Osječki matematički list 15 (2015), 33-40

Kongruencije oblika $x^n \equiv 0 \pmod{m}$

Bernadin Ibrahimpašić*

Sažetak

U radu se opisuje metoda za rješavanje kongruencija oblika $x^n \equiv 0 \pmod{m}$, gdje su m i n prirodni brojevi, te njena primjena na rješavanje nekih polinomijalnih kongruencija.

Ključne riječi: *kongruencije, polinomijalne kongruencije*

Congruences of the type $x^n \equiv 0 \pmod{m}$

Abstract

In this paper we consider a method for solving congruences of the type $x^n \equiv 0 \pmod{m}$, where m and n are natural numbers, and we aplly this method to solving some polynomial congruences.

Keywords: *congruences, polynomial congruences*

1 Kongruencije

Pojam djeljivosti je jedan od najjednostavnijih, ali ujedno i najvažnijih pojmova u teoriji brojeva.

Definicija 1.1. Neka su a i b, $a \neq 0$, cijeli brojevi. Kažemo da je b *djeljiv* s a, odnosno da a *dijeli* b, ako postoji cijeli broj k takav da je $b = ak$. To zapisujemo s $a \mid b$. Ako b nije djeljiv s a, onda pišemo $a \nmid b$. Ako $a \mid b$, onda još kažemo da je a *djelitelj* od b, a da je b *višekratnik* od a.

*Pedagoški fakultet, 77000 Bihać, Bosna i Herzegovina, bernadin@bih.net.ba

Teorem 1.1 (Teorem o dijeljenju s ostatkom). *Za proizvoljan prirodan broj b i cijeli broj a postoje jedinstveni cijeli brojevi q i r takvi da je $a = qb + r, 0 \leq r < b$.*

Broj q se zove količnik a r se zove ostatak.
Uz pojam djeljivosti direktno je vezan i pojam kongruencija, koji je uveo Gauss u svom poznatom djelu "Disquisitiones Arithmeticae" 1801. godine.

Definicija 1.2. Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je *a kongruentan b* modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom kažemo da *a nije kongruentan b* modulo m i pišemo $a \not\equiv b \pmod{m}$.

Iz činjenice da je $a - b$ djeljivo s m ako i samo ako je $a - b$ djeljivo s $-m$, zaključujemo da je dovoljno razmatrati samo slučajeve kada je m prirodan broj.
Iz definicije kongruencija i Teorema o dijeljenju s ostatkom imamo da ako je $a \equiv b \pmod{m}$, onda postoji cijeli broj k takav da je $a = km + b$.
Svojstva kongruencija su iskazana sljedećim teoremom.

Teorem 1.2. *Neka su a, b, c, d cijeli brojevi, $m_1, m_2, \ldots, m_r$ prirodni brojevi i f polinom s cjelobrojnim koeficijentima.*

1. $a \equiv b \pmod{m}$ *ako i samo ako je* $a - b \equiv 0 \pmod{m}$.
2. *Ako je* $a \equiv b \pmod{m}$, *onda je* $a \equiv b + km \pmod{m}, \forall k \in \mathbb{Z}$.
3. *Ako je* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ *i* $ac \equiv bd \pmod{m}$.
4. *Ako je* $a \equiv b \pmod{m}$ *i* $d \mid m$, *onda je* $a \equiv b \pmod{d}$.
5. *Ako je* $a \equiv b \pmod{m}$, *onda je* $ac \equiv bc \pmod{mc}$ *za svaki* $c > 0$.
6. $a \equiv b \pmod{m_i}$, $i = 1, 2, \ldots, r$, *ako i samo ako je* $a \equiv b \pmod{\operatorname{nzv}(m_1, m_2, \ldots, m_r)}$.
7. *Ako je* $a \equiv b \pmod{m}$, *onda je* $f(a) \equiv f(b) \pmod{m}$.
8. $ax \equiv ay \pmod{m}$ *ako i samo ako je* $x \equiv y \pmod{\frac{m}{\operatorname{nzd}(a,m)}}$.

Osim navedenih svojstava treba istaknuti da je relacija "biti kongruentan modulo m" relacija ekvivalencije na skupu $\mathbb{Z}$, tj. ona je refleksivna, simetrična i tranzitivna.

