1 Ojlerova funkcija

4. **a)** Da li 42 deli $n^7 - n$, za bilo koji prirodan broj n?

$42 = 2 \cdot 3 \cdot 7$. Ako brojevi 2, 3 ili 7 dele n, onda će deliti traženi izraz. Pretpotstavimo da n nije deljivo sa 2, 3 ili 7.

Pošto je n neparno, onda je to i n^7, pa je $n^7 - n$ paran broj. Zatim, po Maloj Fermaovoj teoremi, kako je $(3, n) = (7, n)$ (3 i 7 su prosti brojevi), to je $n^2 \equiv 1 \pmod 3$, pa je $n^7 = (n^2)^3 \cdot n \equiv n \pmod 3$, tj. 3 deli $n^7 - n$. Slično, $n^6 \equiv 1 \pmod 7$, pa je $n^7 \equiv n \pmod 7$, odakle 7 deli $n^7 - n$.

4. **b)** Da li 2730 deli $n^{13} - n$, za bilo koji prirodan broj n?

Ovo ide slično prethodnom zadatku: $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. Po Maloj Fermaovoj teoremi dobijamo:

- $n^2 \equiv 1 \pmod 3$
- $n^4 \equiv 1 \pmod 5$
- $n^6 \equiv 1 \pmod 7$
- $n^{12} \equiv 1 \pmod{13}$

Pošto je $n^{13} = (n^2)^6 \cdot n = (n^4)^3 \cdot n = (n^6)^2 \cdot n = n^{12} \cdot n$, to 2730 deli $n^{13} - n$.

5. Neka su p i q različiti prosti brojevi. Da li važi $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$?

Ova kongruencija važi ako i samo ako pq deli $p^{q-1} + q^{p-1} - 1$. Pošto su p i q različiti prosti brojevi, dovoljno je da svaki pojedinačno proverimo. Po

Maloj Fermaovoj teoremi, važi $p^{q-1}-1$ deljivo sa q, pa je izraz deljiv sa q. Slično, $q^{p-1}-1$ je deljivo sa p, pa je izraz deljiv i sa p.

6. Naći ako postoji prost broj p takav da je $5^{p^2}+1=(5^p)^p+1$ deljivo sa p^2.

Svakako, ovo ne važi za $p=5$. Dakle, $(p,5)=1$ pa po Maloj Fermaovoj teoremi važi $5^p \equiv p \pmod{p}$. Sada je $(5^p)^p \equiv 5^p \equiv 5 \pmod{p}$, i imamo da je $5^{p^2}+1 \equiv 6 \pmod{p}$. Pošto p deli $5^{p^2}+1$, onda p mora da deli i 6, pa p može biti ili 2 ili 3. Pošto $4=2^2$ ne deli 5^4+1, a $9=3^2$ deli 5^9+1 to je $p=3$.

7. **a)** Odrediti ostatak pri deljenju 2^{30} sa 13.

Po Maloj Fermaovoj teoremi, $2^12 \equiv 1 \pmod{13}$. Takođe, $2^6=64 \equiv 12 \equiv -1 \pmod{13}$, pa je $2^{30}=(2^{12})^2 \cdot 2^6 \equiv -1 \pmod{13}$.

7. **b)** Odrediti poslednju cifru 7^{7^7}.

Tražimo ostatak pri deljenju ovog broja sa 10 (to će upravo biti poslednja cifra). Po Ojlerovoj teoremi, kako je $(7,10)=1$ i $\varphi(10)=4$, to je $7^4 \equiv 1 \pmod{10}$. Dakle, interesuje nas ostatak pri deljenju 7^7 sa 4. Sada, $(7,4)=1$ i $\varphi(4)=2$, pa je $7^2 \equiv 1 \pmod{4}$, i $7 \equiv 3 \pmod{4}$. Dakle, $7^7 \equiv 3 \pmod{4}$, pa je $7^{7^7} \equiv 7^3 \pmod{10}$, a odavde se vidi računom da će poslednja cifra biti 3.

7. **c)** Odrediti poslednje dve cifre 9^{9^9}.

Kako je $\varphi(100)=100(1-1/2)(1-1/5)=10$ i $(9,100)=1$, to je $9^{10} \equiv 1 \pmod{100}$. Sada tražimo ostatak pri deljenju 9^9 sa 10. Isto, kako je $(9,10)=$

1 i $\varphi(10) = 4$, to je $9^4 \equiv 1 \pmod{10}$, odakle je $9^9 = (9^4)^2 \cdot 9 \equiv 9 \pmod{10}$. Na kraju, $9^{9^9} \equiv 9^9 \pmod{100}$, a ovo se računom proveri da je kongruentno sa 89.

