^2+x+1}$$

nema rješenja. To možemo vidjeti iz Tablice 1 ili možemo staviti $z(x) = ax + b$ i tražiti a i b.

Navodimo općeniti rezultat o invertibilnim elementima i djeliteljima nule modulo $m(x)$:

Propozicija 7. *Neka je F polje i $m(x) \in F[x]$ stupnja većeg od 0. Za $f(x) \in F[x]$ vrijedi:*

a) $f(x) \equiv 0 \pmod{m(x)}$ ako i samo ako $m(x)$ dijeli $f(x)$;

b) $f(x)$ je invertibilan element modulo $m(x)$ ako i samo ako je $(m(x), f(x)) = 1$;

c) $f(x)$ je djelitelj nule modulo $m(x)$ ako i samo ako $f(x)$ nije djeljiv s $m(x)$ i stupanj od $(m(x), f(x))$ je veći ili jednak od 1.

2.2 Kineski teorem o ostatcima

Vidjeli smo da puno svojstava kongruencije za cijele brojeve vrijedi i za polinome, pa nas ne bi trebalo iznenaditi što Kineski teorem o ostatcima vrijedi za polinome. Nakon što dokažemo taj teorem, pokazat ćemo kako je Kineski teorem o ostatcima povezan s interpolacijom polinoma, a pomoću interpolacije polinoma pokazat ćemo teorem koji kaže da se svaki polinom s cjelobrojnim koeficijentima može faktorizirati u konačno mnogo koraka.

Teorem 8 (Kineski teorem o ostatcima)**.** *Neka je F polje i neka su $a_1(x), \ldots, a_d(x)$ proizvoljni polinomi, te $m_1(x), \ldots, m_d(x)$ u parovima relativno prosti polinomi iz $F[x]$. Tada postoji polinom $f(x)$ iz $F[x]$ takav da*

$$\begin{aligned} f(x) &\equiv a_1(x) \pmod{m_1(x)}, \\ &\vdots \\ f(x) &\equiv a_d(x) \pmod{m_d(x)}. \end{aligned}$$

Ako su $f_1(x)$ i $f_2(x)$ rješenja prethodnog sustava kongruencija, onda je

$$f_1(x) \equiv f_2(x) \pmod{m_1(x) \cdots m_d(x)}.$$

Dokaz. Pronađimo $h_i(x)$ takav da

$$\begin{aligned} h_i(x) &\equiv 0 \pmod{m_j(x)} \text{ za } j \neq i \\ h_i(x) &\equiv 1 \pmod{m_i(x)}. \end{aligned}$$

Kako je m_i relativno prost s m_j za $i \neq j$, onda je m_i relativno prost i s produktom

$$l_i(x) = m_1(x)m_2(x) \cdots m_{i-1}(x)m_{i+1} \cdots m_{d-1}m_d(x).$$

Koristeći Bezoutovu lemu možemo pronaći polinome $k_i(x)$ i $g_i(x)$ takve da

$$1 = g_i(x)m_i(x) + k_i(x)l_i(x).$$

Ako stavimo $h_i(x) = k_i(x)l_i(x)$, onda je

$$\begin{aligned} h_i(x) &\equiv 0 \pmod{m_j(x)} \text{ za } j \neq i \\ h_i(x) &\equiv 1 \pmod{m_i(x)}, \end{aligned}$$

s time smo pronašli traženi $h_i(x)$. Stavimo li

$$f_0(x) = a_1(x)h_1(x) + a_2(x)h_2(x) + \cdots + a_d(x)h_d(x),$$

iz prethodnih kongruencija vidimo da je $f_0(x)$ traženo rješenje sustava. Neka je $f(x)$ još jedno rješenje sustava. Tada je

$$f(x) \equiv f_0(x) \pmod{m_1(x) \cdots m_d(x)},$$

jer su svi $m_i(x)$ u parovima relativno prosti. Odatle slijedi da postoji jedinstveno rješenje danog sustava kongruencija čiji je stupanj manji od stupnja polinoma $m_1(x) \cdots m_d(x)$. □

Sad ćemo navesti i dokazati posljedicu Kineskog teorema o ostatcima za polinome koja će nam trebati u sljedećem potpoglavlju.

Korolar 9. *Neka su dani elementi $n_0, \ldots, n_d$ iz polja F. Za bilo koje elemente $s_0, s_1, \ldots, s_d$ iz F postoji jedinstven polinom $q(x) \in F[x]$ stupnja manjeg od $d+1$ takav da*

$$q(n_i) = s_i, \quad i = 0, \ldots, d.$$

Dokaz. Primijetimo da su polinomi $x - n_i$ i $x - n_j$ relativno prosti za različite n_i i n_j. Prema Kineskom teoremu o ostatcima postoji jedinstven polinom $q(x)$ stupnja manjeg od stupnja polinoma $(x - n_0)(x - n_1) \cdots (x - n_d)$ za koji vrijedi $q(x) \equiv s_i \pmod{x - n_i}$, gdje je $i = 0, 1, \ldots, d$. Slijedi da je $q(x) = l(x)(x - n_i) + s_i$ za neki $l(x) \in F[x]$. Evaluacijom $q(x)$ u n_i dobivamo $q(n_i) = s_i$. □

2.3 Metoda Lagrangeove interpolacije

Korolar 9. nam pokazuje da postoji jedinstveni polinom $f(x)$ s realnim koeficijentima stupnja manjeg ili jednakog od d čiji graf $y = f(x)$ prolazi kroz $d+1$ zadanih točaka s različitim x-koordinatama. Pronalaženje polinoma čiji graf prolazi kroz dane točke nazivamo interpolacija. U ovom potpoglavlju pokazat ćemo metodu

Lagrangeove interpolacije koju ćemo poslije koristiti kod faktorizacije polinoma s cjelobrojnim koeficijentima.

