

# 1.mājasdarba atrisinājumi

**1.uzdevums** Zināms, ka  $n$  ir mazākais naturāls skaitlis ar īpašību, ka  $149^n - 2^n$  dalās ar  $3^3 \cdot 5^5 \cdot 7^7$ .  
Atrast skaitļa  $n$  pozitīvo dalītāju skaitu.

**Atrisinājums.** Vispirms ievērosim, ka  $149 - 2 = 147 = 3 \cdot 7^2$ . Izmantojot LTE lemmu un to, ka  $3 \mid 147$ , bet  $3 \nmid 149$  un  $3 \nmid 2$ , iegūstam

$$\nu_3(149^n - 2^n) = \nu_3(147) + \nu_3(n) = \nu_3(n) + 1.$$

Līdz ar to,  $3^3 \mid 149^n - 2^n$  tad un tikai tad, ja  $3^2 \mid n$ . Līdzīgi, tā kā  $7 \mid 147$ , bet  $7 \nmid 149$  un  $7 \nmid 2$ , iegūstam

$$\nu_7(149^n - 2^n) = \nu_7(147) + \nu_7(n) = \nu_7(n) + 2.$$

Līdz ar to,  $7^7 \mid 149^n - 2^n$  tad un tikai tad, ja  $7^5 \mid n$ .

Ievērojam, ka atlikumi no  $149^n \pmod{5}$  veido ciklu 4, 1, 4, 1, bet atlikumi no  $2^n \pmod{5}$  veido ciklu 2, 4, 3, 1. No tā izriet, ka atlikumi no  $149^n - 2^n \pmod{5}$  veido ciklu 2, 2, 1, 0, un līdz ar to  $n \mid 149^n - 2^n$  tad un tikai tad, ja  $n = 4k$  kādam naturālam  $k$ . Tālāk atkal pielietojam LTE, iegūstam

$$\nu_5((149^4)^k - (2^4)^k) = \nu_5(149^4 - 2^4) + \nu_5(k).$$

Tā kā  $149^4 - 2^4 \equiv (-1)^4 - 16 \equiv 15 \pmod{25}$ , secinām, ka  $\nu_5(149^4 - 2^4) = 1$ . Tādējādi

$$\nu_5((149^4)^k - (2^4)^k) = 1 + \nu_5(k).$$

Secinām, ka  $5^5 \mid 149^n - 2^n$  tad un tikai tad, ja  $5^4 \mid k$  jeb  $4 \cdot 5^4 \mid n$ .

Apvienojot šos trīs novērtējumus, secinām, ka  $n = 2^2 \cdot 3^2 \cdot 5^4 \cdot 7^5$ , kam ir  $(2+1)(2+1)(4+1)(5+1) = 270$  pozitīvi dalītāji.

**2.uzdevums** Pierādīt, ka katram naturālam skaitlim  $k > 1$  eksistē bezgalīgi daudz naturālo skaitļu  $n$  ar īpašību, ka

$$n | 1^n + 2^n + 3^n + \dots + k^n$$

**Atrisinājums.** Sakumā apskatīsim gadījumu, kad  $k$  ir nepāra. Tādā gadījumā eksistē nepāra pirmskaitlis  $p$ , kas dala  $k$ . Pierādīsim, ka visi skaitļi formā  $n = p^m$ , kur  $m$  ir naturāls skaitlis, apmierina uzdevuma nosacījumus. Tā kā  $k$  ir nepāra, tad

$$\begin{aligned} 1^n + 2^n + 3^n + \dots + k^n &= (1^n + (k-1)^n) + (2^n + (k-2)^n) + \dots + \left(\left(\frac{k-1}{2}\right)^n + \left(\frac{k+1}{2}\right)^n\right) + k^n = \\ &= k^n + \sum_{i=1}^{\frac{k+1}{2}} (i^n + (k-i)^n) \end{aligned}$$

