Konspekts "Kā – dalās un kā – nedalās?"

Kongruenču atkārtojums

Bezū lemma:

Ja $a, b \in \mathbb{Z}$, tad eksistē tādi $x, y \in \mathbb{Z}$, ka $ax + by = \gcd(a, b)$.

Funkcijas LKD (angl. *gcd*) un MKD (angl. *lcm*):

- $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$
- $\gcd(am, bm) = m \cdot \gcd(a,b)$
- $\gcd(a,b) = \gcd(a, b+ka)$
- $\gcd(a,x) = 1 \Rightarrow \gcd(a,b) = \gcd(a,bx)$
- $\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1$
- $\operatorname{lcm}(1,2,3,\dots,n) < e^{\sqrt{\frac{n(n+1)}{2} \cdot \ln\left(\frac{n(n+1)}{2}\right)}}$

Ķīniešu atlikumu teorēma:

Ja kopai $\{a_1, a_2, \dots, a_n\}$ visiem $1 \le i, j \le n$ izpildās $\gcd(a_i, a_j) = 1$, tad sistēmai

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ \dots \\ x \equiv r_n \pmod{a_n} \end{cases}$$

eksistē tieši viens atrisinājums $x \le a_1 \cdot a_2 \cdot \dots \cdot a_n$.

Pakāpju dalījumi:

Ja p ir nepāra pirmskaitlis, un $\nu_p(a-1) = x$, tad naturālam y izpildās: $n \vdots p^y \Leftrightarrow (a^n - 1) \vdots p^{x+y}$.

Ja $\nu_2(a^2 - 1) = x$, tad naturālam y izpildās: $n \vdots p^y \Leftrightarrow (a^n - 1) \vdots p^{x+y-1}$.

Fermā mazā teorēma:

Ja naturāls skaitlis a nedalās ar pirmskaitli p, tad $a^{p-1} \equiv 1 \pmod{p}$.

Tue lemma(angl. *Thue lemma*):

Jebkurš nenulles atlikums a pēc pirmskaitļa moduļa p, ir izsakāms veidā $a \equiv \frac{x}{y} \pmod{p}$, kur $0 < |x|, |y| < \sqrt{p}$.

Jebkuriem četriem naturāliem skaitļiem a, X, Y, m, kuriem $m > 1$ un $X \le m < XY$, eksistē tādi veseli x, y, kuriem izpildās $|x| < X$, $0 < y < Y$, un $ax \equiv y \pmod{m}$.

Ležandra teorēmas par trīs un četriem kvadrātiem:

Jebkuru naturālu skaitli n var izteikt kā 4 veselo nenegatīvo skaitļu kvadrātu summu.

Visu naturālus skaitļus n, izņemot $n = 4^a \cdot (8m + 7)$, var izteikt kā 3 veselo nenegatīvo skaitļu kvadrātu summu.

Ležandra teorēma par kāda vienādojuma atrisinājuma:

Vienādojumam ar veseliem koeficientiem $ax^2 + by^2 + cz^2 = 0$ eksistē atrisinājums naturālos skaitļos tad un tikai tad, ja

- $-ab$ ir kvadrātisks atlikums pēc moduļa c
- $-bc$ ir kvadrātisks atlikums pēc moduļa a
- $-ca$ ir kvadrātisks atlikums pēc moduļa b

Ležandra teorēma par faktoriālā iekļauto pirmskaitļa pakāpi:

$$\nu_p\left(C_n^k\right) = \frac{n - \Sigma_{ciparu}(n_p)}{p-1} = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

Kummera teorēma:

$$\nu_p(n!) = \frac{\Sigma_{ciparu}(k_p) + \Sigma_{ciparu}((n-k)_p) - \Sigma_{ciparu}(n_p)}{p-1} = \Sigma_{pārnesumu}\left((n-k)_p + k_p\right).$$

Konspekts "Kā – dalās un kā – nedalās?"

Kāpinātāja pacelšanas lemma (angl. *lifting the exponent*)

Apzīmējums:

Vislielāko pirmskaitļa p pakāpi, kas dala naturālu skaitli n, apzīmē ar $\nu_p(n)$ (dažreiz – ar $\|n\|_p$).

Klasiskais apgalvojums LTE-1:

Ja naturāli skaitļi x un y nedalās ar pirmskaitli $p \neq 2$, bet $x - y$ dalās ar p, tad jebkuram naturālām n izpildās $\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)$.

Īpašgadījumi (p = 2) LTE-2:

Ja naturāli skaitļi x un y nedalās ar pirmskaitli 2, bet $x - y$ dalās ar 4, tad jebkuram naturālām n izpildās $\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n)$.

Ja naturāli skaitļi x un y nedalās ar pirmskaitli 2, bet $x - y$ dalās ar 2, tad jebkuram naturālām n izpildās $\nu_2(x^{2n} - y^{2n}) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n)$.

Ja naturāli skaitļi x un y nedalās ar pirmskaitli 2, bet $x - y$ dalās ar 2, tad jebkuram naturālām n izpildās $\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1$.

Īpašgadījumi (pakāpju summa) LTE-3:

Ja naturāli skaitļi x un y nedalās ar pirmskaitli $p \neq 2$, bet $x + y$ dalās ar p, tad jebkuram naturālām n izpildās $\nu_p(x^{2n+1} + y^{2n+1}) = \nu_p(x + y) + \nu_p(2n + 1)$.

Īpašgadījumi (p un n ir savstarpēji pirmskaitļi) LTE-4:

Ja naturāli skaitļi x un y nedalās ar pirmskaitli p, bet $x - y$ dalās ar p, tad jebkuram naturālām n, ja $\gcd(n, p) = 1$, izpildās $\nu_p(x^n - y^n) = \nu_p(x - y)$.

Ja naturāli skaitļi x un y nedalās ar pirmskaitli p, bet $x + y$ dalās ar p, tad jebkuram naturālām n, ja $\gcd(n, p) = 1$, izpildās $\nu_p(x^n + y^n) = \nu_p(x + y)$.

Kongruenču tabulas

3

A	A²
0	0
1	1
2	1
3	**2**

4

A	A²	A³
0	0	0
1	1	1
2	0	0
3	1	3
4	**2**	**3**

5

A	A²	A³	A⁴
0	0	0	0
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1
5	**3**	**5**	**2**

6

A	A²
0	0
1	1
2	4
3	3
4	4
5	1
6	**4**

7

A	A²	A³	A⁴	A⁵	A⁶
0	0	0	0	0	0
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1
7	**4**	**3**	**4**	**7**	**2**

8

A	A²	A³	A⁴
0	0	0	0
1	1	1	1
2	4	0	0
3	1	3	1
4	0	0	0
5	1	5	1
6	4	0	0
7	1	7	1
8	**3**	**5**	**2**

9

A	A²	A³	A⁴	A⁵	A⁶
0	0	0	0	0	0
1	1	1	1	1	1
2	4	8	7	5	1
3	0	0	0	0	0
4	7	1	4	7	1
5	7	8	4	2	1
6	0	0	0	0	0
7	4	1	7	4	1
8	1	8	1	8	1
9	**4**	**3**	**4**	**7**	**2**

10

A	A²	A³	A⁴
0	0	0	0
1	1	1	1
2	4	8	6
3	9	7	1
4	6	4	6
5	5	5	5
6	6	6	6
7	9	3	1
8	4	2	6
9	1	9	1
10	**6**	**10**	**4**

11

A	A²	A³	A⁴	A⁵	A⁶	A⁷	A⁸	A⁹	A¹⁰
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1
11	**6**	**11**	**6**	**3**	**6**	**11**	**6**	**11**	**2**

12

A	A²	A³	A⁴
0	0	0	0
1	1	1	1
2	4	8	4
3	9	3	9
4	4	4	4
5	1	5	1
6	0	0	0
7	1	7	1
8	4	8	4
9	9	9	9
10	4	4	4
11	1	11	1
12	**4**	**9**	**4**