Odaberimo $d+1$ različitih točaka $n_0, \ldots, n_d$. Za svaki i između 0 i d želimo pronaći polinom $h_i(x)$ takav da

$$h_i(n_i) = 1$$
$$h_i(n_j) = 0$$

za $j \neq i$. Neka je

$$g(x) = (x - n_0)(x - n_1) \cdots (x - n_d).$$

Stavimo

$$g_i(x) = \frac{g(x)}{x - n_i}.$$

Uočimo da je $g_i(n_j) = 0$ za $j \neq i$. Sada konstruiramo $h_i(x)$ na sljedeći način:

$$h_i(x) = \frac{g_i(x)}{g'(n_i)} = \frac{g(x)}{(x - n_i)g'(n_i)}$$

gdje je $g'(x)$ derivacija od $g(x)$. Znamo da je $h_i(n_i) = 0$ za $j \neq i$. Pogledajmo kako izgleda $g'(x)$,

$$\begin{aligned} g'(x) = {} & (x - n_1)(x - n_2) \cdots (x - n_d) \\ & + (x - n_0)(x - n_2) \cdots (x - n_d) \\ & + \ldots \\ & + (x - n_0)(x - n_1) \cdots (x - n_{i-1})(x - n_{i+1}) \cdots (x - n_d) \\ & + \ldots \\ & + (x - n_0)(x - n_1) \cdots (x - n_{d-1}). \end{aligned}$$

Vidimo da je $g'(n_i) = (n_i - n_0)(n_i - n_1) \cdots (n_i - n_{i-1})(n_i - n_{i+1}) \cdots (n_i - n_d) = g_i(n_i)$, pa je $h_i(n_i) = 1$. Našli smo $h_i(x)$ koji ima tražena svojstva.

Primjer 7. Neka je $d = 2$ i neka su n_0, n_1, n_2 tri različita realna broja. Pogledajmo kako izgledaju h_0, h_1, h_2:

$$h_0 = \frac{(x - n_1)(x - n_2)}{(n_0 - n_1)(n_0 - n_2)},$$

slijedi da je $h_0(n_0) = 1, h_0(n_1) = h_0(n_2) = 0$;

$$h_1 = \frac{(x - n_0)(x - n_2)}{(n_1 - n_0)(n_1 - n_2)},$$

pa je $h_1(n_1) = 1, h_1(n_0) = h_1(n_2) = 0$;

$$h_2 = \frac{(x - n_0)(x - n_1)}{(n_2 - n_0)(n_2 - n_1)},$$

slijedi da je $h_2(n_2) = 1, h_2(n_0) = h_2(n_1) = 0$.

Općenito, jednom kad pronađemo polinome $h_0(x), \ldots, h_d(x)$, onda za bilo koju uređenu $d+1$-torku $s = (s_0, s_1, \ldots, s_d)$ realnih brojeva, možemo pronaći polinom $a_s(x)$ stupnja manjeg ili jednakog d sa svojstvom $a_s(n_0) = s_0, a_s(n_1) = s_1, \ldots, a_s(n_d) = s_d$ tako da stavimo

$$a_s(x) = s_0 h_0(x) + s_1 h_1(x) + \cdots + s_d h_d(x).$$

Polinom $a_s(x)$ ima stupanj manji ili jednak d i prolazi točkama $(n_0, s_0), \ldots, (n_d, s_d)$. Takav polinom naziva se Lagrangeov interpolacioni polinom.

Primjer 8. Neka je $n_0 = -1, n_1 = 1, n_2 = 4$, onda je

$$\begin{aligned}
h_0(x) &= \frac{(x-1)(x-4)}{(-1-1)(-1-4)} = \frac{1}{10}(x^2 - 5x + 4), \\
h_1(x) &= \frac{(x+1)(x-4)}{(1+1)(1-4)} = -\frac{1}{6}(x^2 - 3x - 4), \\
h_2(x) &= \frac{(x+1)(x-1)}{(4+1)(4-1)} = \frac{1}{15}(x^2 - 1).
\end{aligned}$$

Neka je $s_0 = 4, s_1 = 17, s_2 = -10$, stavimo $s = (4, 17, -10)$. Nađimo $a_s(x)$ stupnja većeg ili jednakog 2 takav da

$$a_s(-1) = 4,\ a_s(1) = 17,\ a_s(4) = -10.$$

Po prethodno opisanom postupku, stavimo

$$\begin{aligned}
a_s(x) &= 4h_0(x) + 17h_1(x) - 10h_2(x) \\
&= \frac{2}{5}(x^2 - 5x + 4) - \frac{17}{6}(x^2 - 3x - 4) - \frac{2}{3}(x^2 - 1) \\
&= -\frac{31}{10}x^2 + \frac{13}{2}x + \frac{68}{5}.
\end{aligned}$$

Pronašli smo polinom $a_s(x)$ takav da $a_s(-1) = 4,\ a_s(1) = 17,\ a_s(4) = -10$.

Po Kineskom teoremu o ostatcima, polinom $a_s(x)$ je jedinstveni polinom stupnja manjeg ili jednakog d takav da $a_s(n_0) = s_0, a_s(n_1) = s_1, \ldots, a_s(n_d) = s_d$.

To možemo pokazati na još jedan način koristeći D'Alembertov teorem koji kaže da ne-nul polinom stupnja n iz $F[x]$, gdje je F polje, može imati najviše n različitih nultočaka. Pretpostavimo da polinomi $a(x)$ i $b(x)$ stupnja manjeg ili jednakog d imaju vrijednosti $s_0, s_1, \ldots, s_d$ u točkama $n_0, n_1, \ldots, n_d$. Tada je $c(x) = a(x) - b(x)$ polinom stupnja manjeg ili jednakog d koji ima $d+1$ nultočaka. Po D'Alembertovom teoremu to nije moguće osim ako je $c(x) = 0$. Stoga slijedi da je $a(x) = b(x)$.

