Poglavlje 2

Kongruencije

Mali Fermatov, Eulerov i Wilsonov teorem

Teorem (**Mali Fermatov teorem**): *Neka je p prost broj i $a \in \mathbb{Z}$. Tada vrijedi $a^p \equiv a \pmod{p}$. Ako $p \nmid a$, tada vrijedi i $a^{p-1} \equiv 1 \pmod{p}$.*

Teorem (**Eulerov teorem**): *Neka su a, n relativno prosti prirodni brojevi. Ako je $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, definirajmo broj $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1)$. Tada vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Iz definicije funkcije φ nije teško pokazati da za sve $n \geq 3$ vrijedi $2 \mid \varphi(n)$ te da je $\varphi(n) = 1$ samo za $n = 1, 2$.

Napomena: Obrat malog Fermatovog teorema ne vrijedi. Štoviše, definiramo da je složen broj $x \in \mathbb{N}$ Fermat pseudoprost ako za svaki $a \in \mathbb{Z}$ relativno prost s x vrijedi $a^{x-1} \equiv 1 \pmod{x}$. Primjeri Fermat pseudoprostih brojeva su $341, 561, 645$. Provjerite to!

Teorem (**Wilson**): *Ako je p prost broj, tada je $(p-1)! \equiv -1 \pmod{p}$.*

Zadatak 2.9. Odredite sve $n \in \mathbb{N}$ za koje je $\varphi(n) = 568$.

Rješenje. Neka je $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $p_1 > \dots > p_k$. Kako je $568 = 2^3 \cdot 71$, iz definicije funkcije $\varphi(n)$ nije teško zaključiti da n mora imati prost djelitelj veći ili jednak 71 pa je $p_1 \geq 71$. Također je $p_1 - 1 \mid \varphi(n) = 568$. Sada imamo nekoliko slučajeva.

- $p_1 - 1 = 568 \implies p_1 = 569, \alpha_1 = 1$. Sada je $\varphi(\frac{n}{569}) = 1$. Jedini brojevi $m \in \mathbb{N}$ za koje je $\varphi(m) = 1$ su $m = 1, 2$ pa su ovdje sva rješenja $n = 569, 1138$.
- $p_1 - 1 = 284$. Ovdje nema rješenja jer 285 nije prost.
- $p_1 - 1 = 142$. Ovdje nema rješenja jer 143 nije prost.
- $p_1 - 1 \mid 71$. Ovdje nema rješenja jer p_1 mora biti neparan.

Dakle, sva rješenja su $569, 1138$.

Zadatak 2.10. Odredite zadnje 3 znamenke broja $6^{666^{666}}$.

Rješenje. Zanima nas koliki ostatak broj $6^{666^{666}}$ daje pri dijeljenju s 8 i 125. Lako vidimo da je djeljiv s 8 pa ostaje odrediti ostatak mod 125. Kako je $\varphi(125) = 100$, Eulerov teorem nam kaže da trebamo odrediti ostatak 666^{666} mod 100 što će nam omogućiti da izračunamo $6^{666^{666}}$ mod 125.

Znamo da je $666^{666} \equiv 0 \pmod 4$, a $\varphi(25) = 20$ pa po Eulerovom teoremu vrijedi

$$666^{666} = 666^{20 \cdot 33 + 6} \equiv 666^6 \equiv 66^6 \equiv 16 \pmod{25}.$$

Sustav

$$\begin{aligned} x &\equiv 0 \pmod 4 \\ x &\equiv 16 \pmod{25} \end{aligned}$$

po CRT-u ima rješenje $x = 16$ pa je $666^{666} \equiv 16 \pmod{100}$ i $6^{666^{666}} \equiv 6^{16} \equiv 81 \pmod{125}$. Sustav

$$\begin{aligned} x &\equiv 0 \pmod 8 \\ x &\equiv 81 \pmod{125} \end{aligned}$$

po CRT-u ima rješenje $x = 456$ pa su to tražene zadnje 3 znamenke.