No LTE lemmas izriet, ka

$$\nu_p(i^n + (k-i)^n) = \nu_p(k) + \nu_p(n) \geq m + 1,$$

no kā var secināt, ka  $n = p^m | i^n + (k-i)^n$  katram  $i = 1, 2, \dots, \frac{k+1}{2}$ . Ievērojam arī, ka  $\nu_p(k^n) = n\nu_p(k) \geq n = p^m \geq m$ , kas nozīmē, ka  $n | k^n$ . Tādējādi esam pierādījuši, ka

$$n | k^n + \sum_{i=1}^{\frac{k+1}{2}} (i^n + (k-i)^n) = 1^n + 2^n + 3^n + \dots + k^n,$$

kas bija jāpierāda. Tagad izskatīsim gadījumu, kad  $k$  ir pāra. Ievērojam, ka tad  $k+1$  ir nepāra un apskatīsim nepāra pirmskaitli  $p$ , kas dala  $k+1$ . Atkal pierādīsim, ka visi skaitļi formā  $n = p^m$ , kur  $m$  ir naturāls skaitlis, apmierina uzdevuma nosacījumus. Tā kā  $k$  ir pāra, tad

$$1^n + 2^n + 3^n + \dots + k^n = (1^n + k^n) + (2^n + (k-1)^n) + \dots + \left(\left(\frac{k}{2}\right)^n + \left(\frac{k}{2} + 1\right)^n\right) = \sum_{i=1}^{\frac{k}{2}} (i^n + (k+1-i)^n).$$

Līdzīgi pielietojot LTE lemmu katram saskaitāmajam  $i^n + (k+1-i)^n$ , iegūsim, ka  $\nu_p(i^n + (k-i)^n) \geq m+1$ , no kā izriet, ka  $n = p^m | i^n + (k+1-i)^n$  katram  $i = 1, 2, \dots, \frac{k}{2}$ , kas dod prasīto.

**3.uzdevums** Atrast visus pirmskaitļu trijniekus  $(p, q, r)$ , kuriem izpildās

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

**Atrisinājums.** Acīmredzami  $p, q, r$  ir dažādi pirmskaitļi, jo citādi, piemēram pieņemot, ka  $p = q$ , iegūstam

$$p \mid p^r + 1 \implies p \mid 1,$$

kas nav iespējams. Tātad nezaudējot vispārīgumu, pieņemsim, ka  $r > p, q$ . Ir dots, ka  $r \mid p^q + 1$  jeb  $p^q \equiv -1 \pmod{r}$ . Kapinot abas puses kvadrātā, iegūstam  $p^{2q} \equiv 1 \pmod{r}$ . Apskatīsim  $d = \text{ord}_r p$ . Sanāk, ka  $d \mid 2q$ . Ja  $d$  ir nepāra, tad  $d \mid q$ , kas nozīmē, ka

$$-1 \equiv p^q \equiv 1 \pmod{r} \implies r = 2 \implies p, q < 2,$$

kas nav iespējams. Tātad  $d$  ir pāra. Tā kā  $d \mid 2q$ , tad  $d = 2$  vai  $d = 2q$ . Ja  $d = 2$ , tad

$$r \mid p^2 - 1 = (p - 1)(p + 1) \implies r \mid p + 1$$

jo  $r > p - 1$ . No otras puses, tad nozīmē, ka  $r \leq p + 1$ , kas kopā ar  $r > p$  dod  $r = p + 1$ . Tas var gadīties tikai ja  $p = 2$  un  $r = 3$ . Tā kā  $r > q$ , tad arī  $q = 2$ . Taču tas nav iespējams, jo  $3 \nmid 2^2 + 1$ .

Palika izskatīt gadījumu, kad  $d = 2q$ . No Mazās Fermā teorēmas un lemmas par orderi izriet, ka  $p^{r-1} \equiv 1 \pmod{r}$  un  $q \mid 2q \mid r - 1$  jeb  $r \equiv 1 \pmod{q}$ . Tā kā  $q \mid r^p + 1$ , tad

$$0 \equiv r^p + 1 \equiv 1^p + 1 \equiv 2 \pmod{q} \implies q = 2.$$

Sanāk, ka  $p \mid 2^r + 1$  jeb  $2^r \equiv -1 \pmod{p}$ . Analogiski kā iepriekš apskatam  $d' = \text{ord}_p 2$ , un secinām, ka  $d' \mid 2r$  un  $d' \mid p - 1$ . Ja  $d'$  ir nepāra, tad  $d' \mid r$ , kas nozīmē, ka

$$-1 \equiv 2^r \equiv 1 \pmod{p} \implies p = 2,$$

kas nav iespējams, jo  $2 \nmid 2^r + 1$ . Tātad  $d'$  ir pāra. Tā kā  $d' \mid 2r$ , tad  $d' = 2$  vai  $d' = 2r$ . Ja  $d' = 2r$ , tad  $2r \mid p - 1$ , taču  $1 \leq p - 1 < 2r$ , kas nav iespējams. Līdz ar to  $d' = 2$  jeb  $p \mid 2^2 - 1 = 3$ , kas nozīmē, ka  $p = 3$ . Tā kā  $r \mid 3^2 + 1 = 10$  un  $r > p = 3$ , tad  $r = 5$ . Secinām, ka vienīgie derīgie trijnieki ir  $(3, 2, 5)$  un tās cikliskās permutācijas.

**4. uzdevums** Pierādīt, ka katram naturālam nepāra skaitlim  $n$  izpildās

$$((n-1)^n + 1)^2 \mid n(n-1)^{(n-1)^n+1} + n$$

**Atrisinājums.** Ievērojām, ka  $((n-1)^n + 1)^2 \equiv ((-1)^n + 1)^2 \equiv 0 \pmod{n}$ , jo  $n$  ir nepāra, no kā izriet, ka  $n$  dala  $((n-1)^n + 1)^2$ . Pierādīsim, ka visiem pirmskaitļiem  $p$ , kas dala  $((n-1)^n + 1)^2$  izpildās

$$\nu_p(((n-1)^n + 1)^2) \leq \nu_p(n(n-1)^{(n-1)^n+1} + n).$$

Apskatīsim gadījumu kad  $p \mid n$ . Tad no LTE lemmas izriet

$$\nu_p(((n-1)^n + 1)^2) = 2\nu_p((n-1)^n + 1) = 2(\nu_p(n) + \nu_p(n)) = 4\nu_p(n)$$

No otras puses, atkal pielietojot LTE lemmu, dabūjam

$$\nu_p(n(n-1)^{(n-1)^n+1} + n) = \nu_p(n) + \nu((n-1)^{(n-1)^n+1} + 1) = \nu_p(n) + \nu_p(n) + \nu_p(((n-1)^n + 1)) = 4\nu_p(n)$$

Tātad  $\nu_p(((n-1)^n + 1)^2) = 4\nu_p(n) \leq 4\nu_p(n) = \nu_p(n(n-1)^{(n-1)^n+1} + n)$  ir patiess. Tagad apskatīsim gadījumu kad  $p \nmid n$ . Pieņemsim, ka  $\nu_p(((n-1)^n + 1)^2) = a$ . Tad izmantojot LTE lemmu, dabūjam

$$\begin{aligned} \nu_p(n(n-1)^{(n-1)^n+1} + n) &= \nu_p((n-1)^{(n-1)^n+1} + 1) = \nu_p(((n-1)^n)^{\frac{(n-1)^n+1}{n}} + 1) = \\ &= \nu_p((n-1)^n + 1) + \nu_p\left(\frac{(n-1)^n + 1}{n}\right) = \nu_p((n-1)^n + 1) + \nu_p((n-1)^n + 1) \\ &= \nu_p(((n-1)^n + 1)^2) = a, \end{aligned}$$

kur mēs izmantojam to, ka  $p \nmid n$  un  $n \mid (n-1)^n + 1$ . Atkal esam ieguvuši  $\nu_p(((n-1)^n + 1)^2) \leq \nu_p(n(n-1)^{(n-1)^n+1} + n)$ . Līdz ar to šī nevienādība izpildās visiem pirmskaitļiem, kas dala  $((n-1)^n + 1)^2$ , kas dod prasīto.

## 2.mājasdarba atrisinājumi

**1.uzdevums** Katram naturālam skaitlim  $k \geq 2$  atrast visus iespējumus naturālus skaitļus  $n_1, n_2, \dots, n_k$  ar īpašību, ka

$$n_1 | 2^{n_2} - 1, n_2 | 2^{n_3} - 1, \dots, n_k | 2^{n_1} - 1.$$

**Atrisinājums.** Pamanīsim, ka ja  $n_i = 1$  kādam  $1 \leq i \leq k$ , tad

$$n_{i-1} | 2^{n_i} - 1 = 1 \implies n_{i-1} = 1.$$

Analoģiski var pierādīt, ka  $n_j = 1$  visiem  $1 \leq j \leq k$ . Var viegli pārbaudīt, ka skaitļi  $n_1 = n_2 = \dots = n_k = 1$  patiešām apmierina uzdevuma nosacījumus. Tagad pieņemsim, ka visi  $n_i > 1$ . Ar  $p$  apzīmēsim mazāko pirmskaitli, kas dala kādu no  $n_i$ . Nezaudējot vispārīgumu, pieņemsim, ka  $p | n_1$ . Pamanīsim, ka  $p \geq 3$  jeb  $p \neq 2$ , jo citādi  $2 | n_1 | 2^{n_2} - 1$ , kas nav iespējams jebkuram naturālam  $n_2$ .

Apskatīsim  $d = \text{ord}_p 2$ . Tā kā  $n_1 | 2^{n_2} - 1$ , tad  $d | n_2$ . Ja  $d = 1$ , tad

$$2^1 \equiv 1 \pmod{p} \implies p = 1,$$

kas ir pretruna. Līdz ar to eksistē pirmskaitlis  $q$ , kas dala  $d$ . Tā kā pēc Mazas Fermā teorēmas  $2^{p-1} \equiv 1 \pmod{p}$ , tad no lemmas par orderi secinām, ka  $q | d | p - 1$ , kas nozīmē, ka  $q \leq p - 1 < p$ . Taču  $q | d | n_2$ . Tātad mēs atradām vēl mazāku pirmskaitli, kas dala kādu no  $n_i$ , kas dod pretrunu ar pieņēmumu, ka  $p$  ir mazākais pirmskaitlis, kas dala kādu no  $n_i$ . Secinām, ka  $n_1 = n_2 = \dots = n_k = 1$  ir vienīgais iespējamais atrisinājums.

**2.uzdevums** Dots naturāls skaitlis  $k$ . Atrast visus naturālus skaitļus  $n$  ar īpašību, ka

$$3^k | 2^n - 1.$$

**Atrisinājums.** Ja  $n$  ir nepāra jeb  $n = 2m - 1$  kādam naturālam skaitlim  $m$ , tad

$$2^n - 1 \equiv (-1)^{2m-1} - 1 \equiv -1 - 1 \equiv 2 \pmod{3},$$

bet no otras puses  $3 | 3^k | 2^n - 1$ , no kā seko, ka  $2^n - 1 \equiv 0 \pmod{3}$ , kad dod pretrunu. Līdz ar to  $n = 2m$  kādam naturālam  $m$ . Ievērojam, ka skaitlis  $n$  apmierina uzdevuma nosacījumus tad un tikai tad, ja  $k \leq \nu_3(2^n - 1)$ . No LTE lemmas izriet, ka

$$\nu_3(2^n - 1) = \nu_3(4^m - 1) = \nu_3(2^n - 1) = \nu_3(3) + \nu_3(m) = \nu_3(m) + 1.$$

Tātad uzdevuma nosacījums izpildās tad un tikai tad, ja  $k \leq \nu_3(m) + 1$  jeb  $3^{k-1} | m \implies m = 3^{k-1} \cdot l$  kādam naturālam  $l$ . Secinām, ka visi skaitli, kas apmierina uzdevuma nosacījumus ir  $n = 2 \cdot 3^{k-1} \cdot l$ , kur  $l$  ir naturāls skaitlis.

**3. uzdevums** Dots naturāls skaitlis  $n$  ar īpašību, ka  $2^a 3^b + 1$  nedalās ar  $n$  jebkuriem naturāliem  $a$  un  $b$ . Vai var gadīties tā, ka  $2^c + 3^d$  dalās ar  $n$  kādiem naturāliem skaitļiem  $c$  un  $d$ ?

**Atrisinājums.** Pieņemsim, ka eksistē tādi naturāli skaitļi  $c$  un  $d$ , ka  $2^c + 3^d$  dalās ar  $n$ . Tādā gadījumā  $2^c \equiv -3^d \pmod{n}$ . Pēc uzdevuma nosacījumiem  $2^a 3^b + 1$  nedalās ar  $n$  jebkuriem naturāliem  $a$  un  $b$ . Izvēlēsimies,  $a = c$ . Tad

$$2^a 3^b + 1 \equiv 2^c 3^b + 1 \equiv -3^{b+d} + 1 \pmod{n}.$$

Apskatīsim pietiekami lielu naturālo skaitli  $k$ , tādu ka  $k\varphi(n) - d > 0$ . Tad paņemot  $b = k\varphi(n) - d$ , iegūstam

$$2^a 3^b + 1 \equiv -3^{b+d} + 1 \equiv -3^{k\varphi(n)} + 1 \equiv -(3^{\varphi(n)})^k + 1 \equiv -1 + 1 \equiv 0 \pmod{n},$$

kur mēs izmantojam Eilera teorēmu. Esam dabūjuši, ka  $2^a 3^b + 1 \equiv 0 \pmod{n}$ , jeb  $2^a 3^b + 1$  dalās ar  $n$ , kas ir pretruna, kas nozīmē, ka mūsu sākuma pieņēmums ir aplams. Līdz ar to secinām, ka nevar gadīties tā, ka  $2^c + 3^d$  dalās ar  $n$  kādiem naturāliem skaitļiem  $c$  un  $d$ .

**4. uzdevums** Pierādīt, ka katram pirmskaitlim  $p$  eksistē bezgalīgi daudz naturālo skaitļu  $n$  tādu, ka

$$2^{2^{2^{\dots^{2^n}}}} \equiv n^{2^{2^{\dots^2}}} \pmod{p},$$

kur katrā pusē pakāpē divnieks parādās 1397 reizes.

**Atrisinājums.** Katram naturālam  $n$  apzīmēsim  $f(n) = 2^{2^{2^{\dots^{2^n}}}} \pmod{p}$  un  $g(n) = n^{2^{2^{\dots^2}}} \pmod{p}$ . Pamanīsim, ka

$$g(n+p) = (n+p)^{2^{2^{\dots^2}}} \equiv n^{2^{2^{\dots^2}}} = g(n) \pmod{p},$$

kas nozīmē, ka  $g$  ir periodiska ar periodu  $p$ . Ievērojam, ka ja  $n_1 \equiv n_2 \pmod{\varphi(p)}$ , tad  $2^{n_1} \equiv 2^{n_2} \pmod{p}$ . Līdzīgi ja  $n_1 \equiv n_2 \pmod{\varphi(\varphi(p))}$ , tad  $2^{n_1} \equiv 2^{n_2} \pmod{\varphi(p)}$ , no kā seko, ka  $2^{2^{n_1}} \equiv 2^{2^{n_2}} \pmod{p}$ . Analogiski turpinot šādus spriedumus, dabūjam, ka ja  $n_1 \equiv n_2 \pmod{\varphi(\dots\varphi(p)\dots)}$ , kur  $\varphi$  tiek ņemta 1397 reizes, tad  $f(n_1) \equiv f(n_2) \pmod{p}$ , no kā izriet, ka  $f$  ir periodiska ar periodu  $\underbrace{\varphi(\dots\varphi(p)\dots)}_{1397 \text{ reizes}}$ . Apzīmēsim šo ar  $\varphi^{(1397)}(p)$ .

1397 reizes

Katram  $n$  definēsim  $h(n) = 2^{2^{2^{\dots^{2^n}}}}$ , kur divnieks parādās 1395 reizes un  $c = 2^{2^{2^{\dots^{2^2}}}}$ , kur divnieks parādās 1396 reizes. Ievērojām, ka  $h(n) > c$  pietiekami lielam  $n$ . Līdz ar to varam definēt  $b = 2^{2^{h(n)-c}}$ . Ievērojām, ka tad

$$g(b) \equiv b^{2^c} = (2^{2^{h(n)-c}})^{2^c} = 2^{2^{h(n)-c} \cdot 2^c} = 2^{2^{h(n)}} \equiv f(n) \pmod{p}.$$

Acīmredzami skaitļi  $\varphi^{(1397)}(p)$  un  $p$  ir savstarpēji pirmskaitļi, līdz ar to no ķīniešu atlikumu teorēmas izriet, ka eksistē skaitlis  $t$ , kuram

$$t \equiv b \pmod{p} \text{ un } t \equiv n \pmod{\varphi^{(1397)}(p)},$$

pie tam, šādu skaitļu eksistē bezgalīgi daudz. Tādējādi, tā kā  $g$  ir periodiska ar periodu  $p$ , un  $f$  ir periodiska ar periodu  $\varphi^{(1397)}(p)$ , tad

$$g(t) = g(b) \equiv f(n) = f(t)$$

jeb  $2^{2^{2^{\dots^{2^t}}}} \equiv t^{2^{2^{\dots^2}}} \pmod{p}$ , kas dod prasīto.