2 Linearne kongruencije

Jedan od problema u teoriji brojeva je i rješavanje linearnih kongruencija oblika $ax \equiv b \pmod{m}$, gdje su a i m prirodni brojevi, te b cijeli broj. Navedena kongruencija ima rješenja ako i samo ako $\text{nzd}(a, m)$ dijeli b, i u tom slučaju postoji beskonačno mnogo rješenja. O uvjetima rješivosti linearnih kongruencija se može vidjeti u [2], gdje je opisana i metoda za njihovo rješavanje pomoću Euklidovog algoritma za određivanje najvećeg zajedničkog djelitelja dva prirodna broja. Euklidov algoritam je efikasan način za određivanje najvećeg zajedničkog djelitelja dva prirodna broja, koji ne zahtijeva njihovu prethodnu faktorizaciju, a osnova mu je Teorem o dijeljenju s ostatkom. Opis Euklidovog algoritma i širok spektar njegovih primjena, kao što su rješavanje linearnih diofantskih jednadžbi, rješavanje linearnih kongruencija, određivanje multiplikativnog inverza u konačnom polju, te određivanje razvoja racionalnog broja u verižni razlomak se može pronaći u [3]. Osim metode za rješavanje linearnih kongruencija pomoću Euklidovog algoritma, u [4] su opisane još tri metode za njihovo rješavanje. To su metoda svođenja na diofantsku jednadžbu i metoda transformacije koeficijenata, te Eulerova metoda.

3 Kongruencije oblika $x^n \equiv 0 \pmod{m}$

Slično kao kod jednadžbi imamo da rješenje kongruencije $f(x) \equiv 0 \pmod{m}$, gdje je $f(x)$ polinom s cjelobrojnim koeficijentima, predstavlja svaki cijeli broj x koji tu kongruenciju zadovoljava. Također imamo da ako je x_1 neko rješenje kongruencije $f(x) \equiv 0 \pmod{m}$, i $x_2 \equiv x_1 \pmod{m}$, onda je i x_2 također rješenje te kongruencije. Za dva rješenja x_1 i x_2 kongruencije $f(x) \equiv 0 \pmod{m}$ kažemo da su ekvivalentna ako je $x_1 \equiv x_2 \pmod{m}$. Pod brojem rješenja kongruencije podrazumijevamo broj neekvivalentnih rješenja.

Za razliku od linearne kongruencije oblika $ax \equiv b \pmod{m}$, koja može ali ne mora imati rješenje, kongruencija oblika $x^n \equiv 0 \pmod{m}$, gdje su m i n prirodni brojevi, mora imati bar jedno rješenje $x \equiv 0 \pmod{m}$. U cilju pronalaženja ostalih rješenja, pogledajmo kanonski rastav broja m na proste faktore. Kako je prema Osnovnom teoremu aritmetike faktorizacija svakog prirodnog broja, većeg od 1, na proste faktore jedinstvena do na poredak prostih faktora, to je zapis broja m u obliku $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gdje su p_i različiti prosti brojevi, a α_i prirodni brojevi, jedinstven. Da bi neki $x_0 > 0$ bio rješenje kongruencije $x^n \equiv 0 \pmod{m}$, to bi on morao biti oblika $x_0 = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, gdje je $n\beta_i \geq \alpha_i$, $i = 1, 2, \ldots, k$. Time smo

dokazali idući teorem.

Teorem 3.1. Neka su n i $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ prirodni brojevi. Tada je jedno rješenje kongruencije $x^n \equiv 0 \pmod{m}$ dano s

$$x_0 = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}, \text{ gdje je } \beta_i = \left\lfloor \frac{\alpha_i + n - 1}{n} \right\rfloor, \ i = 1, 2, \ldots, k,$$

a sva njena rješenja su

$$x = j \cdot x_0, \ \ j \in \mathbb{Z}.$$

Sva nekongruentna rješenja su dana s

$$x = j \cdot x_0, \ \ j = 0, 1, \ldots, \frac{m}{x_0} - 1.$$

Korolar 3.1. *Neka je n prirodan broj i p prost broj. Tada je $x \equiv 0 \pmod{p}$ jedino rješenje kongruencije $x^n \equiv 0 \pmod{p}$.*

U sljedećem primjeru ćemo pokazati primjenu prethodnih tvrdnji u tri slučaja, i to kada je m prost broj, kada je m potencija prostog broja, te kada m ima bar dva različita prosta faktora.