2.4 Faktoriziranje polinoma u $\mathbb{Z}[x]$ je konačan proces

Ranije smo pokazali da kod faktorizacije polinoma s cjelobrojnim koeficijentima uvijek možemo pretpostaviti da i faktori imaju cjelobrojne koeficijente. Tu ćemo informaciju koristiti kako bismo opisali postupak faktoriziranja polinoma u $\mathbb{Z}[x]$ u konačno mnogo koraka. Metoda faktorizacije polinoma u konačno mnogo koraka pripisuje se Kroneckeru 1883. godine, iako ju je ranije otkrio Schubert 1793. godine. Kako se Schubertova metoda pojavila prije računala, danas postoje metode faktoriziranja koje su puno brže. Iako je u praksi spora, mi ćemo proučavati Schubertovu metodu jer algoritam za faktorizaciju polinoma u $\mathbb{Z}[x]$ kod te metode završava u konačno mnogo koraka. Schubertova metoda koristi ideju da postoji isključivo konačan skup racionalnih nultočaka polinoma s cjelobrojnim koeficijentima. Prisjetimo se od ranije, ako polinom $f(x)$ iz $\mathbb{Z}[x]$ ima vodeći koeficijent a_d i slobodan koeficijent a_0, tada svaka racionalna nultočka od $f(x)$ mora biti oblika $x = \frac{r}{s}$, gdje r dijeli a_0, a s dijeli a_d. Kako a_d i a_0 imaju konačan broj djelitelja, postoji konačno mnogo razlomaka oblika $\frac{r}{s}$ takvih da r dijeli a_0, a s dijeli a_d. Provjeravajući mogućnosti pronalazimo nultočku ili otkrivamo da polinom nema nultočaka iz $\mathbb{Q}$.

Traženje nultočaka polinoma $f(x)$ ekvivalentno je traženju faktora tog polinoma stupnja 1, jer znamo da ako je x_0 nultočka polinoma $f(x)$ onda polinom $x - x_0$ dijeli $f(x)$ i obratno.

Zbog toga ćemo koristiti Schubertovu metodu jer ona koristi interpolaciju za pronalaženje faktora danog polinoma.

Neka je $p(x) \in \mathbb{Z}[x]$ polinom koji želimo faktorizirati. Kako $p(x)$ ima cjelobrojne koeficijente tada je $p(r) \in \mathbb{Z}$ za svaki $r \in \mathbb{Z}$.

Ako je $p(x)$ stupnja m i $p(x)$ nije ireducibilan, onda $p(x)$ ima faktor stupnja manjeg ili jednakog $\frac{m}{2}$. Stavimo da je $d = \frac{m}{2}$ ako je m paran, a $d = \frac{m-1}{2}$ ako je m

neparan.

Neka su $n_0, \ldots, n_d$ međusobno različiti cijeli brojevi i $p(n_0) = r_0, \ldots, p(n_d) = r_d$. Slijedi da su $r_0, \ldots, r_d$ također cijeli brojevi. Koristeći Kineski teorem o ostatcima, za svaku uređenu $d+1$-torku $s = (s_0, \ldots, s_d)$ cijelih brojeva, gdje s_i dijeli r_i, $i = 0, \ldots, d$, možemo pronaći jedinstveni polinom $a_s(x)$ iz $\mathbb{Q}[x]$ stupnja manjeg ili jednakog d sa svojstvom $a_s(n_i) = s_i$ za svaki $i = 0, \ldots, d$. Kako svaki r_i ima konačan broj djelitelja s_i, onda postoji konačan broj mogućih s, odnosno konačan broj polinoma $a_s(x)$ za svaki s. Pokažimo da je djelitelj polinoma $p(x)$ iz $\mathbb{Z}[x]$ stupnja manjeg ili jednakog d jednak a_s za neki s.

Neka je $a(x)$ djelitelj polinoma $p(x)$, onda postoji $b(x)$ iz $\mathbb{Z}[x]$ takav da $p(x) = a(x)b(x)$. Za svaki n_i vrijedi $p(n_i) = a(n_i)b(n_i) \in \mathbb{Z}$, pa $a(n_i)$ dijeli $p(n_i) = r_i$. Odatle slijedi da su $a(n_0), \ldots, a(n_d)$ djelitelji od $r_0, \ldots, r_d$, redom. Po Kineskom teoremu o ostatcima slijedi da postoji jedinstveni polinom $a_s(x)$ stupnja manjeg ili jednakog d takav da $a_s(n_0) = a(n_0), \ldots, a_s(n_d) = a(n_d)$. Kako se $a(x)$ i a_s podudaraju u $d+1$ točaka, a stupnja su manjeg ili jednakog d, oni moraju biti jednaki. Zaključujemo da svaki djelitelj $a(x)$ polinoma $p(x)$ stupnja manjeg ili jednakog d mora biti neki od polinoma $a_s(x)$ dobiven pomoću vektora djelitelja s kojih ima konačno mnogo. Kako bismo ispitali je li polinom $p(x)$ ireducibilan u $\mathbb{Z}[x]$, podijelimo $p(x)$ sa svim polinomima $a_s(x)$. Ako pronađemo $a_s(x)$ stupnja većeg ili jednakog od 1 i manjeg ili jednakog od $\deg(p(x))/2$ koji dijeli $p(x)$, onda $p(x)$ nije ireducibilan. Inače je ireducibilan.

