Skaitļu teorija
NMS juniori

Mājasdarbs #2

2020./2021.m.g.

2020.gada 15.novembris

Iesniegšanas termiņš: 2020.g. 5.decembris
Kam iesūtīt: `kalvis.apsitis`, domēns `gmail.com`

Uzdevums 2.1: Regulāra n-stūra virsotnes savienotas ar slēgtu lauztu līniju, kurai ir n posmi.

(A) Pierādīt, ka jebkuram pāra skaitlim $n \geq 4$, lauztajai līnijai ir vismaz divi paralēli posmi.

(B) Pierādīt, ka jebkuram nepāra skaitlim $n > 3$ nav iespējams, ka lauztajai līnijai ir tieši divi paralēli posmi (t.i. divi posmi ir paralēli, bet nekādi citi nav šiem diviem paralēli, vai arī paralēli savā starpā).

Uzdevums 2.2: Dots pirmskaitlis p un naturāli skaitļi $a \geq 2$, $m \geq 1$.
Zināms, ka $a^m \equiv 1 \pmod{p}$ un $a^{p-1} \equiv 1 \pmod{p^2}$.

(A) Pierādīt, ka $a^m \equiv 1 \pmod{p^2}$.

(B) Atrast kādu pirmskaitli $p > 10$ un a, m, kam minētie apgalvojumi izpildās.

Uzdevums 2.3: Vai var atrast piecus tādus pirmskaitļus p, q, r, s, t, ka $p^3 + q^3 + r^3 + s^3 = t^3$?

Uzdevums 2.4: Atrast visus pirmskaitļus p un q, kuriem izpildās vienādība

$$p + q = (p - q)^3.$$

Uzdevums 2.5: Dots nepāra vesels skaitlis a. Pierādīt, ka $a^{2^n} + 2^{2^n}$ un $a^{2^m} + 2^{2^m}$ ir savstarpēji pirmskaitļi visiem naturāliem n un m, kam $n \neq m$.

Piezīme. Pieraksts a^{b^c} vienmēr nozīmē $a^{(b^c)}$, t.i. darbību locekļus saliktās pakāpēs grupē no labās puses uz kreiso, nevis no kreisās uz labo. (Savukārt $(a^b)^c$ ir cita izteiksme, tā ir $a^{b \cdot c}$.)

NMS gatavošanās materiāli

- `https://bit.ly/2Ur4gLs`: *Kongruences, Pretrunas modulis.*
- `https://bit.ly/2H3LSFF`: *Vienādojumi veselos skaitļos.*
- `https://bit.ly/3pyitoa`: *Skaitļu dalāmība un kongruences*

Definīcija. Dots naturāls skaitlis $m > 1$. Veselus skaitļus a, b sauc par *kongruentiem pēc m moduļa*, ja tie dod vienādus atlikumus, dalot ar m (citiem vārdiem, starpība $a - b$ dalās ar m). Pieraksts: $a \equiv b \pmod{m}$.

Piezīme. Apzīmējumu "mod" izmanto arī veselo skaitļu aritmētikas darbībai: atlikuma iegūšanai. Piemēram, $19 \bmod 7 = 5$ un $(-19) \bmod 7 = 2$.
Atlikums vienmēr pieder intervālam $\{0, \ldots, m-1\}$.
$(a \bmod m) = (b \bmod m)$ ir patiess **tad un tikai tad**, ja $a \equiv b \pmod{m}$.
Ar kongruencēm pēc noteikta moduļa m var veikt algebrā pazīstamas darbības (tās var saskaitīt, atņemt, reizināt, pārnest locekļus uz otru pusi ar pretēju zīmi, utml.) Reizēm drīkst arī abas puses saīsināt ar to pašu nenulles reizinātāju k:

Teorēma par saīsināšanu kongruencēs (1). Ja p ir pirmskaitlis, $ka \equiv kb \pmod{p}$ un $k \not\equiv 0 \pmod{p}$, tad $a \equiv b \pmod{p}$.

Piezīme. Ja m nav pirmskaitlis, tad šādi saīsināt nevar. Piemēram, ja $m = 10$, tad $2 \cdot 1 \equiv 2 \cdot 6 \pmod{10}$, bet $1 \not\equiv 6 \pmod{10}$.

Teorēma par saīsināšanu kongruencēs (2). Ja m ir jebkurš skaitlis, bet k ir savstarpējs pirmskaitlis ar m, tad saīsināt drīkst: No $ka \equiv kb \pmod{p}$ seko $a \equiv b \pmod{p}$.

Definīcija. Inversais jeb apgrieztais elements.

Mazā Fermā teorēma. Ja p ir pirmskaitlis un a nedalās ar p, tad $a^{p-1} \equiv 1 \pmod{p}$.

Definīcija. Katram naturālam skaitlim n definējam *Eilera funkciju* $\varphi(n)$: Visu to veselo skaitļu skaits $k \in [1; n]$, kas ir savstarpēji pirmskaitļi ar n.
Sk. `https://bit.ly/38LCKRo`.

Eilera teorēma. Ja $m > 1$ ir jebkurš vesels skaitlis un a ar m ir savstarpēji pirmskaitļi, tad $a^{\varphi(n)} \equiv 1 \pmod{m}$.

Piezīme. Var uzskatīt, ka Mazā Fermā teorēma ir atsevišķs gadījums Eilera teorēmai, jo katram pirmskaitlim p ir spēkā $\varphi(p) = p - 1$.

Definīcija. Par n-to Fermā skaitli sauc $F_n = 2^{2^n} + 1$, kur $n \geq 0$ ir vesels nenegatīvs.
Pirmie Fermā skaitļi ir

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \quad F_5 = 4294967297.$$

(Pirmie pieci šīs virknes locekļi $F_0, \ldots, F_4$ ir pirmskaitļi. Izpētīti arī daudzi citi, bet to vidū citi pirmskaitļi pagaidām nav atrasti. Piemēram, Fermā skaitlis F_5 dalās reizinātājos: $4294967297 = 641 \cdot 6700417$.)

Apgalvojums. Katri divi Fermā skaitļi F_m un F_n ir savstarpēji pirmskaitļi, ja $m \neq n$.
Sk. pamatojumu iepriekšējās lekcijas bildēs: `https://bit.ly/32MHClt`.