MAT–KOL (Banja Luka)
ISSN 0354–6969 (p), ISSN 1986–5228 (o)
Vol. XXI (3)(2015), 159–171
http://www.imvibl.org/dmbl/dmbl.htm

POLINOMSKE KONGRUENCIJE

Bernadin Ibrahimpašić[1]

Sažetak. U članku se opisuju metode za rješavanje polinomskih kongruencija, tj. kongruencija oblika $f(x) \equiv 0 \pmod{m}$, gdje je m prirodan broj a $f(x)$ polinom s cjelobrojnim koeficijentima.

Ključne riječi i fraze: kongruencije, polinomske kongruencije.

Abstract. In this paper we describe some methods for solving the polynomial congruences $f(x) \equiv 0 \pmod{m}$, where $f(x)$ has integer coefficients.

AMS Mathematics Subject Classification (2010): 11A07

Key words and phrases: Congruences, Polynomial congruences.

1 Uvod

Gauss u svom poznatom djelu "Disquisitiones Arithmeticae" 1801. godine uvodi pojam kongruencija. Njihov zapis podsjeća na jednakosti, a kongruencije imaju i mnoga zajednička svojstva s jednakostima.

Definicija 1.1 *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 $a \not\equiv b \pmod{m}$.*

Kako je $a - b$ djeljivo s m ako i samo ako je djeljivo s $-m$, to se obično razmatraju samo slučajevi kada je m prirodan broj.

Iz definicije je očigledno da ako je $a \equiv b \pmod{m}$, to znači da postoji cijeli broj k takav da je $a = km + b$.

Definicija 1.2 *Neka su a i m prirodni brojevi, te b cijeli broj. Kongruencija oblika $ax \equiv b \pmod{m}$ se naziva* linearna kongruencija.

Rješenje kongruencije $ax \equiv b \pmod{m}$, gdje su a i m prirodni brojevi, i b cijeli broj, je svaki cijeli broj x koji je zadovoljava. Ako je x_1 neko rješenje te

[1]Pedagoški fakultet Univerziteta u Bihaću, Luke Marjanovića bb, 77000 Bihać, Bosna i Hercegovina, e-mail: bernadin@bih.net.ba

kongruencije i $x_2 \equiv x_1 \pmod{m}$, onda je i x_2 također njeno rješenje. Za dva rješenja x i x' kongruencije $ax \equiv b \pmod{m}$ kažemo da su ekvivalentna ako je $x \equiv x' \pmod{m}$. Pod brojem rješenja kongruencije podrazumijevamo broj neekvivalentnih rješenja.

Teorem 1.1 *Neka su a i m prirodni brojevi, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = \mathrm{nzd}(a, m)$ dijeli b. Ako je ovaj uslov ispunjen, onda gornja kongruencija ima tačno d rješenja modulo m, i to*

$$x_0 + j \cdot \frac{m}{d}, \quad j = 0, 1, \ldots, d-1,$$

gdje je x_0 jedinstveno rješenje kongruencije $ax/d \equiv b/d \pmod{m/d}$.

O osnovnim osobinama kongruencija, uslovima rješivosti linearnih kongruencija oblika $ax \equiv b \pmod{m}$, gdje su a i m prirodni brojevi, i b cijeli broj, se može pronaći u [3]. Na istom mjestu se mogu pronaći i metode za rješavanje sistema linearnih kongruencija s jednom nepoznatom. U [4] su opisane četiri metode za rješavanje linearnih kongruencija, dok je u [2] opisana metoda za rješavanje kongruencija oblika $x^n \equiv 0 \pmod{m}$, gdje su m i n prirodni brojevi.

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

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

Teorem 2.1 *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*

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

a sva njena rješenja su

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

Sva nekongruentna rješenja su dana s

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

Korolar 2.1 *Neka su n prirodan i p prost broj. Tada je $x \equiv 0 \pmod{p}$ jedino rješenje kongruencije $x^n \equiv 0 \pmod{p}$.*

Primjer 2.1 *Riješiti kongruencije:*

a) $x^7 \equiv 0 \pmod{19}$,

b) $x^3 \equiv 0 \pmod{512}$,

c) $x^4 \equiv 0 \pmod{570752}$.