Primjer 3.1. Riješiti kongruencije:

a) $x^2 \equiv 0 \pmod{13}$,

b) $x^4 \equiv 0 \pmod{1024}$,

c) $x^3 \equiv 0 \pmod{762048}$.

Rješenje.

a) Kako je $m = 13$ prost broj, to je $x \equiv 0 \pmod{13}$ jedino rješenje dane kongruencije.

b) Kako je $m = 1024 = 2^{10}$ to je

$$\alpha_1 = 10 \quad \text{i} \quad \beta_1 = \left\lfloor \frac{10 + 4 - 1}{4} \right\rfloor = 3,$$

pa je $x_0 = 2^3 = 8$ jedno rješenje kongruencije $x^4 \equiv 0 \pmod{1024}$. Kako je $1024/8 - 1 = 128 - 1 = 127$, to su sva njena nekongruentna rješenja

$$x = j \cdot x_0 = 8j, \ \ j = 0, 1, \ldots, 127.$$

c) Kako je

$$m = 2^6 \cdot 3^5 \cdot 7^2,$$

to je

$$\alpha_1 = 6 \qquad \Rightarrow \qquad \beta_1 = \left\lfloor \tfrac{6+3-1}{3} \right\rfloor = 2,$$

$$\alpha_2 = 5 \qquad \Rightarrow \qquad \beta_2 = \left\lfloor \tfrac{5+3-1}{3} \right\rfloor = 2,$$

$$\alpha_3 = 2 \qquad \Rightarrow \qquad \beta_3 = \left\lfloor \tfrac{2+3-1}{3} \right\rfloor = 1.$$

Jedno rješenje kongruencije $x^3 \equiv 0 \pmod{762048}$ dano je s

$$x_0 = 2^2 \cdot 3^2 \cdot 7^1 = 252,$$

a kako je $\dfrac{762048}{252} - 1 = 3023$, to su sva njena nekongruentna rješenja dana s

$$x = j \cdot x_0 = 252j, \quad j = 0, 1, \ldots, 3023.$$

◀

4 Primjena na polinomijalne kongruencije

Definicija 4.1. Neka je m prirodan broj i neka je

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0,\ a_i \in \mathbb{Z},\ i = 1, \ldots, n,$$

polinom s cjelobrojnim koeficijentima. Tada se kongruencija oblika

$$f(x) \equiv 0 \pmod{m}$$

naziva *polinomijalna kongruencija*.

Problem pronalaženja nekongruentnih rješenja polinomijalne kongruencije $f(x) \equiv 0 \pmod{m}$ je težak i mnoge metode za njeno rješavanje su uglavnom vezane za metodu pokušaja i promašaja. Jedna metoda je da provjerimo koje sve vrijednosti iz skupa $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ zadovoljavaju kongruenciju $f(x) \equiv 0 \pmod{m}$.

Primjer 4.1. Riješiti kongruencije

a) $2x^3 - 3x + 1 \equiv 0 \pmod 4$,

b) $3x^3 - 2x^2 + 2 \equiv 0 \pmod 4$.

Rješenje.

a) Provjerimo sve elemente iz skupa $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$$\begin{aligned} f(0) &= 2 \cdot 0^3 - 3 \cdot 0 + 1 = 1 \equiv 1 \not\equiv 0 \pmod 4, \\ f(1) &= 2 \cdot 1^3 - 3 \cdot 1 + 1 = 0 \equiv 0 \pmod 4, \\ f(2) &= 2 \cdot 2^3 - 3 \cdot 2 + 1 = 11 \equiv 3 \not\equiv 0 \pmod 4, \\ f(3) &= 2 \cdot 3^3 - 3 \cdot 3 + 1 = 46 \equiv 2 \not\equiv 0 \pmod 4. \end{aligned}$$

Vidimo da je $x \equiv 1 \pmod 4$ rješenje kongruencije $2x^3 - 3x + 1 \equiv 0 \pmod 4$.

b) Postupimo li analogno kao u prethodnom slučaju, dobivamo da je $3x^3 - 2x^2 + 2 = 2, 3, 18, 65$ redom, pa vidimo da je $3x^3 - 2x^2 + 2 \not\equiv 0 \pmod 4$ što znači da kongruencija $3x^3 - 2x^2 + 2 \equiv 0 \pmod 4$ nema rješenja. ◀

U slučaju kada je m velik broj, ova metoda nije praktična. Pogledajmo sada kako se neke polinomijalne kongruencije mogu riješiti svođenjem polazne kongruencije na kongruenciju oblika $x^n \equiv 0 \pmod m$.