Iz navedenog slijedi sljedeći teorem.

Teorem 10. *Potpunu faktorizaciju bilo kojeg polinoma iz $\mathbb{Z}[x]$ moguće je ostvariti u konačno mnogo koraka.*

Primjer 9. Faktorizirajmo polinom $p(x) = x^4 - x + 1$ koristeći Lagrangeov interpolacioni polinom. Ako se $p(x)$ može faktorizirati, onda sadrži faktor stupnja manjeg ili jednakog od 2. Znamo da je $p(-1) = 3$, $p(0) = 1$, $p(1) = 1$. Za sve $s = (s_{-1}, s_0, s_1)$ koji dijele $(3, 1, 1)$ Lagrangeov interpolator $a_s(x)$ je oblika:

$$\begin{aligned} a_s(x) &= s_{-1}\frac{x(x-1)}{2} + s_0\frac{(x-1)(x+1)}{-1} + s_1\frac{x(x+1)}{2} \\ &= \left(\frac{s_1}{2} + \frac{s_{-1}}{2} - s_0\right)x^2 + \left(\frac{s_1}{2} - \frac{s_{-1}}{2}\right)x + s_0. \end{aligned}$$

Sljedeća tablica pokazuje sve moguće vektore $s = (s_{-1}, s_0, s_1)$ i odgovarajuće polinome $a_s(x)$:

$s = (s_{-1}, s_0, s_1)$	$a_s(x)$
$(3, 1, 1)$	$x^2 - x + 1$
$(1, 1, 1)$	1
$(-3, 1, 1)$	$-2x^2 + 2x + 1$
$(-1, 1, 1)$	$-x^2 + x + 1$
$(3, 1, -1)$	$-2x + 1$
$(1, 1, -1)$	$-x^2 - x + 1$
$(-3, 1, -1)$	$-3x^2 + x + 1$
$(-1, 1, -1)$	$-2x^2 + 1$
$(3, -1, 1)$	$3x^2 - x - 1$
$(1, -1, 1)$	$2x^2 - 1$
$(-3, -1, 1)$	$2x - 1$
$(-1, -1, 1)$	$x^2 + x - 1$
$(3, -1, -1)$	$2x^2 - 2x - 1$
$(1, -1, -1)$	$x^2 - x - 1$
$(-3, -1, -1)$	$-x^2 + x - 1$
$(-1, -1, -1)$	-1

Tablica 2: $s = (s_{-1}, s_0, s_1)$ i odgovarajući polinomi $a_s(x)$

Ako se $x^4 - x + 1$ može faktorizirati, možemo pretpostaviti da su faktori ireducibilni i da imaju cjelobrojne koeficijente. Kako je $x^4 - x + 1$ normiran polinom, vodeći koeficijenti njegovih faktora moraju biti 1 ili -1. Sada možemo izbaciti osam polinoma jer nemaju vodeći koeficijent jednak 1 ili -1, ili su stupnja jednakog 0, a takvi nam polinomi nisu zanimljivi. Preostaje nam šest polinoma koji su potencijalni faktori polinoma $x^4 - x + 1$:

$$\begin{array}{ll} x^2 - x + 1; & -x^2 + x - 1; \\ x^2 + x - 1; & -x^2 - x + 1; \\ x^2 - x - 1; & -x^2 + x + 1. \end{array}$$

Kako su polinomi u lijevom stupcu asocirani s polinomima u desnom stupcu, možemo provjeriti jesu li faktori polinomi samo iz lijevog stupca. Tri brza dijeljenja pokazuju da niti jedan polinom nije faktor. Slijedi da je polinom $x^4 - x + 1$ ireducibilan.

Primijetimo da broj mogućih faktora $a_s(x)$ od $p(x)$ ovisi o d, ali ovisi i o broju djelitelja od $p(n_i)$. Broj mogućih faktora u prethodnom primjeru je mali zbog činjenice da $p(0) = p(1) = 1$ ima samo dva djelitelja u $\mathbb{Z}$. Općenito, broj faktora $a_s(x)$ može biti izrazito velik.

3 Brzo množenje polinoma

U ovom poglavlju pokazat ćemo postupak od 3 koraka pomoću kojeg računamo produkt dva polinoma, te ćemo vidjeti da je taj postupak učinkovitiji od klasičnog množenja. U smislu da ćemo koristiti manje množenja.

Podsjetimo se množenja dva polinoma. Neku su dana dva polinoma stupnja d:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \text{ i } g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_dx^d.$$

Njihov produkt

$$f(x)g(x) = (a_0 + a_1x + a_2x^2 + \cdots + a_dx^d)(b_0 + b_1x + b_2x^2 + \cdots + b_dx^d)$$

dobijemo tako da a_ix^i pomnožimo sa svakim b_jx^j i onda grupiramo koeficijente uz istu potenciju od x. Time dobivamo

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{2d}x^{2d},$$

gdje je

$$\begin{aligned}
c_0 &= a_0b_0,\\
c_1 &= a_0b_1 + a_1b_0,\\
c_2 &= a_0b_2 + a_1b_1 + a_2b_2,\\
&\vdots\\
c_d &= a_0b_d + a_1b_{d-1} + \cdots + a_{d-1}b_1 + a_db_0,\\
c_{d+1} &= a_1b_d + a_2b_{d-1} + \cdots + a_{d-1}b_2 + a_db_1,\\
&\vdots\\
c_{2d} &= a_db_d.
\end{aligned}$$

Učinkovitost ove metode provjerit ćemo tako da izračunamo koliko je množenja potrebno za izračunavanje produkta. Ako su $f(x)$ i $g(x)$ stupnja d, onda oba polinoma imaju $d+1$ koeficijenata te za njihov produkt moramo svaki koeficijent od $f(x)$ pomnožiti sa svakim koeficijentom od $g(x)$. To znači da nam je potrebno $(d+1)^2$ množenja.