Zadatak 2.11. Dokažite da za sve proste brojeve $p \neq q$ vrijedi $pq \mid p^{q-1} + q^{p-1} - 1$.

Rješenje. Po Malom Fermatovom teoremu je

$$p^{q-1} + q^{p-1} \equiv 0 + 1 = 1 \pmod p,$$

$$p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \pmod q.$$

Kako je $p \neq q$, vrijedi $(p, q) = 1$ pa je izraz $p^{q-1} + q^{p-1} - 1$ djeljiv s pq.

Zadatak 2.12. Dokažite da za sve proste brojeve $p \neq q$ i sve $a \in \mathbb{Z}$ vrijedi $a^{pq-p-q+2} \equiv a \pmod{pq}$.

Rješenje. Po Malom Fermatovom teoremu je

$$a^{pq-p-q+2} - a = a^{(p-1)(q-1)+1} - a \equiv a - a = 0 \pmod p$$

i analogno za q.

Zadatak 2.13. Odredite sve proste brojeve p za koje $p \mid 4^p + 5^p$.

Rješenje. Po Malom Fermatovom teoremu je $4^p + 5^p \equiv 4 + 5 = 9 \pmod p$. Zato je jedino rješenje $p = 3$.

Zadatak 2.14. Neka je p prost broj i $a \in \mathbb{Z}$ takav da $p \mid a^p - 1$. Dokažite da $p^2 \mid a^p - 1$.

Rješenje. Vrijedi $a^p \equiv a \pmod p$. Stoga je $a = pk + 1$ pa je

$$a^p - 1 = (pk + 1)^p - 1 = (pk)^p + \ldots + pk \cdot p + 1 - 1 \equiv 0 \pmod{p^2}.$$

Zadatak 2.15. Dokažite da za svaki prost broj p i svaki $c \in \mathbb{Z}$ postoji $x \in \mathbb{Z}$ takav da je $x^x \equiv c \pmod{p}$.

Rješenje. Očito želimo namjestiti $x \mod p$, a kako se x pojavljuje i u eksponentu, nameće se i potreba da namjestimo $x \mod p-1$. Ako je $x \equiv 1 \pmod{p-1}$, tada je

$$x^x \equiv x \pmod{p}$$

pa je dovoljno uzeti $x \equiv c \pmod{p}$. Sustav

$$\begin{aligned} x &\equiv 1 \pmod{p-1} \\ x &\equiv c \pmod{p} \end{aligned}$$

ima rješenje u $\mathbb{Z}$ po CRT-u.

Zadatak 2.16. Dokažite da za svaki prost broj p postoji beskonačno mnogo $n \in \mathbb{N}$ takvih da $p \mid 2^n - n$.

Rješenje. Kako i u prošlom zadatku, logično je namjestiti $n \mod p, p-1$. Ako je $p = 2$, možemo uzeti bilo koji paran n. Neka je sada $p \geq 3$.

Možemo npr. uzeti $n \equiv 0 \pmod{p-1}$. Tada je $2^n \equiv 1 \pmod{p}$ pa je dovoljno uzeti $n \equiv 1 \pmod{p}$. Sustav

$$\begin{aligned} n &\equiv 0 \pmod{p-1} \\ n &\equiv 1 \pmod{p} \end{aligned}$$

ima beskonačno mnogo rješenja u $\mathbb{Z}$ po CRT-u.

Zadatak 2.17. Odredite sve proste brojeve p za koje $p^2 \mid 5^{p^2} + 1$.

Rješenje. Po Malom Fermatovom teoremu je $5^{p^2} + 1 \equiv 5 + 1 \equiv 6 \pmod{p}$. Stoga su jedini kandidati $p = 2, 3$. Za $p = 2$ je $5^4 + 1 \equiv 2 \pmod{4}$, a za $p = 3$ je $5^9 + 1 \equiv 5^3 + 1 = 126 \equiv 0 \pmod{9}$. Stoga je jedino rješenje $p = 3$.

Zadatak 2.18. Ovisno o vrijednosti prirodnog broja n odredite $(n! + 1, (n+1)!)$.

Rješenje. Vidimo da je $(n! + 1, (n+1)!) = (n! + 1, n! \cdot (n+1)) = (n! + 1, n + 1)$. Ako je $n + 1$ prost, tada je $n! + 1$ djeljivo s $n + 1$ po Wilsonovom teoremu. Ako je $n + 1$ složen, tada je $n + 1 = ab$ za neke $2 \leq a, b \leq n$ i $n!$ je djeljivo s a i b. Stoga je

$$(n! + 1, n + 1) = \begin{cases} n + 1, & n + 1 \text{ prost}, \\ 1, & n + 1 \text{ složen}. \end{cases}$$

Zadatak 2.19. Dokažite da je za svaki $n \in \mathbb{N}$ niz $2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots$ od nekog elementa nadalje periodičan mod n.

Rješenje. Promatramo niz $a_1 = 2, a_{n+1} = 2^{a_n}$. Primijetimo da je niz oblika

$$a_1, 2^{a_1}, 2^{a_2}, 2^{a_3}, \ldots$$

pa je po Eulerovom teoremu dovoljno dokazati da je niz eksponenata periodičan mod $\varphi(n)$.

Preciznije, za dokaz tvrdnje koristimo jaku indukciju. Baza $n = 1$ je trivijalna jer su svi prirodni brojevi djeljivi s 1. Neka je n sad neki prirodan broj i neka je $n = 2^a b$ t.d. $2 \nmid b$. Po pretpostavci indukcije niz je periodičan mod $\varphi(b)$ od nekog mjesta nadalje. Stoga je niz

$$2^{a_1}, 2^{a_2}, 2^{a_3}, \ldots$$

periodičan mod b, a svi osim konačno elemenata niza su djeljivi s 2^a. Slijedi da je niz od nekog elementa nadalje periodičan mod n po CRT-u.

Zadatak 2.20 (Međunarodna matematička olimpijada 1975 *)**.** Neka je $A = 4444^{4444}$, B zbroj znamenki broja A, a C zbroj znamenki broja B. Odredite zbroj znamenki broja C.

Rješenje. Neka je $s(n)$ zbroj znamenki prirodnog broja n. Znamo da je $n \equiv s(n) \pmod 9$. Još preostaje ograničiti brojeve B, C. Kako je

$$A = 4444^{4444} < 10000^{4444} = 10^{4 \cdot 4444}.$$

mora vrijediti $B = s(A) < 9 \cdot 4 \cdot 4444 < 10^6$. Stoga je i $C = s(B) < 9 \cdot 6 = 54 < 100$ pa je $s(C) < 9 \cdot 2 = 18$.

Također, vrijedi

$$A = 4444^{4444} \equiv 7^{4444} \equiv 7^4 = 2401 \equiv 7 \pmod 9.$$

Zato je $s(C) \equiv 7 \pmod 9$ pa zaključujemo $s(C) \in \{7, 16\}$. Međutim, $s(C) < 18$ pa mora vrijediti $s(C) = 7$.

Zadatak 2.21 (Međunarodna matematička olimpijada 2005 *)**.** Odredite sve prirodne brojeve koji su relativno prosti sa svim elementima niza $a_n = 2^n + 3^n + 6^n - 1, n \geq 1$.

Rješenje. Dokažimo da svaki prost broj p dijeli neki član niza (a_n). Kako je $a_2 = 48$, možemo pretpostaviti da je $p \geq 5$. Činjenica da je n u eksponentu nas navodi na Mali Fermatov teorem. Primijetimo da za svaki a relativno prost s p vrijedi

$$a^{p-1} \equiv 1 \pmod p \implies a^{p-2} \equiv a^{-1} \pmod p.$$

Ovdje je a^{-1} multiplikativni inverz broja a mod p. Stoga je

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 2^{-1} + 3^{-1} + 6^{-1} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0 \pmod p.$$

Čitatelju za vježbu ostavljamo da dokaže da se s multiplikativnim inverzima može raditi kao s racionalnim brojevima.

Dakle, jedini prirodan broj relativno prost sa svim brojevima a_n je 1.