Rješenje:

a) Kako je $m = 19$ prost broj, to je $x \equiv 0 \pmod{19}$ jedino rješenje kongruencije $x^7 \equiv 0 \pmod{19}$.

b) Kako je $m = 512 = 2^9$ to je

$$\alpha_1 = 9 \quad \text{i} \quad \beta_1 = \left\lfloor \frac{9+3-1}{3} \right\rfloor = 3,$$

pa je $x_0 = 2^3 = 8$ jedno rješenje kongruencije $x^3 \equiv 0 \pmod{512}$. Kako je $512/8 - 1 = 64 - 1 = 63$, to su sva njena nekongruentna rješenja

$$x = j \cdot x_0 = 8j, \quad j = 0, 1, \ldots, 63.$$

c) Kako je

$$m = 2^7 \cdot 7^3 \cdot 13^1,$$

to je

$$\begin{aligned} \alpha_1 &= 7 && \Rightarrow && \beta_1 = \left\lfloor \tfrac{7+4-1}{4} \right\rfloor = 2, \\ \alpha_2 &= 3 && \Rightarrow && \beta_2 = \left\lfloor \tfrac{3+4-1}{4} \right\rfloor = 1, \\ \alpha_3 &= 1 && \Rightarrow && \beta_3 = \left\lfloor \tfrac{1+4-1}{4} \right\rfloor = 1. \end{aligned}$$

Jedno rješenje kongruencije $x^4 \equiv 0 \pmod{570752}$ dano je s

$$x_0 = 2^2 \cdot 7^1 \cdot 13^1 = 364,$$

a kako je $570752/364 - 1 = 1567$, to su sva njena nekongruentna rješenja dana s

$$x = j \cdot x_0 = 364j, \quad j = 0, 1, \ldots, 1567.$$

♢

3 Polinomske kongruencije

Definicija 3.1 *Neka je m prirodan broj i neka je*

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

polinom s cjelobrojnim koeficijentima. Tada se kongruencija oblika

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

naziva polinomska kongruencija.

Općenito, kao i kod linearnih kongruencija, ako je x_0 neko rješenje polinomske kongruencije $f(x) \equiv 0 \pmod{m}$, onda je svaki x, takav da je $x \equiv x_0 \pmod{m}$, također rješenje posmatrane kongruencije. Međutim, nas interesuju samo nekongruentna rješenja,

Teorem 3.1 (Lagrange) *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stepena n. Neka je p prost broj koji ne dijeli vodeći koeficijent polinoma f. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.*

Propozicija 3.1 *Neka je p prost broj. Ako $d|(p-1)$ onda kongruencija $x^d \equiv 1 \pmod{p}$ ima tačno d rješenja, tj. polinom $x^d - 1$ ima tačno d nultačaka u $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.*

Teorem 3.2 *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Za prirodan broj m s $N(m)$ označimo broj nekongruentnih rješenja kongruencije $f(x) \equiv 0 \pmod{m}$. Ako je $m = m_1 \cdot m_2$, gdje je $\mathrm{nzd}(m_1, m_2) = 1$, tada je $N(m) = N(m_1) \cdot N(m_2)$. Ako je $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ kanonski rastav broja m, onda je $N(m) = \prod_k N(p_k^{\alpha_k})$.*

Problem nalaženja nekongruentnih rješenja polinomske kongruencije $f(x) \equiv 0 \pmod{m}$ je težak. Mnoge metode za njeno rješavanje su uglavnom vezane za metodu pokušaja i promašaja. Tako imamo da je jedna metoda rješavanja da provjerimo koje sve vrijednosti iz skupa $\{0, 1, \ldots, m-1\}$ (ili iz nekog drugog potpunog sistema ostataka modulo m) zadovoljavaju kongruenciju $f(x) \equiv 0 \pmod{m}$. Na taj način možemo odrediti sva nekongruentna rješenja posmatrane kongruencije.

Definicija 3.2 *Neka je m prirodan broj. Skup $\{x_1, x_2, \ldots, x_m\}$ od m cijelih brojeva se zove* potpun sistem ostataka *modulo m ako ne sadrži nijedan par brojeva kongruentnih modulo m, tj. ako sadrži tačno po jedan element iz svake klase ostataka modulo m. Drugim riječima, taj skup će biti potpun sistem ostataka ako za svaki cijeli broj y postoji tačno jedan element tog skupa x_j takav da je $y \equiv x_j \pmod{m}$.*

Treba istaknuti da je za svaki cijeli broj a, skup $\{a, a+1, \ldots, a+(m-1)\}$ potpun sistem ostataka modulo m. Potpunih sistema ostataka modulo m ima beskonačno mnogo, ali se posebno ističe sistem najmanjih nenegativnih ostataka $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