Pokazat ćemo metodu koja koristi Kineski teorem o ostacima i za koju je potrebno manje od $(d+1)^2$ množenja.

Množenje koristeći Kineski teorem o ostatcima. Ukratko ćemo opisati postupak učinkovitog množenja polinoma $f(x)$ i $g(x)$ stupnja d s kompleksnim koeficijentima u 3 koraka.

1. Evaluacija. Odabrati $2d+1$ različitih točaka $a_1, a_2, \ldots, a_{2d+1}$ i zatim evaluirati polinome $f(x)$ i $g(x)$ u odabranim točkama, tj. odrediti $f(a_1), \ldots, f(a_{2d+1})$ i $g(a_1), \ldots, g(a_{2d+1})$.

2. Množenje. Pomnožiti $f(a_i)$ i $g(a_i)$, $i = 1, \ldots, 2d+1$.

3. Interpolacija. Pronaći polinom $h(x)$ stupnja manjeg ili jednakog $2d$ takav da $h(a_i) = f(a_i)g(a_i)$ za $i = 1, \ldots, 2d+1$.

Ovaj postupak čini se složenijim od klasičnog množenja, ali primijetimo da u drugom koraku kod množenja imamo samo $2d+1$ množenja za razliku od $(d+1)^2$ množenja koliko ima u klasičnom množenju. Još trebamo provjeriti koliko množenja ima u prvom i trećem koraku.

Prije nego što to napravimo primijetimo da je polinom $h(x)$ zaista jednak $f(x)g(x)$. To slijedi iz Korolara 9 iz prethodnog poglavlja, jer po Korolaru 9 znamo da postoji jedinstven polinom $h(x)$ za koji vrijedi $h(a_i) = f(a_i)g(a_i)$, $i = 1, \ldots, 2d+1$. Dakle, polinomi $h(x)$ i $f(x)g(x)$ su polinomi stupnja manjeg ili jednakog $2d$ koji se podudaraju u $2d+1$ točaka, pa moraju biti jednaki. Korolar 9 slijedi iz Kineskog teorema o ostacima i zato za ovu metodu kažemo da koristimo Kineski teorem o ostatcima.

Primjer 1. Neka su $f(x) = x + 2$ i $g(x) = x - 1$. Odredimo $f(x)g(x)$ koristeći prethodni postupak. Odaberimo $a_1 = -1$, $a_2 = 0$, $a_3 = 1$. Prvi i drugi korak su brzi:

$$\begin{array}{llll} f(a_1) = 1, & g(a_1) = -2 & \Rightarrow & f(a_1)g(a_1) = -2; \\ f(a_2) = 2, & g(a_2) = -1 & \Rightarrow & f(a_2)g(a_2) = -2; \\ f(a_3) = 3, & g(a_3) = 0 & \Rightarrow & f(a_3)g(a_3) = 0. \end{array}$$

U trećem koraku interpolacijom trebamo naći polinom $h(x)$ stupnja manjeg ili jednakog 2 takav da $h(-1) = -2$, $h(0) = -2$ i $h(1) = 0$.

To ćemo postići korištenjem Lagrangeova interpolacionog polinoma. Dobivamo

$$h_0 = \frac{(x-1)(x+1)}{-1},$$
$$h_{-1} = \frac{x(x-1)}{2},$$
$$h_1 = \frac{x(x+1)}{2}.$$

Sada znamo kako izgleda $h(x)$,

$$h(x) = -2h_0(x) - 2h_{-1} + 0h_1 = x^2 + x - 2.$$

Slijedi da je $f(x)g(x) = h(x) = x^2 + x - 2$.

U prethodnom primjeru je očito da bismo brže izračunali produkt dva polinoma da smo umjesto metode od 3 koraka koristili klasično množenje.

Kako bismo prethodnu metodu napravili učinkovitijom, moramo odabrati povoljne točke $a_1, \ldots, a_{2d+1}$. U nastavku ćemo se posvetiti odabiru povoljnih točaka.

Definicija. Za element ω iz polja F kažemo da je n-ti korijen iz jedinice ako vrijedi $\omega^n = 1$, gdje je $n \in \mathbb{N}$.

Primjer 2. 1 i -1 su drugi korijeni iz jedinice u $\mathbb{R}$.

Ako je p prost broj, onda je po Fermatovom teoremu bilo koji $a \in \mathbb{Z}_p$ p minus prvi korijen iz jedinice.

Prema Osnovnom teoremu algebre polinom $x^n - 1$ ima n nultočaka u $\mathbb{C}$. Svaka nultočka od $x^n - 1$ je n-ti korijen iz jedinice u $\mathbb{C}$.

Neka je ω korijen iz jedinice u polju F. Red od ω definiramo kao najmanji eksponent $l > 0$ takav da je $\omega^l = 1$. Ako je l red od ω, onda ω zovemo primitivni l-ti korijen iz jedinice.

Primjer 3. U $\mathbb{Z}$, -1 je primitivni drugi korijen iz jedinice.

U $\mathbb{Z}_7$, 2 je primitivni treći korijen iz jedinice.

U $\mathbb{C}$, $\omega = \cos\left(\frac{2\pi}{m}\right) + i\sin\left(\frac{2\pi}{m}\right)$ je primitivni m-ti korijen iz jedinice.

Ako je ω primitivni m-ti korijen iz jedinice i $(r, m) = 1$, onda je ω^r također primitivni m-ti korijen iz jedinice.