Primjer 4.2. Riješiti kongruenciju $3x^2 + 10x \equiv 1 \pmod{28}$.

Rješenje. Kako je zbog refleksivnosti $1 \equiv 1 \pmod{28}$, to prema tvrdnji 3. teorema 1.2 imamo da je polazna kongruencija ekvivalentna s kongruencijom $3x^2 + 10x - 1 \equiv 0 \pmod{28}$. Kako je $\text{nzd}(3, 28) = 1$, to je prema tvrdnji 8 Teorema 1.2, dobivena kongruencija ekvivalentna s kongruencijom $9x^2 + 30x - 3 \equiv 0 \pmod{28}$. Svedemo li izraz na lijevoj strani na potpun kvadrat dobivamo

$$\begin{aligned} 9x^2 + 30x - 3 &\equiv 0 \pmod{28}, \\ (3x + 5)^2 - 5^2 - 3 &\equiv 0 \pmod{28}, \\ (3x + 5)^2 - 28 &\equiv 0 \pmod{28}, \\ (3x + 5)^2 &\equiv 28 \pmod{28}, \\ (3x + 5)^2 &\equiv 0 \pmod{28}. \end{aligned}$$

Dobili smo da je polazna kongruencija ekvivalentna kongruenciji

$$(3x + 5)^2 \equiv 0 \pmod{28}.$$

Uvedemo li supstituciju $3x + 5 = t$, imamo za riješiti kongruenciju

$$t^2 \equiv 0 \pmod{28}.$$

Na ranije opisani način dobivamo da su njena rješenja $t = 0, 14$. Vratimo li nazad supstituciju $3x + 5 \equiv t \pmod{28}$, možemo odrediti rješenja polazne kongruencije rješavajući dobivene linearne kongruencije.

$$\begin{aligned} 3x + 5 &\equiv 0 \pmod{28} \\ 3x &\equiv -5 \pmod{28} \\ 3x &\equiv 23 \pmod{28} \\ x &\equiv 17 \pmod{28} \end{aligned}$$

$$\begin{aligned} 3x + 5 &\equiv 14 \pmod{28} \\ 3x &\equiv 9 \pmod{28} \\ x &\equiv 3 \pmod{28} \end{aligned}$$ ◀

Rješenja kongruencije $3x^2 + 10x \equiv 1 \pmod{28}$ su

$$x \equiv 3, 17 \pmod{28}.$$

Primjer 4.3. Riješiti kongruenciju $8x^3 + 10x^2 + 25 \equiv 0 \pmod{50}$.

Rješenje. Kako je $10 \equiv 60$, $0 \equiv 150$ i $25 \equiv 125 \pmod{50}$, to je polazna kongruencija ekvivalentna kongruenciji

$$8x^3 + 60x^2 + 150x + 125 = (2x + 5)^3 \equiv 0 \pmod{50}.$$

Uvedemo li supstituciju $2x + 5 = t$, dobivamo kongruenciju $t^3 \equiv 0 \pmod{50}$ čija su rješenja $t \equiv 0, 10, 20, 30, 40 \pmod{50}$. Vratimo li supstituciju dobivamo linearne kongruencije $2x + 5 \equiv 0, 10, 20, 30, 40 \pmod{50}$, a one su redom ekvivalentne linearnim kongruencijama $2x \equiv -5, 5, 15, 25, 35 \pmod{50}$. Kako je $\text{nzd}(2, 50) = 2$ a kako $2 \nmid -5, 5, 15, 25, 35$, to posljednje kongruencije nemaju rješenja. Zaključujemo da polazna kongruencija nema rješenja. ◀

Literatura

[1] B. IBRAHIMPAŠIĆ, *Uvod u teoriju brojeva*, Pedagoški fakultet, Bihać, 2014.

[2] B. Ibrahimpašić, S. Ibrahimpašić-, *Linearne kongruencije i sistemi linearnih kongruencija*, MAT–KOL Vol XX (1)(2014), 27–36.

[3] B. Ibrahimpašić, A. Zolić, *Euklidov algoritam i njegove primjene*, Nastava matematike, LVIII 1–2(2013), 14–23.

[4] B. Ibrahimpašić, A. Zolić, *Četiri metode za rješavanje linearnih kongruencija*, preprint