Osječki matematički list 12 (2012), 105-126

Kineski teorem o ostatcima za polinome

Suzana Bingulac* Ivan Matić †

Sažetak

U radu najprije kratko opisujemo klasični oblik Kineskog teorema o ostatcima za cijele brojeve te potom definiramo pojmove najvećeg zajedničkog djelitelja polinoma i kongruencije modulo polinom. Ovi pojmovi nam omogućuju da iskažemo i dokažemo *Kineski teorem o ostatcima za polinome*. Nakon navođenja nekih bitnih posljedica tog teorema, pokazujemo primjene na faktorizaciju polinoma i brzo množenje polinoma.

Ključne riječi: *Kineski teorem o ostatcima, kongruencije modulo polinom, interpolacija, množenje polinoma.*

Chinese remainder theorem for polynomials

Abstract

We start by giving a brief description of the classical Chinese remainder theorem for integers, after which we define the greatest common divisor of two polynomials and congruences modulo a polynomial. These concepts allow us to state and prove the Chinese remainder theorem for polynomials. After presenting some important consequences of that theorem, we give its applications to the factorization of polynomials and to fast polynomial multiplication.

Keywords: *Chinese remainder theorem, congruences modulo polynomial, interpolation, polynomial multiplication.*

*Tehnička škola, Vukovar, email: sbingula@mathos.hr
†Odjel za matematiku, Sveučilište J.J. Strossmayera u Osijeku, email: imatic@mathos.hr

1 Uvod

Kineski teorem o ostatcima se smatra jednim od fundamentalnih rezultata elementarne teorije brojeva. Osnovna važnost ovog rezultata, ime kojeg se vezuje uz kineskog matematičara Sun-Tza iz trećeg stoljeća, se nalazi u rješavanju sustava linearnih kongruencija. Podsjetimo se kako za cijele brojeve a i b kažemo da su kongruentni modulo n, gdje je n prirodan broj, ako n dijeli razliku $a - b$. U tom slučaju pišemo $a \equiv b \pmod{n}$. Više o svojstvima kongruencija će biti govora naknadno, dok brojne posljedice tih svojstava i primjene kongruencija zainteresirani čitatelj može naći u [5].

Sun-Tzu (5.st.pr.Kr.), kineski general i strateg, poznat po najstarijoj knjizi o ratovanju: Umijeće ratovanja

Sun-Tzu je postavio sljedeći problem:

"Podijeli broj s 3*, ostatak je* 2*; podijeli broj s* 5*, ostatak je* 3*; podijeli broj sa* 7*, ostatak je* 2*. Koji je to broj?"*

Primijetimo kako su brojevi s kojima dijelimo $(2, 5 \text{ i } 7)$ u parovima relativno prosti, tj. njihov najveći zajednički djelitelj je jednak jedan. Upravo je rješenje takvog problema dano idućim teoremom:

Teorem 1.1. (Kineski teorem o ostatcima) Neka su $m_1, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija

$$x \equiv a_1 \pmod{m_1}, \quad \ldots, \quad x \equiv a_r \pmod{m_r}$$

ima rješenja.
Ako je x_0 jedno rješenje, onda su sva rješenja sustava dana s $x \equiv x_0 \pmod{m_1 \cdots m_r}$.

Dokaz. Neka je $m = m_1 \cdots m_r$, te neka je $n_j = \frac{m}{m_j}$ za $j = 1, 2, \ldots, r$. Tada je $(m_j, n_j) = 1$, pa postoji cijeli broj x_j takav da je $n_j x_j \equiv a_j \pmod{m_j}$. Promotrimo broj $x_0 = n_1 x_1 + \cdots + n_r x_r$. Za njega vrijedi $x_0 \equiv n_j x_j \equiv a_j \pmod{m_j}$. Prema tome, x_0 je rješenje sustava kongruencija.

Ako su x, y dva rješenja sustava kongruencija, onda je $x \equiv y \pmod{m_j}$ za $j = 1, 2, \ldots, r$. Budući su m_j u parovima relativno prosti, dobivamo da je $x \equiv y \pmod{m}$. □

Prema ovom važnom teoremu, ukoliko sustav kongruencija ima rješenje, tada ih ima beskonačno mnogo, a sva rješenja su međusobno kongruentna modulo produkt zadanih djelitelja.

Primjer 1. Riješimo početni problem koji možemo zapisati kao sustav kongruencija $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$.
Koristeći oznake iz prethodnog teorema, dobivamo: $a_1 = 2$, $m_1 = 3$, $a_2 = 3$, $m_2 = 5$, $a_3 = 2$, $m_3 = 7$ te $m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$. Nadalje je $n_1 = \frac{m}{m_1} = \frac{105}{3} = 35$, $n_2 = \frac{m}{m_2} = \frac{105}{5} = 21$ i $n_3 = \frac{m}{m_3} = \frac{105}{7} = 15$.

Kako je očito $33x \equiv 0 \pmod 3$, $20x \equiv 0 \pmod 5$ i $14x \equiv 0 \pmod 7$, slijedi

$$\begin{aligned} & n_1 x \equiv a_1 \pmod{m_1} \\ & 35x \equiv 2 \pmod 3 \\ & 2x \equiv 2 \pmod 3 \\ \Rightarrow \quad & x_1 = 1, \end{aligned}$$

$$\begin{aligned} & n_2 x \equiv a_2 \pmod{m_2} \\ & 21x \equiv 3 \pmod 5 \\ & x \equiv 3 \pmod 5 \\ \Rightarrow \quad & x_2 = 3, \end{aligned}$$

$$\begin{aligned} & n_3 x \equiv a_3 \pmod{m_3} \\ & 15x \equiv 2 \pmod 7 \\ & x \equiv 2 \pmod 7 \\ \Rightarrow \quad & x_3 = 2. \end{aligned}$$

Rješenje problema je dano s

$$\begin{aligned} x &= 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 \pmod{105} \\ &= 35 + 63 + 30 \pmod{105} \\ &= 128 \pmod{105} \\ &= 23 \pmod{105}. \end{aligned}$$

Prema tome, neki od cijelih brojeva koji zadovoljavaju problem koji je postavio Sun-Tzu su $23, 128, 578, -82, -187$.

Prema predaji, Kinezi su se često u primjenama koristili opisanim postupkom. Neki navodi govore kako je opisani postupak prvenstveno korišten u vojne svrhe prilikom prebrojavanja preživjelih vojnika nakon bitke. Naime, umjesto da se nepotrebno troši vrijeme na dugačka prebrojavanja, preživjeli vojnici bi se jednostavno postrojili u redove od po $3, 4, 5, 7, 11$ i eventualno 13 vojnika (ukoliko bi se radilo o većem broju preživjelih vojnika), a potom bi se pomoću broja vojnika preostalih u zadnjem redu dobivao sustav kongruencija. Rješavanje tako dobivenog sustava bi rezultiralo kongruencijom iz koje bi se direktno dobio točan broj preživjelih vojnika. Naravno, broj vojnika u pojedinom redu se mogao i mijenjati, jedino se

uvijek moralo paziti da brojevi budu međusobno relativno prosti te njihov produkt dovoljno velik kako bi se iz završne kongruencije mogao očitati točan broj preživjelih vojnika.

Više o povijesnom razvoju te pozadinama spomenutog i sličnih problema se može vidjeti u [2] i [3].

No, s vremenom se pojavljuju raznolika poopćenja Kineskog teorema o ostatcima i na brojne druge skupove, izuzev skupa cijelih brojeva. Pokazalo se da neka od tih poopćenja posjeduju važne dalekosežne primjene kako na proučavanje svojstava određenih skupova, tako i u praksi. Cilj ovog rada je upravo prikazati neke od tih primjena.

2 Kineski teorem o ostatcima za polinome

2.1 Kongruencije modulo polinom

Kako se moglo vidjeti iz uvodnog poglavlja, u samoj jezgri Kineskog teorema o ostatcima se nalazi teorija kongruencija. Jedino svojstvo potrebno da bi se ova teorija zasnovala je svojstvo djeljivosti, te se ona može proširiti na svaki skup u kome se djeljivost može promatrati.

Nas će posebno interesirati teorija kongruencija za polinome s koeficijentima iz nekog, unaprijed zadanog prstena. Nadalje ćemo promatrati polinome u jednoj varijabli (koja će uvijek biti označena s x) s realnim, kompleksnim, racionalnim ili cjelobrojnim koeficijentima. Redom, skup polinoma u jednoj varijabli s realnim koeficijentima će biti označen s $\mathbb{R}[x]$, s kompleksnim koeficijentima $\mathbb{C}[x]$, s racionalnim koeficijentima $\mathbb{Q}[x]$, a s cjelobrojnim $\mathbb{Z}[x]$. U diplomskom radu [1] je čitava situacija promatrana na nešto općenitiji način.

Neka je $p(x)$ ne-nul polinom s koeficijentima iz prstena K, tj. $p(x) \in K[x]$, gdje je s K označen prsten realnih, kompleksnih, racionalnih ili cijelih brojeva. Kažemo da je polinom $f(x)$ iz $K[x]$ kongruentan polinomu $g(x)$ iz $K[x]$ modulo $p(x)$ i pišemo $f(x) \equiv g(x) \pmod{p(x)}$, ako $p(x)$ dijeli $f(x) - g(x)$, ili ekvivalentno, ako je $f(x) = g(x) + m(x)p(x)$ za neki polinom $m(x)$ iz $K[x]$.

Na primjer, polinom x^5 je kongruentan konstantnom polinomu 1 modulo $x - 1$, tj. $x^5 \equiv 1 \pmod{x-1}$, jer $x - 1$ dijeli razliku $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$.

Time su definirane kongruencije modulo polinom. Njihova svojstva su identična svojstvima kongruencija modulo prirodan broj, a slijede direktno iz definicije. Navedimo neka od najvažnijih:

- Ako je $f(x) \equiv g(x) \pmod{p(x)}$, tada je $h(x)f(x) \equiv h(x)g(x) \pmod{p(x)}$ za svaki $h(x) \in K[x]$;
- Ako je $f_1(x) \equiv g_1(x) \pmod{p(x)}$ i $f_2(x) \equiv g_2(x) \pmod{p(x)}$, tada je $f_1(x) + f_2(x) \equiv g_1(x) + g_2(x) \pmod{p(x)}$ i $f_1(x) \cdot f_2(x) \equiv g_1(x) \cdot g_2(x) \pmod{p(x)}$;
- Ako je $f(x) \equiv g(x) \pmod{p(x)}$ i $g(x) \equiv h(x) \pmod{p(x)}$, tada je i $f(x) \equiv h(x) \pmod{p(x)}$.

Ilustrirajmo idućim primjerom kako se mogu iskoristiti neka od navedenih svojstava:

Primjer 2. Za polinom $f(x)$ iz $K[x]$, pokažimo da je $f(x) \equiv f(1) \pmod{x-1}$.

Možemo primijetiti da vrijedi kongruencija $x - 1 \equiv 0 \pmod{x-1}$. Zbrajanjem obje strane kongruencije s 1, tj. s konstantnim polinomom, kao u drugom od navedenih svojstava, dobivamo $x \equiv 1 \pmod{x-1}$.

Podignemo li dobivenu kongruenciju na r-tu potenciju, gdje je r proizvoljan prirodan broj, uzastopnom primjenom drugog od navedenih svojstava slijedi $x^r \equiv 1 \pmod{x-1}$. Prema tome, zamijenimo li u polinomu $f(x)$ izraz x^r s 1, dobivamo polinom koji je kongruentan s $f(x)$ modulo $x - 1$. Zapišemo li polinom $f(x)$ u obliku $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, tada je $f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \pmod{x-1}$, tj. $f(x) \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{x-1}$ i desna strana posljednje kongruencije je jednaka $f(1)$.

Pokažimo i jedno vrlo korisno svojstvo kongruencija modulo polinom.

Primjer 3. Neka je $f(x) \in K[x]$ te $a, b \in K$. Tada je $f(x)$ kongruentno b modulo $x - a$ ako i samo ako je $f(a) = b$.

Najprije, ako je $f(x) \equiv b \pmod{x-a}$, tada postoji polinom $g(x)$ takav da je $f(x) - b = (x-a)g(x)$ te uvrštavanjem $x = a$ dobivamo $f(a) - b = 0$, tj. $f(a) = b$.

S druge strane, ako je $f(a) = b$, tada je a nultočka polinoma $f(x) - b$ te je taj polinom djeljiv s polinomom $x - a$, odakle slijedi tražena tvrdnja.

Kako bi došli u situaciju iskazati rezultat analogan Kineskom teoremu o ostatcima u slučaju polinoma, moramo najprije definirati kada ćemo polinome smatrati relativno prostima.

Neka su $f(x)$ i $g(x)$ polinomi iz $K[x]$, gdje je K polje racionalnih, realnih ili kompleksnih brojeva. Za polinome $f(x)$ i $g(x)$ ćemo reći da su relativno prosti ukoliko ih ne dijeli niti jedan polinom stupnja barem 1. Na primjer,

polinomi $x+1$ i $x-1$ su relativno prosti jer su jedini njihovi zajednički djelitelji konstantni ne-nul polinomi. *Najveći zajednički djelitelj* polinoma $f(x)$ i $g(x)$ je svaki polinom $p(x)$ iz $K[x]$ koji dijeli i $f(x)$ i $g(x)$ i ima svojstvo da svaki polinom $q(x)$ iz $K[x]$ koji dijeli i $f(x)$ i $g(x)$ ima stupanj manji ili jednak stupnju polinoma $p(x)$. Dakle, $p(x)$ je zajednički djelitelj polinoma $f(x)$ i $g(x)$ najvećeg stupnja. Primijetimo kako najveći zajednički djelitelj ne mora biti jedinstven, jer npr. polinomi x^2-1 i $5x^2+5x+5$ imaju mnoge najveće zajedničke djelitelje, od kojih su neki $x+1$, $2x+2$, $\frac{x}{17}+\frac{1}{17}$. No, među najvećim zajedničkim djeliteljima postoji samo jedan koji je normiran, tj. koji je polinom vodećeg koeficijenta jednakog 1. Jedinstveni normirani najveći zajednički djelitelj polinoma $f(x)$ i $g(x)$ ćemo nadalje označavati s $(f(x),g(x))$. Primijetimo da se svi najveći zajednički djelitelji polinoma $f(x)$ i $g(x)$ dobivaju iz $(f(x),g(x))$ množenjem elementom iz K različitim od nule.

Postupak određivanja najvećeg zajedničkog djelitelja dvaju polinoma je sličan postupku za cijele brojeve. Kako bi ga opisali, najprije trebamo

Teorem 2.1. (Teorem o dijeljenju s ostatkom za polinome) Neka su $f(x)$ i $g(x)$ polinomi iz $K[x]$, gdje je s K označeno polje racionalnih, realnih ili kompleksnih brojeva, te neka je $f(x)$ ne-nul polinom. Tada postoje polinomi $q(x)$ i $r(x)$, gdje je stupanj od $r(x)$ strogo manji od stupnja od $f(x)$, takvi da je $g(x)=f(x)q(x)+r(x)$. Ako je također $g(x)=f(x)q_1(x)+r_1(x)$, tada vrijedi $q(x)=q_1(x)$ i $r(x)=r_1(x)$, tj. takvi polinomi $q(x)$ i $r(x)$ su jedinstveni.

Dokaz. Fiksirajmo polinom $f(x)$ te dokažimo da za svaki polinom $g(x)$ postoje traženi polinomi $q(x)$ i $r(x)$ indukcijom po stupnju polinoma $g(x)$.

Ukoliko je stupanj polinoma $g(x)$ manji od stupnja polinoma $f(x)$, stavimo li $q(x)=0$ i $r(x)=g(x)$, očito vrijedi $g(x)=f(x)q(x)+r(x)$.

Pretpostavimo sada da je stupanj polinoma $g(x)$ veći ili jednak stupnju polinoma $f(x)$. Zapišimo polinom $f(x)$ u obliku

$$f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_0$$

gdje je $a_d\neq 0$ te polinom $g(x)$ u obliku

$$g(x)=b_{d+s}x^{d+s}+d_{d+s-1}x^{d+s-1}+\cdots+b_0$$

gdje je $b_{d+s}\neq 0$. Primijetimo da je $s\geq 0$. Definirajmo polinom $g_1(x)$ s $g_1(x)=g(x)-\frac{b_{d+s}}{a_d}x^sf(x)$. Tada je stupanj polinoma $g_1(x)$ strogo manji od stupnja polinoma $g(x)$ te prema induktivnoj pretpostavci postoje polinomi

$q_1(x)$ i $r(x)$ takvi da je $g_1(x) = f(x)q_1(x) + r(x)$ te je stupanj od $r(x)$ strogo manji od stupnja od $f(x)$. No tada je

$$\begin{aligned} g(x) &= g_1(x) + \frac{b_{d+s}}{a_d}x^s f(x) \\ &= f(x)q_1(x) + r(x) + \frac{b_{d+s}}{a_d}x^s f(x) \\ &= f(x)(q_1(x) + r(x) + \frac{b_{d+s}}{a_d}x^s) + r(x), \end{aligned}$$

čime dobivamo tražene polinome. Prema principu matematičke indukcije, dokazali smo postojanje polinoma $q(x)$ i $r(x)$.

Kako bi dokazali jedinstvenost, pretpostavimo da je $g(x) = f(x)q(x) + r(x) = f(x)q_2(x) + r_2(x)$, gdje je i stupanj polinoma $r(x)$ i stupanj polinoma $r_2(x)$ strogo manji od stupnja polinoma $f(x)$. No, tada je

$$f(x)(q(x) - q_2(x)) = r_2(x) - r(x).$$

Polinom na lijevoj strani prethodne jednakosti je ili jednak 0 ili je stupnja većeg ili jednakog od stupnja polinoma $f(x)$, dok je stupanj polinoma s desne strane prethodne jednakosti strogo manji od stupnja polinoma $f(x)$. Prema tome, obje strane su jednake 0, tj. $q(x) = q_2(x)$ i $r(x) = r_2(x)$. □

Primijetimo kako prethodni teorem ne vrijedi u slučaju da je $K = \mathbb{Z}$, tj. u slučaju da promatramo samo polinome s cjelobrojnim koeficijentima. Primjerice, pokušamo li podijeliti polinom x^2 s $2x$ tražeći da i kvocijent i ostatak budu polinomi s cjelobrojnim koeficijentima, dobivamo $x^2 = 0 \cdot 2x + x^2$.

Kako sada raspolažemo s Teoremom o dijeljenju s ostatkom za polinome, u mogućnosti smo opisati postupak određivanja najvećeg zajedničkog djelitelja dvaju polinoma. Postupak koji ćemo opisati se naziva Euklidov algoritam za polinome, a datira još od Simona Stevina, iz 1585.

Neka su $f(x)$ i $g(x)$ polinomi iz $K[x]$ te neka je $f(x) \neq 0$. Neka je uzastopnom primjenom prethodnog teorema dobiven sljedeći niz jednakosti:

$$\begin{aligned} g(x) &= f(x)q_1(x) + r_1(x) \\ f(x) &= r_1(x)q_2(x) + r_2(x) \\ r_1(x) &= r_2(x)q_3(x) + r_3(x) \\ &\vdots \\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x) \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x) + 0 \end{aligned}$$

gdje je stupanj polinoma $r_1(x)$ manji od stupnja polinoma $f(x)$, stupanj polinoma $r_2(x)$ manji od stupnja polinoma $r_1(x)$ itd. Tada vrijedi idući

rezultat, koji se može pokazati na identičan način kao i klasični Euklidov algoritam (koji je detaljno obrađen u [6]):

Teorem 2.2. Posljednji ne-nul ostatak $r_n(x)$ je najveći zajednički djelitelj polinoma $f(x)$ i $g(x)$.

Primjer 4. Euklidovim algoritmom za polinome odredimo $(x^2-1, 5x^2+10x+5)$. Redom dobivamo

$$5x^2+10x+5 = (x^2-1)\cdot 5 + 10x + 10$$
$$x^2-1 = (10x+10)\cdot(\frac{1}{10}x - \frac{1}{10}) + 0.$$

Prema tome, jedan najveći zajednički djelitelj je $10x+10$. Tražimo li normirani polinom, množenjem s recipročnom vrijednosti vodećeg koeficijenta dobivamo $(x^2-1, 5x^2+10x+5) = x+1$.

Kombiniranjem jednakosti dobivenih u provedbi Euklidova algoritma za polinome (uvrštavanjem dobivenih polinoma iz krajnjih jednakosti prema početnima, analogno postupku kod klasičnog Euklidova algoritma), dobivamo idući rezultat.

Lema 2.1. (Bezoutova lema) *Za polinome $f(x)$ i $g(x)$ iz $K[x]$ postoje polinomi $s(x)$ i $t(x)$ iz $K[x]$ takvi da je $(f(x), g(x)) = s(x)f(x) + t(x)g(x)$.*

U Primjeru 4 se tvrdnja Bezoutove leme može jednostavno zapisati u obliku $x+1 = \frac{1}{10}(5x^2+10x+5) - \frac{1}{2}(x^2-1)$.

Pogledajmo sada kongruencije u prstenu polinoma $K[x]$.

Općenito, kongruencija $f(x)z(x) \equiv h(x) \pmod{m(x)}$ ima rješenje $z(x)$ u prstenu $K[x]$ ako i samo ako $(f(x), m(x))$ dijeli $h(x)$. Traženje rješenja kongruencije $f(x)z(x) \equiv h(x) \pmod{m(x)}$ je isto što i rješavanje jednadžbe $f(x)z(x) + m(x)y(x) = h(x)$. Ako postoji rješenje, tada $(f(x), m(x))$ mora dijeliti $h(x)$. S druge strane, pomoću Bezoutovog identiteta možemo pronaći polinome $r(x)$ i $s(x)$ takve da je $f(x)r(x) + m(x)s(x) = (f(x), m(x))$. Ako $(f(x), m(x))$ dijeli $h(x)$, tada postoji polinom $c(x)$ takav da je $h(x) = (f(x), m(x))\cdot c(x)$ te uvrštavanjem $y(x) = s(x)c(x), z(x) = r(x)c(x)$ dobivamo rješenje jednadžbe.

Specijalno, ukoliko su polinomi $f(x)$ i $m(x)$ relativno prosti možemo riješiti kongruenciju $f(x)z(x) \equiv q \pmod{m(x)}$.

2.2 Kineski teorem o ostatcima za polinome

U ovom potpoglavlju ćemo iskazati i dokazati Kineski teorem o ostatcima za polinome te iznijeti važnu posljedicu tog teorema. Ponovno će s K biti označeno polje racionalnih, realnih ili kompleksnih brojeva.

Teorem 2.3. (Kineski teorem o ostatcima za polinome)
Neka su $a_1(x), \ldots, a_r(x)$ proizvoljni polinomi iz $K[x]$, te neka su $m_1(x), \ldots, m_r(x)$ u parovima relativno prosti polinomi iz $K[x]$. Tada postoji polinom $f(x)$ iz $K[x]$ takav da je

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

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

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

Dokaz. Budući je $m_i(x)$ relativno prost s $m_j(x)$ za svaki $j \neq i$, $m_i(x)$ je relativno prost i s produktom $l_i(x) = m_1(x)m_2(x) \cdots m_{i-1}(x)m_{i+1}(x) \cdots m_r$. Zbog toga pomoću Bezoutove leme možemo pronaći polinome $k_i(x)$ i $h_i(x)$ za koje vrijedi $1 = h_i(x)m_i(x) + k_i(x)l_i(x)$.

Tada polinom $k_i(x)l_i(x)$ zadovoljava sljedeće kongruencije:

$$\begin{aligned} k_i(x)l_i(x) &\equiv 1 \pmod{m_i(x)}, \\ k_i(x)l_i(x) &\equiv 0 \pmod{m_j(x)}, \quad za \quad j \neq i. \end{aligned}$$

Stavimo li

$$f_0(x) = a_1(x)k_1(x)l_1(x) + \cdots + a_r(x)k_r(x)l_r(x),$$

iz prethodnih kongruencija se direktno vidi da je $f_0(x)$ traženo rješenje sustava.

S druge strane, za bilo koje rješenje $f(x)$ vrijedi

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

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

Iduća posljedica Kineskog teorema o ostatcima za polinome će biti od posebne važnosti u narednom poglavlju.

Korolar 2.1. Neka su $r_1, \ldots, r_n$ različiti elementi iz K te $s_1, \ldots, s_n$ proizvoljni elementi iz K. Tada postoji jedinstveni polinom $f(x) \in K[x]$ stupnja manjeg od n za koji vrijedi $f(r_i) = s_i$, za $i = 1, 2, \ldots, n$.

Dokaz. Primijetimo da su za različite r_i i r_j polinomi $x - r_i$ i $x - r_j$ relativno prosti. Prema prethodnom teoremu postoji jedinstveni polinom $f(x)$ stupnja manjeg od stupnja polinoma $(x - r_1)(x - r_2) \cdots (x - r_n)$ (tj. stupnja manjeg od n) za koji vrijedi $f(x) \equiv s_i \pmod{x - r_i}$, gdje je $i = 1, 2, \ldots, n$.

No, prema Primjeru 3, posljednja kongruencija je ekvivalentna s $f(r_i) = s_i$ iz čega proizlazi tvrdnja korolara. □

3 Primjene Kineskog teorema o ostatcima za polinome

3.1 Metoda Lagrangeove interpolacije

Problem faktorizacije polinoma je sličan problemu faktorizacije cijelog broja, tj. prikazu cijelog broja u obliku produkta prostih faktora. Polazna ideja je pokušati prikazati dani polinom u obliku produkta polinoma manjeg stupnja koji se ne mogu dalje rastavljati.

Općenito, za polinom $p(x) \in K[x]$ stupnja n, gdje je K polje, ćemo reći da je ireducibilan u prstenu polinoma $K[x]$ ukoliko ne postoje polinomi $q(x), r(x) \in K[x]$ stupnja barem jedan takvi da je $p(x) = q(x)r(x)$. Ako takvi polinomi postoje, primijetimo kako su oni stupnja strogo manjeg od n. Ukoliko polinom nije ireducibilan, kažemo da je reducibilan.

Na primjer, polinom $x^2 - 1 \in \mathbb{Q}[x]$ je reducibilan, jer se može prikazati u obliku $(x - 1)(x + 1)$ te ovaj produkt tada nazivamo faktorizacija polinoma $x^2 - 1$. S druge strane, polinom $x^2 + 1$ je ireducibilan u prstenu $\mathbb{Q}[x]$, kao i u prstenu $\mathbb{R}[x]$. No, ovaj polinom je reducibilan u prstenu $\mathbb{C}[x]$, jer je $x^2 + 1 = (x - i)(x + i)$ u $\mathbb{C}[x]$. No, kako je polje kompleksnih brojeva algebarski zatvoreno, tj. svaki nekonstantan polinom s kompleksnim koeficijentima ima kompleksnu nultočku, izbjegavamo korištenje kompleksnih brojeva u faktorizaciji jer ju čine trivijalnom.

U ovom potpoglavlju ćemo proučavati faktorizaciju isključivo polinoma s cjelobrojnim koeficijentima.

Joseph Louis Lagrange (1736.-1813.) francuski matematičar

Kod postupka faktorizacije polinoma s cjelobrojnim koeficijentima, možemo pretpostaviti da faktori također imaju cjelobrojne koeficijente (ovo je posljedica općenitijeg rezultata poznatog pod nazivom *Gaussova lema*, u detalje kojeg na ovom mjestu nećemo ulaziti, a više o toj temi se može naći u [4], Poglavlje 18). Metoda Lagrangeove interpolacije je postupak faktorizacije bilo kojeg polinoma iz $\mathbb{Z}[x]$. Otkriće metode 1883. godine pripisuje se Kroneckeru, iako ju je zapravo već 1793. otkrio Schubert. Metoda se temelji na Kineskom teoremu o ostatcima.

Neka je $p(x)$ iz $\mathbb{Z}[x]$ polinom koji želimo faktorizirati.

Primijetimo da ako je stupanj polinoma $p(x)$ jednak n i ako $p(x)$ nije ireducibilan, tada je stupanj jednog od njegovih faktora manji ili jednak $\frac{n}{2}$. Neka je $d = \frac{n}{2}$ ako je n paran i $d = \frac{n-1}{2}$ ako je n neparan.

Neka su $n_0, \ldots, n_d$ međusobno različiti cijeli brojevi i $p(n_0) = r_0, \ldots, p(n_d) = r_d$. Budući je $p(x)$ iz $\mathbb{Z}[x]$, $r_0, \ldots, r_d$ su cijeli brojevi. Na svaku uređenu d–torku $s = (s_0, \ldots, s_d)$ cjelobrojnih djelitelja od $(r_0, \ldots, r_d)$ ($s_i | r_i$ za svaki $i = 0, \ldots, d$), možemo primijeniti korolar Kineskog teorema o ostatcima kako bismo dobili jedinstveni polinom $a_s(x)$ iz $\mathbb{Q}[x]$ stupnja manjeg ili jednakog d takav da je $a_s(n_i) = s_i$ za svaki i. U daljnjem ćemo, jednostavnosti notacije radi, uređenu d–torku cjelobrojnih djelitelja s kratko nazivati vektorom. Budući svaki r_i ima konačan broj pozitivnih ili negativnih djelitelja s_i, postoji konačan broj mogućih vektora s i konačan broj polinoma $a_s(x)$ za svaki vektor s.

Prema tome, djelitelj polinoma $p(x)$ iz $\mathbb{Z}[x]$ stupnja manjeg ili jednakog d je a_s za neki s. Neka je $a(x)$ iz $\mathbb{Z}[x]$ stupnja manjeg ili jednakog d i $a(x)b(x) = p(x)$ za neki $b(x)$ iz $\mathbb{Z}[x]$. Tada za svaki n_i vrijedi $a(n_i)b(n_i) = p(n_i)$ u $\mathbb{Z}$. Stoga, $a(n_i)$ dijeli $p(n_i) = r_i$. Odatle slijedi da je vektor $s = (a(n_0), \ldots, a(n_d))$ vektor djelitelja od $(r_0, \ldots, r_d)$. Iz Kineskog teorema o ostatcima slijedi da postoji jedinstveni polinom $a_s(x)$ stupnja manjeg ili jednakog d takav da $a_s(n_0) = a(n_0), \ldots, a_s(n_d) = a(n_d)$.

Budući da su polinomi $a(x)$ i $a_s(x)$ oba stupnja manjeg ili jednakog d te im se vrijednosti podudaraju u $d+1$ različitih elemenata, moraju biti jednaki (jer je razlika polinoma $a(x)$ i $a_s(x)$ polinom stupnja manjeg od $d+1$ koji ima $d+1$ nultočku te stoga mora biti nul–polinom). Možemo zaključiti da se svaki djelitelj $a(x)$ polinoma $p(x)$ stupnja manjeg ili jednakog d mora nalaziti među polinomima $a_s(x)$ dobivenim pomoću vektora djelitelja s.

Kako bismo ispitali je li polinom $p(x)$ ireducibilan ili ne, moramo podijeliti $p(x)$ svakim polinomom $a_s(x)$ kako bi vidjeli je li $a_s(x)$ možda djelitelj. Ako neki nekonstantan polinom $a_s(x)$ stupnja manjeg od n dijeli $p(x)$, tada se polinom $p(x)$ može faktorizirati. U suprotnom, $p(x)$ mora biti ireducibilan.

Iz konačnosti broja potencijalnih djelitelja $a_s(x)$ slijedi:

Teorem 3.1. Potpunu faktorizaciju bilo kojeg polinoma iz $\mathbb{Z}[x]$ je moguće ostvariti u konačno mnogo koraka.

Polinom $a_s(x)$ nazivamo **Lagrangeov interpolator**. Moguće ga je konstruirati na sljedeći način:

Neka su $n_0, \ldots, n_d$, $s_0, \ldots, s_d$ kao gore i neka je $g(x) = (x - n_0) \cdots (x - n_d)$, te neka je $g'(x)$ derivacija od $g(x)$. Nakon skraćivanja $\frac{g(x)}{(x-n_i)}$ je polinom

stupnja d. Stoga, $\frac{g(x)}{(x-n_i)g'(n_i)} = h_i(x)$ je polinom stupnja d takav da je

$$h_i(n_i) = 1 \quad i \quad h_i(n_0) = \cdots = h_i(n_{i-1}) = h_i(n_{i+1}) = \cdots = h_i(n_s) = 0.$$

Prema tome, traženi polinom je dan s

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

Primjer 5. Neka je $p(x) = x^4 + x + 1$. Ako se $p(x)$ može faktorizirati, tada mora sadržavati faktor stupnja manjeg ili jednakog 2. Znamo da je $p(-1) = 1$, $p(0) = 1$ i $p(1) = 3$. Dakle, $g(x) = x^3 - x$, $g'(x) = 3x^2 - 1$. Za svaki $s = (s_{-1}, s_0, s_1)$ koji dijeli $(1, 1, 3)$ odgovarajući Lagrangeov interpolator $a_s(x)$ je

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

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

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

Tablica 5.1 *Vektori $s = (s_{-1}, s_0, s_1)$ i odgovarajući polinomi $a_s(x)$*

Ako se polinom $x^4 + x + 1$ može faktorizirati, možemo pretpostaviti da su svi faktori ireducibilni i imaju cjelobrojne koeficijente. Budući je polinom $x^4 + x + 1$ normiran, vodeći koeficijenti njegovih faktora moraju biti jednaki ± 1. Osam polinoma $a_s(x)$ nemaju vodeće koeficijente jednake ± 1, pa ne mogu biti faktori. Dva polinoma $a_s(x)$ nisu zanimljiva jer su stupnja 0. Dakle, samo šest polinoma $a_s(x)$ su mogući 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 se polinomi s desne strane mogu dobiti množenjem polinoma s lijeve strane s -1, dovoljno je provjeriti samo tri polinoma s lijeve strane. Tri brza dijeljenja pokazuju da niti jedan polinom nije faktor.

Možemo primijetiti da broj mogućih faktora $a_s(x)$ polinoma $p(x)$ ovisi o d (koji je manji ili jednak od $\frac{n}{2}$, gdje je n stupanj polinoma $p(x)$). No, često je mnogo značajnija činjenica da broj mogućih faktora također ovisi i o broju djelitelja od $p(n_i)$. Broj mogućih faktora u primjeru je mali zbog činjenice da je $p(1) = p(0) = 1$, koji ima samo dva faktora u $\mathbb{Z}$.

Općenito, broj faktora $a_s(x)$ može biti izrazito velik. Posljednjih nekoliko godina razvijena je puno učinkovitija metoda faktorizacije koja se temelji na faktorizaciji modulo M za odgovarajući prirodan broj M.

3.2 Brzo množenje polinoma

Ubrzani razvoj računala nakon 40-tih godina prošlog stoljeća je nanovo otvorio brojna pitanja starije matematike, čije rješavanje je do tada bilo gotovo neizvedivo. Jedno od tih pitanja, na koje ćemo sada pokušati odgovoriti je: Kako možemo učinkovito pomnožiti dva polinoma?

Množenje je jedna od osnovnih algebarskih operacija s polinomima. Prisjetimo se ukratko tog postupka.

Pretpostavimo da su dana dva polinoma stupnja d:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d, g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d.$$

Njihov produkt

$$f(x)g(x) = (a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d) \cdot (b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d)$$

dobivamo tako da svaki $a_i x^i$ pomnožimo sa svakim $b_j x^j$ i grupiramo sve koeficijente uz odgovarajuću potenciju od x-a:

$$f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{2d} x^{2d},$$

gdje su

$$\begin{aligned}
c_0 &= a_0 b_0, \\
c_1 &= a_0 b_1 + a_1 b_0, \\
c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\
&\vdots \\
c_d &= a_0 b_d + a_1 b_{d-1} + \cdots + a_{d-1} b_1 + a_d b_0, \\
c_{d+1} &= a_1 b_d + a_2 b_{d-1} + \cdots + a_{d-1} b_2 + a_d b_1, \\
&\vdots \\
c_{2d} &= a_d b_d.
\end{aligned}$$

Kako bismo ispitali učinkovitost ove metode, moramo odrediti broj potrebnih množenja. Budući da su polinomi $f(x)$ i $g(x)$ oba stupnja d, oba imaju $d+1$ koeficijent, i svaki koeficijent od $f(x)$ je pomnožen sa svakim koeficijentom od $g(x)$. Stoga, standardni postupak množenja dva polinoma stupnja d zahtijeva $(d+1)^2$ operacija množenja.

Postoji li učinkovitiji način množenja dva polinoma? Preciznije, postoji li postupak množenja dva polinoma stupnja d koji zahtijeva manje od $(d+1)^2$ množenja?

Iako donekle iznenađujući, odgovor je da postoji.

Opišimo ukratko strategiju učinkovitijeg postupka množenja dvaju polinoma $f(x)$ i $g(x)$ stupnja d s kompleksnim koeficijentima:

I. Evaluacija. Odabrati $2d+1$ točaka $a_1, a_2, \ldots, a_{2d+1}$ te evaluirati polinome $f(x)$ i $g(x)$ u svakoj od odabranih točaka, tj. odrediti $f(a_1), \ldots, f(a_{2d+1})$ i $g(a_1), \ldots, g(a_{2d+1})$.

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

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

Ovaj postupak izgleda prilično složeno. No, on ima jednu značajnu prednost, a ta je da u II. koraku broj množenja iznosi $2d+1$ što je puno manje od $(d+1)^2$ množenja u standardnom postupku.

Prema tome, ukoliko je učinkovitost I. i III. koraka velika, izgledno je da opisani postupak bude mnogo učinkovitiji od standardnog.

Prije nego komentiramo učinkovitost I. i III. koraka, primijetimo ključni detalj - polinom $h(x)$ dobiven u III. koraku je doista jednak $f(x)g(x)$, prema Korolaru 2.1.

Primijenimo li taj korolar na III. korak postupka množenja dva polinoma $f(x)$ i $g(x)$ stupnja d, možemo pronaći polinom $h(x)$ stupnja manjeg ili

jednakog $2d$ takav da je $h(a_i) = f(a_i)g(a_i)$ za svaki $i = 1, 2, \ldots, 2d+1$. Budući je $f(x)g(x)$ također polinom stupnja manjeg ili jednakog $2d$ s istim vrijednostima u točkama $a_1, a_2, \ldots, a_{2d+1}$ kao i polinom $h(x)$, polinomi $h(x)$ i $f(x)g(x)$ moraju biti jednaki. Dakle, postupak za pronalaženje polinoma $f(x)g(x)$ će zaista dati traženi rezultat.

Primjer 6. Neka su $f(x) = x + 1$ i $g(x) = x - 2$. Želimo pronaći $f(x)g(x)$ danim postupkom.
Neka je $a_1 = 0$, $a_2 = 3$, $a_3 = -1$. I. i II. korak su brzi:

$$\begin{aligned} f(a_1) = 1, \quad g(a_1) = -2 \quad &\Rightarrow \quad f(a_1)g(a_1) = -2; \\ f(a_2) = 4, \quad g(a_2) = 1 \quad &\Rightarrow \quad f(a_2)g(a_2) = 4; \\ f(a_3) = 0, \quad g(a_3) = -3 \quad &\Rightarrow \quad f(a_3)g(a_3) = 0. \end{aligned}$$

U III. koraku moramo interpolirati polinom $h(x)$ stupnja strogo manjeg od 3 s $h(0) = -2, h(3) = 4, h(-1) = 0$.
To možemo učiniti na jedan od sljedeća dva načina.
Prvi način je da korištenjem Lagrangeovih interpolatora pronađemo

$$\begin{aligned} h_0(x) &= \frac{(x-3)(x+1)}{-3}, \qquad h_0(0) = 1, h_0(3) = h_0(-1) = 0; \\ h_3(x) &= \frac{x(x+1)}{12}, \qquad h_3(0) = h_3(-1) = 0, h_3(3) = 1; \\ h_{-1}(x) &= \frac{x(x-3)}{4}, \qquad h_{-1}(0) = h_{-1}(3) = 0, h_{-1}(-1) = 1. \end{aligned}$$

Tada $h(x) = -2h_0(x) + 4h_3(x) + 0h_{-1}(x) = x^2 - x - 2$ zadovoljava $h(0) = -2, h(3) = 4, h(-1) = 0$, pa mora biti jednak $f(x)g(x)$.
Drugi način da odredimo polinom $h(x)$ stupnja manjeg ili jednakog 2 s $h(0) = -2, h(3) = 4, h(-1) = 0$ je da zapišemo $h(x)$ kao $h(x) = rx^2 + sx + t$ i evaluiramo $h(x)$ u $0, 3, -1$ te tako dobivamo tri jednadžbe s nepoznatim koeficijentima:

$$\begin{aligned} -2 = h(0) &= t, \\ 4 = h(3) &= 9r + 3s + t, \\ 0 = h(-1) &= r - s + t. \end{aligned}$$

Rješavanjem ovih jednadžbi dobivamo $t = -2$, $r = 1$, $s = -1$ i $h(x) = x^2 - x - 2$.

Očito je ova interpolacijska metoda puno sporija od jednostavnog množenja $f(x)g(x) = (x+1)(x-2)$.

Ključna činjenica za povećanje učinkovitosti ovog postupka leži u odabiru što povoljnijeg skupa točaka $a_1, a_2, \ldots, a_{2d+1}$. U nastavku ćemo se posvetiti opisu povoljnijeg odabira.

Definicija 3.1. Korijenom jedinice nazivamo kompleksan broj ω takav da je $\omega^n = 1$ za neki $n > 0$.

Primjer 7. 1 i -1 su jedini realni brojevi koji su korijeni jedinice.

Prema Osnovnom teoremu algebre, polinom $x^n - 1$ ima n korijena u skupu $\mathbb{C}$. Ako je ω korijen polinoma $x^n - 1$, tada je ω korijen jedinice.

Za korijen jedinice ω, definiramo red od ω kao najmanji eksponent $l > 0$ takav da je $\omega^l = 1$. Ako je l red od ω, tada se ω naziva **primitivni l-ti korijen jedinice**.

Primjer 8. -1 je primitivni drugi korijen jedinice.

$\omega = \cos(\frac{2\pi}{m}) + i\sin(\frac{2\pi}{m})$ je primitivni m-ti korijen jedinice.

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

Teorem 3.2. Za bilo koji n postoji primitivni n-ti korijen jedinice.

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

Vratimo se problemu interpolacije. Neka je r prirodan broj za koji vrijedi $2^{r-1} < 2d + 1 \leq 2^r$ te neka je ω primitivni 2^r-ti korijen jedinice. U postupku pronalaženja umnoška $f(x)g(x)$, gdje su $f(x)$ i $g(x)$ oba stupnja d, moramo evaluirati $f(x)$ i $g(x)$ u potencijama od ω. To je ključna činjenica koja ovu metodu čini učinkovitom.

Teorem 3.3. Neka je ω primitivni 2^r-ti korijen jedinice i $f(x)$ polinom stupnja $d < 2^{r-1}$. Tada evaluacija $f(x)$ u $1, \omega, \omega^2, \ldots, \omega^{2^r-1}$ zahtijeva najviše $2^r(r-1)$ množenja.

Dokaz. Pretpostavimo da je stupanj polinoma $f(x)$ jednak $d = 1$. Tada je $r = 2$, $2^r = 4$ i $2^{r-1} = 2$, $f(x) = a_0 + a_1 x$ gdje su a_0 i a_1 kompleksni brojevi te ω primitivni četvrti korijen jedinice. Računanje

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

zahtjeva najviše četiri množenja (točnije, tri: $a_1\omega, a_1\omega^2, a_1\omega^3$).

Pretpostavimo sada da je $r = 3$. Tada je ω primitivni osmi korijen jedinice, a $f(x)$ je stupnja 3; $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$. Da bismo evaluirali $f(x)$ u $1, \omega, \omega^2, \ldots, \omega^7$, moramo učiniti sljedeće:

$$\begin{aligned} f(x) &= (a_0 + a_2x^2) + x(a_1 + a_3x^2) \\ &= (a_0 + a_2y) + x(a_1 + a_3y), \end{aligned}$$

za $y = x^2$,

$$= g_0(y) + xg_1(y),$$

gdje je $g_0(y) = a_0 + a_2y$ i $g_1(y) = a_1 + a_3y$.

Stoga, evaluirati $f(x)$ u $1, \omega, \omega^2, \ldots, \omega^7$ je isto što i evaluirati $g_0(y) = g_0(x^2)$ u $y = 1, \omega^2, \omega^4, \omega^6$, zatim evaluirati $g_1(y) = g_1(x^2)$ u $y = 1, \omega^2, \omega^4, \omega^6$, te pomnožiti $g_1(y)$ s $x = 1, \omega, \omega^2, \ldots, \omega^7$.
Evaluacija $g_0(y) = g_0(x^2)$ u $y = 1, \omega^2, \omega^4, \omega^6$ zahtjeva najviše četiri množenja (slijedi iz slučaja $r = 2$), te evaluacija $g_1(y) = g_1(x^2)$ u $y = 1, \omega^2, \omega^4, \omega^6$ također zahtjeva najviše četiri množenja (slijedi iz slučaja $r = 2$). Nadalje, množenje $g_1(x^2)$ s x za $x = 1, \omega, \omega^2, \ldots, \omega^7$ zahtjeva najviše osam množenja (točnije najviše sedam jer imamo jedno množenje s jedinicom što zapravo i nije množenje).

Prema tome, evaluacija polinoma $f(x)$ stupnja $3 < 2^2$ na osmu potenciju primitivnog osmog korijena jedinice zahtjeva najviše $16 = 8 \cdot 2$ množenja.

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

Neka je $f(x)$ polinom stupnja strogo manjeg od 2^r. Želimo ga evaluirati u svakoj potenciji $1, \omega, \omega^2, \ldots, \omega^{2^{r+1}-1}$ primitivnog 2^{r+1}-tog korijena jedinice. Kao za polinom stupnja 3, zapišemo $f(x)$ kao sumu parnih potencija od x, tj. polinom $g_0(x^2)$, i sumu neparnih potencija od x, tj. polinom $g_1(x^2)$ puta x. Dakle, $f(x) = g_0(x^2) + xg_1(x^2)$. Sada stavimo $y = x^2$.

Evaluacija $g_0(x^2)$ u $x = 1, \omega, \omega^2, \ldots, \omega^{2^r-1}$ je isto što i evaluacija $g_0(y)$ u $y = 1, \omega^2, \omega^4, \ldots, \omega^{2(2^r-1)}$. Ali, ω^2 je primitivni 2^r-ti korijen jedinice pa zato evaluiramo polinom $g_0(y)$ stupnja strogo manjeg od 2^{r-1} u potencijama od ω^2. Prema induktivnoj pretpostavci to zahtjeva najviše M_{r-1} množenja.

Slično, potrebno je najviše M_{r-1} množenja da bismo evaluirali $g_1(y)$ za $y = 1, \omega^2, \omega^4, \ldots, \omega^{2(2^r-1)}$.

Konačno, potrebno je najviše 2^{r+1} množenja da bismo pomnožili vrijednosti $g_1(y) = g_1(x^2)$ s $x = 1, \omega, \omega^2, \ldots, \omega^{2^{r+1}-1}$.

Dakle, ukupan broj potrebnih množenja iznosi M_r, gdje je

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

□

Dokaz prethodnog teorema opisuje algoritam poznat pod nazivom Brza Fourierova transformacija. Evaluacija polinoma $f(x)$ u $1, \omega, \omega^2, \ldots, \omega^{2^r-1}$ je isto što i primjena diskretne Fourierove transformacije na $f(x)$. Dokaz pokazuje kako doći do rezultata vrlo brzo.

Vratimo se postupku određivanje produkta $f(x)g(x)$ dva polinoma stupnja d.

Za I. korak pretpostavimo da je $2^{r-2} \leq d < 2^{r-1}$ i evaluirajmo $f(x)$ i $g(x)$ u svim potencijama primitivnog 2^r-tog korijena ω. Prema prethodnom teoremu za to je potrebno $2 \cdot 2^r(r-1)$ množenja. Očito vrijedi $2^{r-1} \leq 2d < 2^r \leq 4d$. Stoga je $r - 1 \leq \log_2 2d$ pa slijedi

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

Korolar 3.1. I. korak postupka za pronalaženje produkta dva polinoma stupnja d zahtijeva najviše $8d \log_2 2d$ množenja.

Primijetimo da je dobiveni broj znatno manji od $(d+1)^2$ za veliki d.

Rekli smo ranije da je za II. korak postupka potrebno $2d + 1$ množenja, što je daleko manje od $(d+1)^2$ za veliki d. Sada znamo da ukoliko odaberemo odgovarajuće elemente za evaluaciju polinoma, tada će za provedbu prvog koraka postupka također biti potrebno znatno manje množenja od $(d+1)^2$ za veliki d.

Preostaje još ispitati III. korak postupka.

Propozicija 3.1. Neka je ζ primitivni l-ti korijen jedinice. Tada je

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{l-1} = 0 \quad \textit{ako} \quad \textit{je} \quad \zeta \neq 1,$$

i

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{l-1} = l \quad \textit{ako} \quad \textit{je} \quad \zeta = 1,$$

Dokaz. Druga jednakost je očita. Za dokaz prve jednakosti, uočimo da je ζ korijen od $x^l - 1 = (x-1)(1 + x + \cdots + x^{l-1})$, ali nije korijen od $x - 1$ ako je $\zeta \neq 1$. Stoga, ζ mora biti korijen faktora $1 + x + \cdots + x^{l-1}$. Dakle, $1 + \zeta + \zeta^2 + \cdots + \zeta^{l-1} = 0$. □

Teorem 3.4. Neka je $l = 2^r$, ω primitivni l-ti korijen jedinice te

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{l-1} x^{l-1}.$$

Pretpostavimo da su nam poznate vrijednosti $c_0 = h(1)$, $c_1 = h(\omega)$, …, $c_{l-1} = h(\omega^{l-1})$. Neka je $c(x)$ polinom

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{l-1} x^{l-1}.$$

Tada možemo pronaći koeficijente $h_0, h_1, \ldots, h_{l-1}$ tako da evaluiramo polinom $c(x)$, tj.

$$h_m = \frac{c(\omega^{l-m})}{l} \quad za \quad m = 0, 1, 2, \ldots, l-1.$$

Prema tome je

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

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

Dokaz. U dokazu teorema koristit ćemo vektorsku i matričnu notaciju. Ako je

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{l-1} x^{l-1},$$

tada je za svaki i

$$c_i = h(\omega^i) = h_0 + h_1 \omega^i + h_2 \omega^{2i} + \cdots + h_{l-1} \omega^{(l-1)i}.$$

Stoga, vektor redak

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

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

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

vektor redak čiji su elementi koeficijenti polinoma $h(x)$, a $\boldsymbol{F}$ je $l \times l$ matrica

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

koja se naziva diskretna Fourierova transformacija. Inverz matrice $\boldsymbol{F}$ je matrica $\frac{\widehat{\boldsymbol{F}}}{l}$ gdje su elementi od $\widehat{\boldsymbol{F}}$ inverzi elemenata od $\boldsymbol{F}$. Matrica $\widehat{\boldsymbol{F}}$ se naziva inverzna diskretna Fourierova transformacija od $\boldsymbol{F}$.

Da bismo pokazali da je $\frac{\widehat{\boldsymbol{F}}}{l}$ inverzna matrica matrice $\boldsymbol{F}$, najprije treba primijetiti da je i-ti redak matrice $\widehat{\boldsymbol{F}}$ jednak

$$(1, \omega^{-i}, \omega^{-2i}, \omega^{-3i}, \dots, \omega^{-(l-1)i}),$$

a j-ti stupac matrice $\boldsymbol{F}$ je transponirani redak

$$(1, \omega^{j}, \omega^{2j}, \omega^{3j}, \dots, \omega^{(l-1)j}).$$

Množenjem i-tog retka matrice $\widehat{\boldsymbol{F}}$ s j-tim stupcem matrice $\boldsymbol{F}$ dobivamo:

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

Neka je $\zeta = \omega^{j-i}$. Tada je ζ l-ti korijen jedinice i

$$q_{ij} = 1 + \zeta + \zeta^2 + \dots + \zeta^{l-1}.$$

Iz Propozicije 3.1 slijedi je $q_{ij} = 0$ za $j \neq i$, te $q_{ii} = l$. Stoga, $\widehat{\boldsymbol{F}}\boldsymbol{F} = l\boldsymbol{I}$, tj. dokazali smo da je matrica $\frac{\widehat{\boldsymbol{F}}}{l}$ inverzna matrica matrice $\boldsymbol{F}$.

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

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

□

Sada smo u poziciji odrediti ukupan broj množenja opisanog postupka za pronalaženje produkta $f(x)g(x)$ gdje su $f(x)$ i $g(x)$ polinomi stupnja $d < 2^{r-1}$, koji se sastoji od tri koraka:

I. Evaluacija polinoma $f(x)$ i $g(x)$ u potencijama od ω, primitivnog 2^r-tog korijena jedinice: za evaluaciju polinoma $f(x)$ potrebno je $2^r(r-1)$ množenja, kao i za evaluaciju polinoma $g(x)$.

II. Množenje $f(\omega^i)g(\omega^i) = h(\omega^i)$ za $i = 0, 1, 2, \ldots, 2^{r-1}$: potrebno je 2^r množenja.

III. Interpolacija polinoma $h(x)$ pomoću $h(\omega^i)$, $i = 0, 1, \ldots, 2^{r-1}$: pokazali smo da je ovaj postupak identičan evaluaciji polinoma

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

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

Dakle, ukupan broj množenja je najviše

$$2^r(r-1) + 2^r(r-1) + 2^r + 2^r r = 2^r(3r-1).$$

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

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

Za veliki d, $4d(3\log_2 4d)$ je znatno manji od $(d+1)^2$. Preciznije, ako d raste, kvocijent $4d(3\log_2 4d)/(d+1)^2$ teži prema nuli.

Na ovaj način smo opisali postupak brzog množenja polinoma s kompleksnim koeficijentima. Uz određene izmjene, uglavnom algebarske prirode, postupak se može prilagoditi i za primjenu na množenje polinoma s cjelobrojnim koeficijentima.

U postupku pretvorbe vektora $\boldsymbol{H}$ koeficijenata polinoma $h(x)$ u vektor $\boldsymbol{C} = (h(1), h(\omega), \ldots, h(\omega^{l-1}))$ množenjem s $\boldsymbol{F}$, diskretnu Fourierovu transformaciju možemo odrediti metodom opisanom u Teoremu 3.3. Opisana metoda je primjena algoritma poznatog pod nazivom Brza Fourierova transformacija, kojeg su 1965. objavili J.W.Cooley (IBM) i J.W.Tukey (Princeton). Brza Fourierova transformacija se često naziva najznačajnijim numeričkim algoritmom modernog doba.

Literatura

[1] S. Bingulac, *Primjene Eulerova teorema i Kineskog teorema o ostatcima*, diplomski rad, Odjel za matematiku, Sveučilište u Osijeku, 2011.

[2] F. M. Brückler, *Povijest matematike 1*, Odjel za matematiku, Sveučilište u Osijeku, 2007.

[3] F. M. Brückler, *Povijest matematike 2*, Odjel za matematiku, Sveučilište u Osijeku, 2010.

[4] L. N. Childs, *A concrete introduction to higher algebra*, Springer Verlag, Berlin, 1995.

[5] A. Dujella, *Uvod u teoriju brojeva* (skripta), Prirodoslovno-matematički fakultet, Matematički odsjek, Sveučilište u Zagrebu, 2008., dostupno na *http://web.math.hr/ duje/utb/utblink.pdf*

[6] I. Matić, D. Ševerdija, *Grčko-kineski stil u teoriji brojeva*, Osječki matematički list, Vol. 10(2010), 43–58.