9. Ispitati da li za sve proste brojeve p, i za sve cele brojeve a koji nisu deljivi sa p važi da je $a^p + (p-1)!a$ deljivo sa p.

Po Maloj Fermaovoj teoremi, $a^p \equiv a \pmod{p}$, a po Vilsonovoj teoremi $(p-1)!a \equiv -a \pmod{p}$, pa je $a^p + (p-1)!a \equiv 0 \pmod{p}$.

2 Kvadratna kongruencija

2. Da li sledeće kongruencije imaju rešenje?

1. $x^2 \equiv 68 \pmod{113}$,
2. $x^2 \equiv 310 \pmod{521}$,
3. $x^2 + 174 \equiv 0 \pmod{619}$.

Ovde samo treba da izračunamo odgovarajuće Ležandrove simbole.

Prvi: $\left(\frac{68}{113}\right)$. Imamo da je $68 = 4 \cdot 17$, pa je $\left(\frac{68}{113}\right) = \left(\frac{4}{113}\right) \cdot \left(\frac{17}{113}\right) = \left(\frac{17}{113}\right)$. Po Gausovom zakonu reciprociteta, $\left(\frac{17}{113}\right)\left(\frac{113}{17}\right) = (-1)^{\frac{17-1}{2}\frac{113-1}{2}} = 1$, pa je $\left(\frac{17}{113}\right) = \left(\frac{113}{17}\right) = \left(\frac{11}{17}\right)$. Gaus: $\left(\frac{11}{17}\right)\left(\frac{17}{11}\right) = 1$, pa je $\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. Sada je $\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1$, a po Gausu, $\left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = (-1)^{\frac{3-1}{2}\frac{11-1}{2}} = -1$, pa je $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$. Prem tome, $\left(\frac{68}{113}\right) = -1$, pa 68 nije kvadrat modulo 113.

Drugi: $\left(\frac{310}{521}\right)$. Imamo da je $310 = 2 \cdot 10 \cdot 31$, pa je $\left(\frac{310}{521}\right) = \left(\frac{2}{521}\right)\left(\frac{5}{521}\right)\left(\frac{31}{521}\right)$. Prvi simbol je jednak $\left(\frac{2}{521}\right) = (-1)^{\frac{521^2-1}{8}} = (-1)^{\frac{520 \cdot 522}{8}} = 1$. Drugi simbol, po

Gausu: $\left(\frac{5}{521}\right)\left(\frac{521}{5}\right) = (-1)^{\frac{521-1}{2}\frac{5-1}{2}} = 1$, pa je $\left(\frac{310}{521}\right)\left(\frac{5}{521}\right) = \left(\frac{521}{5}\right) = \left(\frac{1}{5}\right) = 1$. Na kraju, treći simbol je $\left(\frac{31}{521}\right)\left(\frac{521}{31}\right) = 1$, odakle je $\left(\frac{31}{521}\right) = \left(\frac{521}{31}\right) = \left(\frac{25}{521}\right) = 1$. Dakle, $\left(\frac{310}{521}\right) = 1$, tj. 310 je kvadrat modulo 521.

Treći: $\left(\frac{-174}{619}\right)$. Imamo da je $\left(\frac{-1}{619}\right) = (-1)^{\frac{619-1}{2}} = -1$, pa je $\left(\frac{-174}{619}\right) = -\left(\frac{174}{619}\right)$. Kako je $174 = 2 \cdot 3 \cdot 29$, to je $\left(\frac{174}{619}\right) = \left(\frac{2}{619}\right)\left(\frac{3}{619}\right)\left(\frac{29}{619}\right)$. Prvi simbol je $\left(\frac{2}{619}\right) = (-1)^{\frac{618\cdot 620}{8}} = -1$. Drugi simbol, po Gausu: $\left(\frac{3}{619}\right)\left(\frac{619}{3}\right) = (-1)^{\frac{3-1}{2}\frac{619-1}{2}} = -1$, pa je $\left(\frac{3}{619}\right) = -\left(\frac{619}{3}\right) = -\left(\frac{1}{3}\right) = -1$. Treći simbol je $\left(\frac{29}{619}\right)\left(\frac{619}{29}\right) = (-1)^{\frac{29-1}{2}\frac{619-1}{2}} = 1$, pa je $\left(\frac{29}{619}\right) = \left(\frac{619}{29}\right) = \left(\frac{10}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{5}{29}\right)$. Imamo da je $\left(\frac{2}{29}\right) = (-1)^{\frac{28\cdot 30}{8}} = -1$. Po Gausu, $\left(\frac{5}{29}\right)\left(\frac{29}{5}\right) = (-1)^{\frac{5-1}{2}\frac{29-1}{2}} = 1$, pa je $\left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1$. Kada pomnožimo ova tri simbola, dobijamo da je $\left(\frac{174}{619}\right) = (-1)\cdot(-1)\cdot(-1) = -1$, odakle je $\left(\frac{-174}{619}\right) = 1$. Dakle, -174 jeste kvadrat modulo 619

2. **b)** Ima li $9x^2 + 11x - 2 \equiv 0 \pmod{41}$ rešenja?