Propozicija 1. *U $\mathbb{C}$ postoji primitivni n-ti korijen iz jedinice za svaki prirodan broj n.*

Dokaz. Tvrdnja slijedi iz činjenice da je za bilo koji n, $\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ primitivni n-ti korijen iz jedinice. □

Neka su $f(x)$ i $g(x)$ polinomi stupnja d. Neka je $2^{r-1} < 2d+1 \leq 2^r$, gdje je r prirodan broj i ω primitivni 2^r-ti korijen iz jedinice u $\mathbb{C}$. Postupak od 3 koraka bit će učinkovitiji ako polinome koje množimo evaluiramo u potencijama od ω. To ćemo i pokazati.

Teorem 2. *Neka je ω primitivni 2^r-ti korijen iz jedinice i $f(x)$ polinom stupnja $d < 2^{r-1}$. Tada evaluiranje $f(x)$ u $1, \omega, \omega^2, \ldots, \omega^{2^r-1}$ zahtijeva najviše $2^r(r-1)$ množenja.*

Dokaz. Neka je $r = 2$. Tada je zbog $d < 2^{r-1} = 2$, $d = 1$ i ω je primitivni četvrti korijen iz jedinice. Stavimo $f(x) = a_0 + a_1 x$. Kako bismo izračunali

$$\begin{aligned} f(1) &= a_0 + a_1, \\ f(\omega) &= a_0 + a_1\omega, \\ f(\omega^2) &= a_0 + a_1\omega^2 \text{ i} \\ f(\omega^3) &= a_0 + a_1\omega^3, \end{aligned}$$

trebamo napraviti najviše 4 množenja (točnije, tri: $a_1\omega, a_1\omega^2, a_1\omega^3$). Kako je $4 \leq 2^2(2-1)$, tvrdnja vrijedi za $r = 2$.

Neka je sada $r = 3$. Tada je ω primitivni osmi korijen iz jedinice i stupanj od $f(x)$ je manji od $2^{3-1} = 4$. Stavimo

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3.$$

Kako bismo lakše prebrojali množenja, stavit ćemo $y = x^2$ i $f(x)$ ćemo zapisati preglednije

$$\begin{aligned} f(x) &= (a_0 + a_2 x^2) + x(a_1 + a_3 x^2) \\ &= (a_0 + a_2 y) + x(a_1 + a_3 y) \\ &= g_0(y) + x g_1(y), \end{aligned}$$

gdje je $g_0(y) = a_0 + a_2 y$ i $g_1(y) = a_1 + a_3 y$.

Stoga je evaluirati $f(x)$ u $1, \omega, \omega^2, \ldots, \omega^7$ isto kao evaluirati $g_0(y) = g_0(x^2)$ i $g_1(y) = g_1(x^2)$ u $1, \omega^2, \omega^4$ i ω^6. Iz slučaja kada je $r = 2$ znamo da je za evaluiranje $g_0(y)$ u $1, \omega^2, \omega^4$ i ω^6 potrebno najviše četiri množenja. Isto vrijedi i za $g_1(y)$. Kako

bismo pomnožili $g_1(x^2)$ s $1, \omega, \omega^2, \ldots, \omega^7$ potrebno je 8 množenja, odnosno 7 jer ne moramo brojati množenje s 1. Dakle, za evaluiranje $f(x)$ stupnja $3 < 2^2$ u 8 potencija primitivnog osmog korijena jedinice potrebno je najviše $4 + 4 + 8 = 16$ množenja. Kako je $16 \leq 2^3(3-1)$, tvrdnja vrijedi za $r = 3$.

Slučaj za $r > 2$ je isti kao za $r = 3$.
Pretpostavimo induktivno da evaluacija polinoma $g(y)$ stupnja manjeg od 2^{r-1} u potencijama od primitivnog 2^r-tog korijena jedinice zahtijeva najviše $M_{r-1} = 2^r(r-1)$ množenja.

Neka je $f(x)$ polinom stupnja manjeg ili jednakog 2^r. Želimo evaluirati točke $1, \omega, \omega^2, \ldots, \omega^{2^{r+1}-1}$ u $f(x)$, gdje je ω primitivni 2^{r+1}-ti korijen iz jedinice. Kao što smo napravili za slučaj kad je polinom stupnja 3, zapišemo $f(x)$ kao sumu parnih potencija od x i nazovemo taj polinom $g_0(x^2)$, te na to dodamo sumu neparnih potencija od x, što možemo zapisati kao x puta $g_1(x^2)$. Dobivamo

$$f(x) = g_0(x^2) + xg_1(x^2).$$

Stavimo $y = x^2$.

Evaluirati $g_0(x^2)$ u točkama $1, \omega, \omega^2, \ldots, \omega^{2^{r+1}-1}$ je isto kao evaluirati $g_0(y)$ u točkama $1, \omega^2, \omega^4, \ldots, \omega^{2(2^{r+1}-1)}$. Primijetimo da je ω^2 primitivni 2^r-ti korijen iz jedinice, te mi evaluiramo polinom stupnja manjeg ili jednakog 2^{r-1} u potencijama od ω^2. Po pretpostavci indukcije, za to je potrebno najviše M_{r-1} množenja. Isto vrijedi i za evaluaciju polinoma $g_1(y)$ u točkama $1, \omega^2, \omega^4, \ldots, \omega^{2(2^{r+1}-1)}$. Još trebamo pomnožiti x s $g_1(y)$, gdje je $x = 1, \omega, \omega^2, \ldots, \omega^{2^{r+1}-1}$, a za to je potrebno najviše 2^{r+1} množenja. Ukupan broj množenja iznosi M_r, gdje je

$$\begin{aligned} M_r &= M_{r-1} + M_{r-1} + 2^{r+1} \\ &= 2^r(r-1) + 2^r(r-1) + 2^{r+1} = 2^{r+1}r. \end{aligned}$$