Primjer 3.1 *Riješiti kongruenciju $x^3 + 3x - 4 \equiv 0 \pmod{5}$.*

Rješenje: Možemo provjeriti sve elemente iz jednog od potpunih sistema ostataka modulo 5. Najlakše je raditi sa sistemom najmanjih nenegativnih ostataka $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

$$\begin{aligned}
f(0) &= 0^3 + 3 \cdot 0 - 4 = -4 \equiv 1 \not\equiv 0 \pmod 5 \\
f(1) &= 1^3 + 3 \cdot 1 - 4 = 0 \equiv 0 \pmod 5 \\
f(2) &= 2^3 + 3 \cdot 2 - 4 = 10 \equiv 0 \pmod 5 \\
f(3) &= 3^3 + 3 \cdot 3 - 4 = 32 \equiv 2 \not\equiv 0 \pmod 5 \\
f(4) &= 4^3 + 3 \cdot 4 - 4 = 72 \equiv 2 \not\equiv 0 \pmod 5
\end{aligned}$$

Vidimo da su

$$x \equiv 1 \pmod 5 \qquad \text{i} \qquad x \equiv 2 \pmod 5$$

rješenja kongruencije $f(x) \equiv 0 \pmod 5$.

♢

Primjer 3.2 *Riješiti kongruenciju* $x^3 + 2x^2 - 3x + 1 \equiv 0 \pmod 4$.

Rješenje: Kako je $f(0) \equiv f(1) \equiv f(3) \equiv 1 \pmod 4$ i $f(2) \equiv 3 \pmod 4$, to posmatrana kongruencija nema rješenja.

♢

Teorem 3.3 *Neka je $M = m_1 m_2 \cdot \ldots \cdot m_r$, gdje su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi. Tada je cijeli broj x_0 rješenje kongruencije*

$$f(x) \equiv 0 \pmod M$$

ako i samo ako je x_0 rješenje sistema od r kongruencija

$$\begin{aligned}
f(x) &\equiv 0 \pmod{m_1}, \\
f(x) &\equiv 0 \pmod{m_2}, \\
&\vdots \\
f(x) &\equiv 0 \pmod{m_r}.
\end{aligned}$$

Primjer 3.3 *Riješiti kongruenciju* $x^3 - 2x^2 + 1 \equiv 0 \pmod{20}$.

Rješenje: Kako je $20 = 2^2 \cdot 5$, to ćemo rješavati sistem

$$\begin{aligned}
x^3 - 2x^2 + 1 &\equiv 0 \pmod 4, \\
x^3 - 2x^2 + 1 &\equiv 0 \pmod 5.
\end{aligned}$$

Rješavajući svaku kongruenciju na opisani način dobijamo da je rješenje prve kongruencije $x \equiv 1 \pmod 4$, a da su rješenja druge $x \equiv 1, 3 \pmod 5$. Sada sisteme

$$\begin{aligned}
x &\equiv 1 \pmod 4 \\
x &\equiv 1 \pmod 5
\end{aligned}
\qquad\qquad
\begin{aligned}
x &\equiv 1 \pmod 4 \\
x &\equiv 3 \pmod 5
\end{aligned}$$

riješimo (npr. pomoću Kineskog teorema o ostacima [3]) i dobijemo da je rješenje prvog sistema $x \equiv 1 \pmod{20}$, a da je $x \equiv 13 \pmod{20}$ rješenje drugog sistema. Tako smo dobili da su

$$x \equiv 1 \pmod{20} \qquad \text{i} \qquad x \equiv 13 \pmod{20}$$

rješenja kongruencije $x^3 - 2x^2 + 1 \equiv 0 \pmod{20}$.

$\diamondsuit$

Primjer 3.4 *Riješiti kongruenciju* $2x^3 - 3x + 5 \equiv 0 \pmod{30}$.

Rješenje: Kako je $30 = 2 \cdot 3 \cdot 5$, to broj 30 možemo rastaviti na proizvod u parovima relativno prostih brojeva na sljedeća 4 načina

$$30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6 = 2 \cdot 3 \cdot 5.$$

To znači da zadatak možemo riješiti rješavajući jedan od sljedeća četiri sistema.

$$\begin{array}{llll} f(x) \equiv 0 \pmod{2} & f(x) \equiv 0 \pmod{3} & f(x) \equiv 0 \pmod{5} & f(x) \equiv 0 \pmod{2} \\ f(x) \equiv 0 \pmod{15} & f(x) \equiv 0 \pmod{10} & f(x) \equiv 0 \pmod{6} & f(x) \equiv 0 \pmod{3} \\ & & & f(x) \equiv 0 \pmod{5} \end{array}$$

gdje je $f(x) = 2x^3 - 3x + 5$.

Kako je rješenje prve kongruencije prvog sistema $x \equiv 1 \pmod{2}$, a druge $x \equiv 2, 5, 8 \pmod{15}$, to rješavamo sljedeće sisteme.

$$\begin{array}{lll} x \equiv 1 \pmod{2} & x \equiv 1 \pmod{2} & x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{15} & x \equiv 5 \pmod{15} & x \equiv 8 \pmod{15} \end{array}$$

Rješenja ovih sistema su $x \equiv 17, 5, 23 \pmod{30}$.