U ovom slučaju, diskriminanta je $D = 11^2 - 4\cdot 9\cdot(-2) = 121 + 72 = 193 \equiv 29 \pmod{41}$. Dakle, gledamo da li je 29 kvadrat modulo 29, tj. simbol $\left(\frac{29}{41}\right)$. Po Gausu, imamo da je $\left(\frac{29}{41}\right)\left(\frac{41}{29}\right) = (-1)^{\frac{29-1}{2}\frac{41-1}{2}} = 1$, pa je $\left(\frac{29}{41}\right) = \left(\frac{41}{29}\right) = \left(\frac{12}{29}\right) = \left(\frac{4}{29}\right)\left(\frac{3}{29}\right) = \left(\frac{3}{29}\right)$. Opet, po Gausu, $\left(\frac{3}{29}\right)\left(\frac{29}{3}\right) = (-1)^{\frac{3-1}{2}\frac{29-1}{2}} = 1$, pa je $\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1$. Dakle, ova jednačina nema rešenja modulo 41.

4. Neka su a i b celi brojevi, i p prost broj koji ne deli a. Dokazati da je

$$\sum_{k=0}^{p-1} \left(\frac{ak+b}{p}\right) = 0.$$

Pošto p ne deli a, kada k prolazi kroz skup $\{0, 1, \ldots, p-1\}$, to $ak + b$ prolazi kroz skup svih ostataka modulo p. Znamo da je broj kvadratnih ostataka jednak broju kvadratnih neostataka, pa ova suma ima isti broj 1 i -1 zbog čega ona mora biti jednaka nuli.

3 Kvadratna raširenja

3. Odrediti najveći zajednički delilac brojeva $13+2i$ i $4+5i$.

Kako je $N(13+2i) = 173 > 41 = N(4+5i)$, delimo $13+2i$ sa $4+5i$.

$$\frac{13+2i}{4+5i} = \frac{62-57i}{41}.$$

Najbliži Gausov ceo je $1-i$, pa je $13+2i = (4+5i)(1-i)+(4+i)$. Sada:

$$\frac{4+5i}{4+i} = \frac{21+16i}{17}.$$

Najbliži Gausov ceo je $1+i$, pa je $4+5i = (4+i)(1+i)+1$. Pošto je $N(1) = 1$, ovde stajemo (sledeći ostatak bi bio strogo manje norme, a jedini Gausov ceo sa normom manjom od 1 je 0), i zaključujemo da je $(13+2i, 4+5i) = 1$, tj. ova dva broja su uzajamno prosta.

4. Odrediti najveći zajednički delilac brojeva $12+4i$ i $9-2i$.

Pošto je $N(12+4i) = 160 > 85 = N(9-2i)$, delimo $12+4i$ sa $9-2i$.

$$\frac{12+4i}{9-2i} = \frac{100+60}{85}.$$

Najbliži Gausov ceo je $1+i$, pa je $12+4i = (9-2i)(1+i)+(1-3i)$. Sada:

$$\frac{9-2i}{1-3i} = \frac{15+25i}{10}.$$

Ovde imamo četiri Gausova cela koja su podjednako udaljena od razlomka, pa možemo uzeti bilo koji, npr. $1+2i$. To nam daje $9-2i = (1-3i)(1+2i)+(2-i)$. Sada:

$$\frac{1-3i}{2-i} = \frac{5-5i}{5} = 1-i.$$

Kako je $1-3i$ deljivo sa $2-i$, ovde stajemo. Poslednji nenula ostatak u ovom nizu je $2-i$, i zaključujemo da je $(12+4i, 9-2i) = 2-i$. Pošto je $N(2-i) = 5 > 1$, vidimo da ova dva broja nisu uzajamno prosta.

3. Odrediti faktorizaciju $12+5i \in \mathbb{Z}[i]$ na proste.

Norma ovog elementa je $N(12+5i) = 169 = 13^2$. Ako ovaj broj nije prost, jedini prosti faktori koje ovaj broj može da ima su oni norme 13: $3+2i$ i $3-2i$. Samo treba da proverima tri njihova moguća proizvoda:

- $(3+2i)(3-2i) = 13$;
- $(3+2i)^2 = 5+12i$;
- $(3-2i)^2 = 5-12i = -i(12+5i)$.

Dakle, $12+5i = i(3-2i)^2$.