□

Za prvi korak pretpostavili smo da je $2^{r-2} \leq d < 2^{r-1}$ i evaluirali smo $f(x)$ i $g(x)$ u potencijama primitivnog 2^r-tog korijena jedinice. Po prethodnom teoremu za to je potrebno najviše $2 \cdot 2^r(r-1)$ množenja. Očito je $2^{r-1} \leq 2d < 2^r \leq 4d$, stoga je $r - 1 \leq \log_2 2d$. Time dobivamo

$$2 \cdot 2^r(r-1) \leq 8d \log_2 2d.$$

Korolar 3. *Prvi korak postupka od* 3 *koraka s kojim računamo produkt dva polinoma stupnja* d *zahtijeva najviše* $8d \log_2 2d$ *množenja.*

Primijetimo da je broj koji smo dobili znatno manji od $(d+1)^2$ za veliki d. Sjetimo se da smo za drugi korak dobili $2d+1$ množenja, što je također znatno manje od $(d+1)^2$ za veliki d. Još nam preostaje provjeriti koliko najviše množenja imamo kod interpolacije u trećem koraku.

Propozicija 4. *Neka je v primitivni l-ti korijen iz jedinice. Tada je*

$$1 + v + v^2 + \cdots + v^{l-1} = 0 \text{ ako je } v \neq 1$$

i

$$1 + v + v^2 + \cdots + v^{l-1} = l \text{ ako je } v = 1.$$

Dokaz. Ako je $v = 1$, onda je očito $1 + v + v^2 + \cdots + v^{l-1} = l$. Neka je $v \neq 1$. Kako je v primitivni l-ti korijen iz jedinice, slijedi $v^l - 1 = 0$. Znamo da je $v^l - 1 = (v-1)(1 + v + v^2 + \cdots + v^{l-1}) = 0$. Kako je $v - 1 \neq 0$, slijedi da je $1 + v + v^2 + \cdots + v^{l-1} = 0$. □

Ovaj rezultat će nam trebati za sljedeći teorem.

Teorem 5. *Neka je $l = 2^r$, ω primitivni l-ti korijen iz jedinice i*

$$h(x) = h_0 + h_1 x + \cdots + h_{l-1} x^{l-1}.$$

Za dane koeficijente $c_0 = h(1)$, $c_1 = h(\omega)$, $c_2 = h(\omega^2)$,..., $c_{l-1} = h(\omega^{l-1})$ polinoma

$$c(x) = c_0 + c_1 x + \cdots + c_{l-1} x^{l-1}$$

vrijedi

$$h(x) = \frac{c(1)}{l} + \frac{c(\omega^{l-1})}{l} x + \cdots + \frac{c(\omega^{l-(l-1)})}{l} x^{l-1}.$$

Ovaj teorem nam govori da možemo interpolirati $h(x)$ sa svojstvom $h(1) = c_0$, $h(\omega) = c_1, \ldots, h(\omega^{l-1}) = c_{l-1}$ za dane $c_0, \ldots, c_{l-1}$ tako da evaluiramo polinom $c(x)$ u točkama $1, \omega^{l-1}, \omega^{l-2}, \ldots, \omega$. Dakle, interpolacija je učinkovita kao evaluacija.

Dokaz. Iz pretpostavki slijedi $c_i = h(\omega^i) = h_0 + h_1\omega^i + h_2\omega^{2i} + \cdots + h_{l-1}\omega^{(l-1)i}$ za svaki i. Stoga, vektor

$$\boldsymbol{C} = (c_0, c_1, \ldots, c_{l-1}) = (h(1), h(\omega), h(\omega^2), \ldots, h(\omega^{l-1}))$$

možemo zapisati kao $\boldsymbol{C} = \boldsymbol{H}\boldsymbol{F}$, gdje je

$$\boldsymbol{H} = (h_0, h_1, h_2, \ldots, h_{l-1})$$

vektor koeficijenata od $h(x)$ i

$$\boldsymbol{F} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{l-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(l-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{l-1} & \omega^{2(l-1)} & \cdots & \omega \end{pmatrix},$$

matrica tipa $l \times l$. Matrica $\boldsymbol{F}$ naziva se diskretna Fourierova transformacija.

Inverz matrice $\boldsymbol{F}$ je matrica $\frac{1}{l}\hat{\boldsymbol{F}}$, gdje su elementi od $\hat{\boldsymbol{F}}$ inverzi elemenata od $\boldsymbol{F}$. Matrica $\hat{\boldsymbol{F}}$ zove se inverzna diskretna Fourierova transformacija od $\boldsymbol{F}$. Pokažimo da je $\frac{1}{l}\hat{\boldsymbol{F}}$ inverz matrice $\boldsymbol{F}$. Primijetimo da je i-ti redak matrice $\hat{\boldsymbol{F}}$ jednak

$$(1, \omega^{-i}, \omega^{-2i}, \ldots, \omega^{-(l-1)i}),$$

a j-ti stupac matrice $\boldsymbol{F}$ je dobiven transponiranjem retka

$$(1, \omega^{j}, \omega^{2j}, \ldots, \omega^{(l-1)j}).$$

Množenjem i-tog retka matrice $\hat{\boldsymbol{F}}$ i j-tog stupca matrice $\boldsymbol{F}$ dobivamo

$$\begin{aligned} q_{ij} &= 1 + \omega^{j}\omega^{-i} + \omega^{2j}\omega^{-2j} + \cdots + \omega^{(l-1)j}\omega^{-(l-1)i} \\ &= 1 + \omega^{j-i} + \omega^{2j-2i} + \cdots + \omega^{(l-1)j-(l-1)i} \\ &= 1 + \omega^{(j-i)} + \omega^{2(j-i)} + \cdots + \omega^{(l-1)(j-i)}. \end{aligned}$$

Stavimo $\zeta = \omega^{(j-i)}$, onda je ζ l-ti korijen iz jedinice. Prema propoziciji 4. vrijedi

$$q_{ij} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{l-1} = 0$$

za $i \neq j$, a za $i = j$ je $q_{ii} = l$. Stoga je $\hat{\boldsymbol{F}}\boldsymbol{F} = l\boldsymbol{I}$, gdje je $\boldsymbol{I}$ jedinična matrica tipa l. Slijedi da je $\frac{1}{l}\hat{\boldsymbol{F}}$ inverz od $\boldsymbol{F}$.