Kako je rješenje prve kongruencije drugog sistema $x \equiv 2 \pmod{3}$, a druge $x \equiv 3, 5, 7 \pmod{10}$, to rješavamo sljedeće sisteme.

$$\begin{array}{lll} x \equiv 2 \pmod{3} & x \equiv 2 \pmod{3} & x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{10} & x \equiv 5 \pmod{10} & x \equiv 7 \pmod{10} \end{array}$$

Rješenja ovih sistema su $x \equiv 23, 5, 17 \pmod{30}$, redom.

Kako su rješenja prve kongruencije trećeg sistema $x \equiv 0, 2, 3 \pmod{5}$, a druge $x \equiv 5 \pmod{6}$, to rješavamo sljedeće sisteme.

$$\begin{array}{lll} x \equiv 0 \pmod{5} & x \equiv 2 \pmod{5} & x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{6} & x \equiv 5 \pmod{6} & x \equiv 5 \pmod{6} \end{array}$$

Rješenja ovih sistema su $x \equiv 5, 17, 23 \pmod{30}$, redom.

Kako je rješenje prve kongruencije četvrtog sistema $x \equiv 1 \pmod{2}$, druge $x \equiv 2 \pmod{3}$ i treće $x \equiv 0, 2, 3 \pmod{5}$, to rješavamo sljedeće sisteme.

$$\begin{array}{lll} x \equiv 1 \pmod 2 & x \equiv 1 \pmod 2 & x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 & x \equiv 2 \pmod 3 & x \equiv 2 \pmod 3 \\ x \equiv 0 \pmod 5 & x \equiv 2 \pmod 5 & x \equiv 3 \pmod 5 \end{array}$$

Rješenja ovih sistema su $x \equiv 5, 17, 23 \pmod{30}$, redom.

Vidimo da smo u sva četiri slučaja dobili ista rješenja, tj. rješenja kongruencije $2x^3 - 3x + 5 \equiv 0 \pmod{30}$ su

$$x \equiv 5 \pmod{30}, \qquad x \equiv 17 \pmod{30}, \qquad x \equiv 23 \pmod{30}.$$

$\diamondsuit$

Kako je jednostavan put za riješiti polinomsku kongruenciju modulo p^k, gdje je p prost broj, ako su joj poznata rješenja modulo p, to ćemo rješavanje kongruencije $f(x) \equiv 0 \pmod{p^k}$ svoditi na rješavanje kongruencije $f(x) \equiv 0 \pmod p$. Pomoću dobijenih rješenja modulo p ćemo tražiti rješenja modulo p^2. Nakon toga ćemo dobijena rješenja modulo p^2 iskoristiti za dobijanje rješenja modulo p^3, itd. Zbog toga ćemo kongruenciju $f(x) \equiv 0 \pmod m$ rješavati tako što ćemo rješavati sistem kongruencija

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}}, \quad i = 1, 2, \ldots, k,$$

gdje je $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ kanonski rastav modula m.

Primjer 3.5 *Riješiti kongruenciju* $3x^5 - x^3 + 3x^2 + 4 \equiv 0 \pmod{99}$.

Rješenje: Kako je $99 = 3^2 \cdot 11$, to ćemo rješavati sistem

$$\begin{aligned} 3x^5 - x^3 + 3x^2 + 4 &\equiv 0 \pmod 9, \\ 3x^5 - x^3 + 3x^2 + 4 &\equiv 0 \pmod{11}. \end{aligned}$$

Kako je rješenje prve kongruencije $x \equiv 1, 4, 7 \pmod 9$, a druge kongruencije $x \equiv 8 \pmod{11}$, to imamo za riješiti tri sistema.

$$\begin{array}{lll} x \equiv 1 \pmod 9 & x \equiv 4 \pmod 9 & x \equiv 7 \pmod 9 \\ x \equiv 8 \pmod{11} & x \equiv 8 \pmod{11} & x \equiv 8 \pmod{11} \end{array}$$

Rješenje prvog sistema je $x \equiv 19 \pmod{99}$, drugog je $x \equiv 85 \pmod{99}$ a trećeg $x \equiv 52 \pmod{99}$, pa zaključujemo da su rješenja polazne kongruencije

$$x \equiv 19, 52, 85 \pmod{99}.$$

$\diamondsuit$

Sada ćemo opisati metodu za rješavanje kongruencija $f(x) \equiv 0 \pmod{p^k}$, gdje je p prost broj a $f(x)$ polinom s cjelobrojnim koeficijentima. Kako se u rješavanju koristi i prva derivacija $f'(x)$ polinoma $f(x)$, to ćemo prvo nju definirati.

Definicija 3.3 *Neka je* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ *polinom s realnim koeficijentma. Prva* derivacija (izvod) *polinoma* $f(x)$*, u oznaci* $f'(x)$*, je polinom*

$$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2x + a_1.$$

Osim definicije prve derivacije napomenimo da x predstavlja multiplikativni inverz od a modulo p ako je x rješenje kongruencije $ax \equiv 1 \pmod{p}$.

Teorem 3.4 (Henselova lema) *Neka je* $f(x)$ *polinom s cjelobrojnim koeficijentima,* p *prost broj i* $k \geq 2$ *prirodan broj. Neka je* r *rješenje kongruencije* $f(x) \equiv 0 \pmod{p^{k-1}}$.

(*i*) *Ako je* $f'(r) \not\equiv 0 \pmod{p}$ *tada postoji jedinstven* $t \in \{0, 1, \ldots, p-1\}$*, takav da je* $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$*, dan s*

$$t \equiv -\left(f'(r)\right)^{-1} \cdot \frac{f(r)}{p^{k-1}} \pmod{p},$$

gdje $\left(f'(r)\right)^{-1}$ *označava multiplikativni inverz od* $f'(r)$ *modulo* p.

(*ii*) *Ako je* $f'(r) \equiv 0 \pmod{p}$ *i* $f(r) \equiv 0 \pmod{p^k}$ *tada vrijedi da je* $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$ *za svaki cijeli* t.

(*iii*) *Ako je* $f'(r) \equiv 0 \pmod{p}$ *i* $f(r) \not\equiv 0 \pmod{p^k}$ *tada kongruencija* $f(x) \equiv 0 \pmod{p^k}$ *nema rješenja* $x \equiv r \pmod{p^{k-1}}$.

Propozicija 3.2 *Kongruencija* $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima tačno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j.

Primjer 3.6 *Riješiti kongruenciju* $x^3 - 4x + 7 \equiv 0 \pmod{49}$.

Rješenje: Kako je $49 = 7^2$, to prvo direktnom provjerom za elemente skupa $\{0, 1, \ldots, 6\}$ rješavamo kongruenciju $x^3 - 4x + 7 \equiv 0 \pmod{7}$ i dobijamo da su njena rješenja $x \equiv 0, 2, 5 \pmod{7}$. Kako je $f'(x) = 3x^2 - 4$, to vrijedi

$$\begin{aligned} f'(0) &= -4 \equiv 3 \not\equiv 0 \pmod{7}, \\ f'(2) &= 8 \equiv 1 \not\equiv 0 \pmod{7}, \\ f'(5) &= 71 \equiv 1 \not\equiv 0 \pmod{7}. \end{aligned}$$

Vidimo da ćemo u sva tri slučaja primijeniti tvrdnju (*i*) Henselove leme.

Neka je $x \equiv 0 \pmod{7}$.

$$t \equiv -\left(f'(0)\right)^{-1} \cdot \frac{f(0)}{7} \equiv -3^{-1} \cdot \frac{7}{7} \equiv -5 \cdot 1 \equiv -5 \equiv 2 \pmod{7}$$

$$\Rightarrow \qquad x \equiv 0 + 2 \cdot 7 \equiv 14 \pmod{7^2}$$

Neka je $x \equiv 2 \pmod 7$.

$$t \equiv -\left(f'(2)\right)^{-1} \cdot \frac{f(2)}{7} \equiv -1^{-1} \cdot \frac{7}{7} \equiv -1 \cdot 1 \equiv -1 \equiv 6 \pmod 7$$

$$\Rightarrow \qquad x \equiv 2 + 6 \cdot 7 \equiv 44 \pmod{7^2}$$

Neka je $x \equiv 5 \pmod 7$.

$$t \equiv -\left(f'(5)\right)^{-1} \cdot \frac{f(5)}{7} \equiv -1^{-1} \cdot \frac{112}{7} \equiv -1 \cdot 16 \equiv -16 \equiv 5 \pmod 7$$

$$\Rightarrow \qquad x \equiv 5 + 5 \cdot 7 \equiv 40 \pmod{7^2}$$

Dobili smo da su rješenja kongruencije $x^3 - 4x + 7 \equiv 0 \pmod{49}$

$$x \equiv 14, 40, 44 \pmod{49}.$$

$\diamondsuit$

Primjer 3.7 *Riješiti kongruenciju* $2x^2 + 2x + 41 \equiv 0 \pmod{243}$.

Rješenje: Kako je $243 = 3^5$, to prvo direktnom provjerom za elemente skupa $\{0, 1, 2\}$ rješavamo kongruenciju $2x^2 + 2x + 41 \equiv 0 \pmod 3$ i dobijamo da je njeno rješenje $x \equiv 1 \pmod 3$. Vrijedi

$$f'(x) = 4x + 2 \qquad \Rightarrow \qquad f'(1) = 6 \equiv 0 \pmod 3.$$

Kako je

$$f(1) = 45 \equiv 0 \pmod{3^2},$$

to je prema tvrdnji (*ii*) Henselove leme $f(1 + 3t) \equiv 0 \pmod{3^2}$ za svaki cijeli t.

$$1 + 3 \cdot 0 = 1, \qquad 1 + 3 \cdot 1 = 4, \qquad 1 + 3 \cdot 2 = 7$$

Dobili smo da su

$$x \equiv 1, 4, 7 \pmod{3^2}$$

rješenja kongruencije

$$2x^2 + 2x + 41 \equiv 0 \pmod{3^2}.$$

Kako znamo da je $f'(x) = 4x + 2$, to vrijedi

$$\begin{aligned} f'(1) &= 6 \equiv 0 \pmod 3, \\ f'(4) &= 18 \equiv 0 \pmod 3, \\ f'(7) &= 30 \equiv 0 \pmod 3. \end{aligned}$$

Vidimo da ćemo u sva tri slučaja primijeniti tvrdnju (*ii*) ili (*iii*) Henselove leme.

Neka je $x \equiv 1 \pmod 9$. Kako je $f(1) = 45 \equiv 18 \not\equiv 0 \pmod{3^3}$, to prema tvrdnji (*iii*) Henselove leme kongruencija $2x^2 + 2x + 41 \equiv 0 \pmod{3^3}$ nema rješenja tako da je $x \equiv 1 \pmod 9$.

Neka je $x \equiv 4 \pmod 9$. Kako je $f(4) = 81 \equiv 0 \pmod{3^3}$, to je prema tvrdnji (ii) Henselove leme $f(4 + 3^2t) \equiv 0 \pmod{3^3}$ za svaki cijeli t.

$$4 + 9 \cdot 0 = 4, \qquad 4 + 9 \cdot 1 = 13, \qquad 4 + 9 \cdot 2 = 22$$

Neka je $x \equiv 7 \pmod 9$. Kako je $f(7) = 153 \equiv 18 \not\equiv 0 \pmod{3^3}$, to prema tvrdnji (iii) Henselove leme kongruencija $2x^2 + 2x + 41 \equiv 0 \pmod{3^3}$ nema rješenja tako da je $x \equiv 7 \pmod 9$.

Zaključujemo da su
$$x \equiv 4, 13, 22 \pmod{3^3}$$
rješenja kongruencije
$$2x^2 + 2x + 41 \equiv 0 \pmod{3^3}.$$

Sada ćemo posmatrati rješenja kongruencije $2x^2 + 2x + 41 \equiv 0 \pmod{3^4}$. Kako vrijedi
$$f'(4) = 18 \equiv 0 \pmod 3,$$
$$f'(13) = 54 \equiv 0 \pmod 3,$$
$$f'(22) = 90 \equiv 0 \pmod 3,$$
to vidimo da ćemo i ovdje u sva tri slučaja primijeniti tvrdnju (ii) ili (iii) Henselove leme.

Neka je $x \equiv 4 \pmod{27}$. Kako je $f(4) = 81 \equiv 0 \pmod{3^4}$, to je prema tvrdnji (ii) Henselove leme $f(4 + 3^3t) \equiv 0 \pmod{3^4}$ za svaki cijeli t.

$$4 + 27 \cdot 0 = 4, \qquad 4 + 27 \cdot 1 = 31, \qquad 4 + 27 \cdot 2 = 58$$

Neka je $x \equiv 13 \pmod{27}$. Kako je $f(13) = 405 \equiv 0 \pmod{3^4}$, to je prema tvrdnji (ii) Henselove leme $f(13 + 3^3t) \equiv 0 \pmod{3^4}$ za svaki cijeli t.

$$13 + 27 \cdot 0 = 13, \qquad 13 + 27 \cdot 1 = 40, \qquad 13 + 27 \cdot 2 = 67$$

Neka je $x \equiv 22 \pmod{27}$. Kako je $f(22) = 1053 \equiv 0 \pmod{3^4}$, to je prema tvrdnji (ii) Henselove leme $f(22 + 3^3t) \equiv 0 \pmod{3^4}$ za svaki cijeli t.

$$22 + 27 \cdot 0 = 22, \qquad 22 + 27 \cdot 1 = 49, \qquad 22 + 27 \cdot 2 = 76$$

Zaključujemo da su
$$x \equiv 4, 13, 22, 31, 40, 49, 58, 67, 76 \pmod{3^4}$$
rješenja kongruencije
$$2x^2 + 2x + 41 \equiv 0 \pmod{3^4}.$$

Još nam je preostalo naći rješenja kongruencije $2x^2 + 4x + 11 \equiv 0 \pmod{3^5}$. Kako je $f'(4) \equiv f'(13) \equiv f'(22) \equiv f'(31) \equiv f'(40) \equiv f'(49) \equiv f'(58) \equiv$

$f'(67) \equiv f'(76) \equiv 0 \pmod 3$ to ponovo vidimo da ćemo i ovdje u svih devet slučajeva primijeniti tvrdnju (*ii*) ili (*iii*) Henselove leme.

Kako za $x = 4, 13, 22, 31, 40, 49, 58, 67, 76$ imamo da je $f(x) = 81, 405, 1053, 2025, 3321, 4941, 6885, 9153, 11745$, redom, što je redom kongruentno s $81, 162, 81, 81, 162, 81, 81, 162, 81$, modulo 3^5, to prema tvrdnji (*iii*) Henselove leme zaključujemo da kongruencija $2x^2 + 2x + 41 \equiv 0 \pmod{3^5}$ nema rješenja.

$\diamondsuit$

U prethodnom primjeru smo vidjeli da iz pojedinog rješenja kongruencije modulo p^k, gdje je p prost broj, možemo dobiti rješenja kongruencija kod kojih je modul veća potencija od p, ali da to ne mora nužno voditi do rješenja kongruencije s proizvoljnom potencijom broja p.

Teorem 3.5 *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima, p prost i k prirodan broj. Neka je $f(a) \equiv 0 \pmod{p^j}$, $p^k \| f'(a)$ i $j \geq 2k + 1$. Ako je $b \equiv a \pmod{p^{j-k}}$ tada je $f(b) \equiv f(a) \pmod{p^j}$ i vrijedi $p^k \| f'(b)$, te postoji jedinstven $t \in \{0, 1, \dots, p-1\}$ takav da je $f(a + tp^{j-k}) \equiv 0 \pmod{p^{j+1}}$.*

Napomenimo da oznaka oznaka $p^k \| f$ znači da $p^k | f$, ali $p^{k+1} \nmid f$.

Vidimo da kolekcija od p^k rješenja modulo p^j daje p^k rješenja modulo p^{j+1} dok potencija od p dijeli f'. Kako se prema teoremu a mijenja s $a + tp^{j-k}$ i modul p^j modulom p^{j+1}, dok k ostaje nepromijenjeno, to se dobijanje novih rješenja može nastaviti neograničeno.

Primjer 3.8 *Riješiti kongruenciju $x^2 + x + 223 \equiv 0 \pmod{3^j}$.*

Rješenje: Rješavajući danu kongruenciju dobijamo da je $x \equiv 1 \pmod 3$ jedino rješenje dane kongruencije modulo 3, da su $x \equiv 1, 4, 7 \pmod{3^2}$ rješenja dane kongruencije modulo 3^2, da su $x \equiv 4, 13, 22 \pmod{3^3}$ rješenja modulo 3^3, te da su $x \equiv 4, 13, 22, 31, 40, 49, 58, 67, 76 \pmod{3^4}$ rješenja kongruencije $x^2 + x + 223 \equiv 0 \pmod{3^4}$. Vidimo da posljednja kongruencija ima devet rješenja.

Kako je $f(4) \equiv 0 \pmod{3^5}$ i $3^2 \| f'(4)$, to je 4 modulo 3^5 jedno od 9 rješenja oblika $4 + 3^{5-2}t = 4 + 27t$ modulo 3^5. Postoji tačno jedan $t \in \{0, 1, 2\}$, preciznije $t = 2$, takav da je $f(4 + 27t) \equiv 0 \pmod{3^6}$. To nam daje 9 rješenja oblika $4 + 81t$ modulo 3^6.

Slično imamo da je $f(22) \equiv 0 \pmod{3^5}$ i $3^2 \| f'(22)$, pa je 22 modulo 3^5 jedno od 9 rješenja oblika $22 + 3^{5-2}t = 22 + 27t$ modulo 3^5. Postoji tačno jedan $t \in \{0, 1, 2\}$, preciznije $t = 0$, takav da je $f(22 + 27t) \equiv 0 \pmod{3^6}$. To nam daje 9 rješenja oblika $22 + 81t$ modulo 3^6.

S druge strane je $f'(13) \equiv 0 \pmod{27}$ i $f(13 + 27t) \equiv f(13) \pmod{3^6}$. Kako $3^4 \| f(13)$ to zaključujemo da nijedno od tri rješenja oblika $13 + 27t$ modulo 81 ne generira rješenje modulo 3^5.

Na kraju zaključujemo da za svaki $j \geq 5$ postoji tačno 18 rješenja modulo 3^j, od kojih 12 ne generiraju rješenja modulo 3^{j+1}, dok svako od preostalih 6 generira po 3 rješenja modulo 3^{j+1}.

$\diamondsuit$

Napomenimo da se ponekad polinomske kongruencije mogu rješavati uvođenjem odgovarajuće supstitucije i svođenjem dane polinomske kongruencije na jednostavniju kongruenciju, što je prikazano u sljedećim primjerima.

Primjer 3.9 *Riješiti kongruenciju* $x^2 + x + 7 \equiv 0 \pmod{27}$.

Rješenje: Zadatak ćemo riješiti svođenjem izraza na lijevoj strani na potpun kvadrat. Kako je $\mathrm{nzd}(4, 27) = 1$ to je polazna kongruencija ekvivalentna kongruenciji $4(x^2 + x + 7) \equiv 0 \pmod{27}$, tj. kongruenciji $4x^2 + 4x + 28 \equiv 0 \pmod{27}$. Kako je

$$4x^2 + 4x + 28 = (2x + 1)^2 - 1^2 + 28 = (2x + 1)^2 + 27$$

to je kongruencija $4x^2 + 4x + 28 \equiv 0 \pmod{27}$, pa samim tim i polazna, ekvivalentna kongruenciji $(2x+1)^2 + 27 \equiv 0 \pmod{27}$, što je ekvivalentno kongruenciji

$$(2x + 1)^2 \equiv 0 \pmod{27}.$$

Uvedemo li supstituciju $2x + 1 = t$, imamo za riješiti kongruenciju

$$t^2 \equiv 0 \pmod{27}.$$

Iskoristimo li Teorem 2.1 dobijamo da su njena rješenja $t = 0, 9, 18$. Vratimo li nazad supstituciju $2x + 1 \equiv t \pmod{27}$, možemo odrediti rješenja polazne kongruencije.

$$\begin{aligned} 2x + 1 &\equiv 0 \pmod{27} \\ 2x &\equiv -1 \pmod{27} \\ 2x &\equiv 26 \pmod{27} \\ x &\equiv 13 \pmod{27} \end{aligned}$$

$$\begin{aligned} 2x + 1 &\equiv 9 \pmod{27} \\ 2x &\equiv 8 \pmod{27} \\ x &\equiv 4 \pmod{27} \end{aligned}$$

$$\begin{aligned} 2x + 1 &\equiv 18 \pmod{27} \\ 2x &\equiv 17 \pmod{27} \\ x &\equiv 17 \cdot 2^{-1} \pmod{27} \\ x &\equiv 17 \cdot 14 \pmod{27} \\ x &\equiv 22 \pmod{27} \end{aligned}$$

Rješenja kongruencije $x^2 + x + 7 \equiv 0 \pmod{27}$ su

$$x \equiv 4, 13, 22 \pmod{27}.$$

$\diamondsuit$

Primjer 3.10 *Riješiti kongruenciju* $8x^3+4x^2-10x-5 \equiv 0 \pmod{16}$ *svođenjem na puni kub.*

Rješenje: Kako je $4 \equiv 36$, $-10 \equiv 54$ i $-5 \equiv 27 \pmod{16}$, to je polazna kongruencija ekvivalentna kongruenciji

$$8x^3 + 36x^2 + 54x + 27 = (2x+3)^3 \equiv 0 \pmod{16}.$$

Uvedemo li supstituciju $2x+3 = t$, dobijamo kongruenciju $t^3 \equiv 0 \pmod{16}$ čija su rješenja $t \equiv 0, 4, 8, 12 \pmod{16}$. Vratimo li supstituciju dobijamo kongruencije $2x + 3 \equiv 0, 4, 8, 12 \pmod{16}$, a one su redom ekvivalentne kongruencijama $2x \equiv -3, 1, 5, 9 \pmod{16}$. Kako je $\mathrm{nzd}(2, 16) = 2$ a kako $2 \nmid -3, 1, 5, 9$, to posljednje kongruencije nemaju rješenja. Zaključujemo da polazna kongruencija nema rješenja.

$\diamondsuit$

Literatura

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

[2] B. Ibrahimpašić: *Kongruencije oblika* $x^n \equiv 0 \pmod{m}$, OML, 15/1(2015), to appear

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

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

[5] I. Niven, H. S. Zuckerman, H. L. Montgomery: *An Introduction to the Theory of Numbers*, John Wiley & Sons Inc., New York, 1991.

Primljeno u redakciju 08.12.2014; Revidirana verzija 26.01.2015;
dostupno online 03.02.2015.