Kako je $\boldsymbol{C} = \boldsymbol{H}\boldsymbol{F}$, imamo $\boldsymbol{C}\hat{\boldsymbol{F}} = l\boldsymbol{H}$. To znači da je

$$\begin{aligned} c(1) &= lh_0, \\ c(\omega^{l-1}) &= lh_1, \\ c(\omega^{l-2}) &= lh_2, \\ &\vdots \\ c(\omega) &= lh_{l-1}, \end{aligned}$$

□

Sljedeći teorem nam govori koliko je najviše množenja potrebno za množenje dva polinoma u postupku od 3 koraka.

Teorem 6. *Neka su $f(x)$ i $g(x)$ polinomi stupnja $d < 2^{r-1}$. Postupak kojim se u tri koraka određuje produkt $f(x)g(x)$ zahtijeva najviše $2^r(3r-1)$ množenja.*

Dokaz. Pogledajmo koliko je najviše potrebno množenja za svaki korak.

1. Evaluacija $f(x)$ i $g(x)$ u potencijama od ω, gdje je ω primitivni 2^r-ti korijen iz jedinice. Za evaluaciju $f(x)$ potrebno nam je najviše $2^r(r-1)$ množenja, kao i za $g(x)$.

2. Množenje $f(\omega^i)g(\omega^i) = h(\omega^i)$ za $i = 0, 1, 2, \ldots, 2^r - 1$. Za to izračunavanje potrebno je 2^r množenja.

3. Interpolacija $h(x)$ za dane $h(w^i)$, $i = 0, 1, \ldots, 2^r - 1$. Broj množenja za taj korak jednak je broju množenja koji je potreban za evaluaciju

$$c(x) = h(1) + h(\omega)x + h(\omega^2)x^2 + \cdots + h(\omega^{2^r-1})x^{2^r-1}$$

u $x = 1, \omega^{l-1}, \omega^{l-2}, \ldots, \omega$ gdje je $l = 2^r$. Za to je potrebno $2^r r$ množenja.

Stoga za postupak od 3 koraka potrebno je najviše

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

množenja.

□

Ako je $2^{r-2} \leq d < 2^{r-1}$, tada je

$$2^r(3r-1) < 2^r 3r < 4d(3\log_2 4d).$$

Za $d \geq 103$, $4d(3\log_2 4d)$ je manje od $(d+1)^2$. Kako d raste razlomak $\frac{4d(3\log_2 4d)}{(d+1)^2}$ se približava nuli. Vidimo da je metoda od 3 koraka učinkovitija od klasičnog množenja. Kod metode od 3 koraka množili smo polinome s kompleksnim koeficijentima. Uz odgovarajuće izmjene postupak možemo primijeniti na množenje polinoma s cjelobrojnim koeficijentima.

Literatura

[1] S. Bingulac, I. Matić, *Kineski teorem o ostatcima za polinome*, Osječki matematički list, Vol. 12(2012), 105-126.

[2] L. N. Childs, *A Concrete Introduction to Higher Algebra*, 3rd ed., Springer-Verlag, New York, 2009., 339-383

Sažetak

Na početku ovog rada stavljen je naglasak na polinome s racionalnim koeficijentima te na provjeravanje njihove ireducibilnosti. Objašnjeno je zašto polinomi s racionalnim koeficijentima imaju jednaku faktorizaciju kao polinomi s cjelobrojnim koeficijentima, te je iskazana je i dokazana Gaussova lema za polinome s cjelobrojnim koeficijentima. Navedeni su brojni primjeri u kojima se provjerava ireducibilnost polinoma s cjelobrojnim koeficijentima na različite načine. U drugom dijelu iskazan je i dokazan Kineski teorem o ostatcima za polinome te su navedene neke bitne posljedice tog teorema. Na kraju je opisana metoda od tri koraka koja se koristi za brzo množenje polinoma.

Ključne riječi: ireducibilnost polinoma, kongeruencija modulo polinom, interpolacija, Kineski teoreom o ostatcima, množenje polinoma

Summary

In this master's thesis, the initial focus was on polynomials with rational coefficients and determining their ireducibility. The conclusion has been reached as to why polynomials with rational coefficients possess the same factorization as polynomials with integer coefficients. The proof for Gauss lemma for polynomials with integer coefficients has also been presented. Numerous examples that explore the ireducibility of polynomials with integer coefficients have been presented in various ways. Within the second part of this master's thesis, the Chinese polynomial remainder theorem has been presented as well as its proof and some important ramifications of this theorem were discussed. Ultimately, a three-step method used for fast polynomial multiplication was described.

Key words: ireducibility of polynomials, congruence modulo polynomial, interpolation, Chinese remainder theorem, polynomial multiplication

Životopis

Rođen sam 1. listopada 1994. u Osijeku. Osnovnu školu „Bilje“ završio sam 2009. godine. Iste godine upisao sam III. gimnaziju Osijek, te sam 2013. godine upisao Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku.