Konspekts "Pamatīgi pamati"

Pirmskaitļi un to īpašības

2
3
5
7
11
13
17
19
23
29
31
37
41
43
47
53
59
61
67
71
73
79
83
89
97
103
107
109
113
127
131
137
139
149
151
157
163
167
173
179
181
199

Aritmētikas pamatteorēma:
Katru naturālu $n > 1$ var vienā vienīgā veida izteikt reizinājumā: $n = {p_1}^{\propto_1} \cdot {p_2}^{\propto_1} \cdot \ldots \cdot {p_m}^{\propto_m}$.

Pamatfakti:
Skaitlis 1 nav pirmskaitlis. Eksistē viens vienīgs pāra pirmskaitlis: 2. Pirmskaitļu ir bezgalīgi daudz.

Testēšanas algoritms:
Skaitlis n ir pirmskaitlis tad un tikai tad, ja tas nedalās ne ar vienu pirmskaitli, kas nepārsniedz $\sqrt{n}$.

Eiklīda lemma:
Ja p ir pirmskaitlis, un $p|ab$, tad vai nu $p|a$, vai nu $p|b$.

Bertrāna postulāts:
Visiem naturāliem $n > 1$ intervālā $(n; 2n)$ eksistē vismaz viens pirmskaitlis.

Dirihlē teorēma:
Ja skaitļi a un b ir savstārpēji pirmskaitļi, tad eksistē bezgalīgi daudz pirmskaitļu veidā $an + b$, kur n ir naturāls.

Fermā mazā teorēma:
Ja naturāls skaitlis a nedalās ar pirmskaitli p, tad $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Vilsona teorēma:
Ja p ir pirmskaitlis, tad $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.

Grīna – Tao teorēma:
Katram naturālam $n > 2$ eksistē n dažādi pirmskaitļi, kas veido aritmētisko progresiju.

Fermā – Eilera (Ziemassvētku) teorēma:
Jebkurš pirmskaitlis veidā $p = 4n + 1$ izsakāms kā divu naturālu skaitļu kvadrātu summa.

Pirmskaitļa reprezentācija trīs kvadrātu summā:
Ja pirmskaitlis nav izsakāms veidā $8n - 1$, tad to var izteikt kā trīs veselo skaitļu kvadrātu summu.

Pirmskaitļu sadalījums:
Eksistē aptuveni $\frac{n}{\ln n}$ pirmskaitļu, kas nepārsniedz n.

Pirmskaitļu starpības:
Eksistē bezgalīgi daudz pirmskaitļu, kuru starpība ir 246.

Mīdi teorēma:
Pieņemsim, ka naturāls skaitlis a ir mazāks par pirmskaitli p, un $\frac{a}{p} = \overline{0, a_1 a_2 \ldots a_{2m}}$. Tad $a_k + a_{m+k} = 9$.

Apgriezto pirmskaitļu summa:
Apgriezto pirmskaitļu summu var aproksimēt ar formulu $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{p} \approx \ln(\ln p)$.

XXI gadsimta skaitļi																									
2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027
$3 \cdot 23 \cdot 29$	$2 \cdot 7 \cdot 11 \cdot 13$	pirmskaitlis	$2^2 \cdot 3 \cdot 167$	$5 \cdot 401$	$2 \cdot 17 \cdot 59$	$3^2 \cdot 223$	$2^3 \cdot 251$	$7^2 \cdot 41$	$2 \cdot 3 \cdot 5 \cdot 67$	pirmskaitlis	$2^2 \cdot 503$	$3 \cdot 11 \cdot 61$	$2 \cdot 19 \cdot 53$	$5 \cdot 13 \cdot 31$	$2^5 \cdot 3^2 \cdot 7$	pirmskaitlis	$2 \cdot 1009$	$3 \cdot 673$	$2^2 \cdot 5 \cdot 101$	$43 \cdot 47$	$2 \cdot 3 \cdot 337$	$7 \cdot 17^2$	$2^3 \cdot 11 \cdot 23$	$3^4 \cdot 5^2 = 45^2$	$2 \cdot 1013$	pirmskaitlis

1. nodarbība senioriem 07.12.2019.

Konspekts "Pamatīgi pamati"

Funkcijas skaitļu teorijā

Multiplikatīvas funkcijas jēdziens skaitļu teorijā:

Funkciju f sauc par multiplikatīvu, ja visiem naturāliem m un n, kuriem $\gcd(m,n)=1$, izpildās $f(m\cdot n)=f(m)\cdot f(n)$.

Eilera funkcija:

Eilera funkcija $\varphi(n)$ ir naturālo skaitļu, kas mazāki par n un ir savstārpēji pirmskaitļi ar n, skaits. Eilera funkcija ir multiplikatīva funkcija un naturālam skaitlim n tiek definēta šādi:

ja $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_m^{\alpha_m}$, tad $\varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_m}\right)$. Īpašības:

- Pirmskaitļiem $\varphi(p)=p-1$.
- $\sum_{d|n}\varphi(d)=n$.
- Visiem naturāliem m un n izpildās $\varphi(n^m)=n^{m-1}\cdot\varphi(n)$.
- Visiem naturāliem m un n izpildās $\varphi\big(\mathrm{lcm}(m,n)\big)\cdot\varphi\big(\gcd(m,n)\big)=\varphi(n)\cdot\varphi(m)$.

Eilera teorēma: visiem veseliem a un n, kas ir savstārpēji pirmskaitļi, izpildās $a^{\varphi(n)}\equiv 1(\mathrm{mod}\ n)$.

Primitīva sakne: katram pirmskaitlim p eksistē vismaz viena primitīva sakne g pēc moduļa p, kopa $\{1,\ g,\ g^2,\ldots,g^{p-2}\}$ ir kopas $\{1,2,3,\ldots,p-1\}$ permutācija. Pirmskaitļa p primitīvo sakņu skaits ir vienāds ar $\varphi\big(\varphi(p)\big)=\varphi(p-1)$.

Mēbiusa funkcija:

Mēbiusa funkcija $\mu(n)$ pieņem vērtību 0, ja n dalās ar kāda pirmskaitļa kvadrātu, pretējā gadījumā $\mu(n)=(-1)^k$, kur k ir skaitļa n pirmskaitļu dalītāju skaits. Mēbiusa funkcija ir multiplikatīva funkcija, un tai piemīt īpašība $\sum_{d|n}\mu(d)=0$, ja $n>1$.

1. Mēbiusa formula: $g(n)=\sum_{d|n}f(d)\Leftrightarrow f(n)=\sum_{d|n}\mu(d)\cdot g\left(\frac{n}{d}\right)$.

2. Mēbiusa formula: $g(x)=\sum_{n\le x}f\left(\frac{x}{n}\right)\Leftrightarrow f(x)=\sum_{n\le x}\mu(n)\cdot g\left(\frac{x}{n}\right)$, kur $x\ge 1$ ir reāls skaitlis.

Dalītāju funkcijas:

Vispārīgā definīcija: $\sigma_s(n)=\sum_{d|n}d^s$. Ja $n={p_1}^{\alpha_1}\cdot{p_2}^{\alpha_1}\cdot\ldots\cdot{p_m}^{\alpha_m}$, tad

Dalītāju skaits: $\tau(n)=\sigma_0(n)=\sum_{d|n}1=(1+\alpha_1)\cdot(1+\alpha_2)\cdot\ldots\cdot(1+\alpha_m)$,

Dalītāju summa: $\sigma(n)=\sigma_1(n)=\sum_{d|n}d=\left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\cdot\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\cdot\ldots\cdot\left(\frac{p_m^{\alpha_m+1}-1}{p_m-1}\right)$, un īpašības:

$\tau(1)+\tau(2)+\cdots+\tau(n)=\left\lfloor\frac{n}{1}\right\rfloor+\left\lfloor\frac{n}{2}\right\rfloor+\cdots+\left\lfloor\frac{n}{n}\right\rfloor$ un $\sigma(1)+\sigma(2)+\cdots+\sigma(n)=1\cdot\left\lfloor\frac{n}{1}\right\rfloor+2\cdot\left\lfloor\frac{n}{2}\right\rfloor+\cdots+n\cdot\left\lfloor\frac{n}{n}\right\rfloor$.

Ležandra simbols:

Kvadrātiskie atlikumi: Skaitli q sauc par kvadrātisko atlikumu pēc moduļa n, ja eksistē naturāls x, ka $x^2\equiv q(\mathrm{mod}\ n)$. Pēc pirmskaitļa moduļa tieši puse atlikumu ir kvādrātiska. Ja tāda x nav, skaitli q sauc par ne-kvadrātisku atlikumu pēc moduļa n.

Ležandra simbols un Eilera kriterijs:

Ja p ir pirmskaitlis, tad $\left(\frac{a}{p}\right)_L=a^{\frac{p-1}{2}}(\mathrm{mod}\ p)=\begin{cases}0, \text{ ja } a \text{ dalās ar } p.\\ 1, \text{ ja } a \text{ ir kvadrātisks atlikums pēc moduļa } p.\\ -1, \text{ ja } a \text{ ir ne-kvadrātisks atlikums pēc moduļa } p.\end{cases}$

Īpašības: Ležandra simbolam ir multiplikatīva īpašība, ka arī $\left(\frac{a}{p}\right)_L=\left(\frac{b}{p}\right)_L\Leftrightarrow a\equiv b(\mathrm{mod}\ p)$ un $p\equiv q(\mathrm{mod}\ 4a)\Leftrightarrow\left(\frac{p}{a}\right)_L=\left(\frac{q}{a}\right)_L$.

Teorēmas (nepāra pirmskaitļiem p un q):

1. teorēma: $\left(\frac{p}{q}\right)_L=\left(\frac{q}{p}\right)_L\cdot(-1)^{\frac{(p-1)(q-1)}{4}}$
2. teorēma: $\left(\frac{-1}{p}\right)_L=(-1)^{\frac{p-1}{2}}=\begin{cases}1, \text{ ja } p\equiv 1(\mathrm{mod}\ 4)\\ -1, \text{ ja } p\equiv 3(\mathrm{mod}\ 4)\end{cases}$
3. teorēma: $\left(\frac{2}{p}\right)_L=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, \text{ ja } p\equiv 1 \text{ vai } 7(\mathrm{mod}\ 8)\\ -1, \text{ ja } p\equiv 3 \text{ vai } 5(\mathrm{mod}\ 8)\end{cases}$

Gausa lemma: Ja $\gcd(a,p)=1$, un ir x atlikumu $a(\mathrm{mod}\ p), 2a(\mathrm{mod}\ p),\ldots,\frac{p-1}{2}\cdot a(\mathrm{mod}\ p)$ skaits, kuri pārsniedz $\frac{p}{2}$, tad $\left(\frac{a}{p}\right)_L=x$.

Jakobī simbols:

Ja $n={p_1}^{\alpha_1}\cdot{p_2}^{\alpha_1}\cdot\ldots\cdot{p_m}^{\alpha_m}$, tad $\left(\frac{a}{n}\right)_J=\left(\frac{a}{p_1}\right)_L^{\alpha_1}\cdot\left(\frac{a}{p_2}\right)_L^{\alpha_2}\cdot\ldots\cdot\left(\frac{a}{p_m}\right)_L^{\alpha_m}$. Ja $\left(\frac{a}{n}\right)_J=-1$, tad a ir ne-kvadrātisks atlikums pēc moduļa n.

1. nodarbība senioriem 07.12.2019.

Konspekts "Pamatīgi pamati"

Faktoriāli, binomiālie koeficienti, skaitļa pieraksts, dalīšanas pazīmes

Faktoriāli:

Skaitļa izvirzījums faktoriālos: Jebkuram naturālam skaitlim n eksistē tieši viens veids, kā to pierakstīt formā $n = f_1 \cdot (1!) + f_2 \cdot (2!) + \cdots + f_m \cdot (m!)$, kur f_i ir vesels nenegatīvs skaitlis, kas nepārsniedz i, un $f_m > 0$.

Stirlinga formula: $\sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot e^{\frac{1}{12n}}$.

Binomiālie koeficienti:

Binomiālie koeficienti parāda, cik daudz kombināciju ar izmēru k var iegūt no n dažādiem elementiem: $C_n^k = \frac{n!}{(n-k)!\cdot k!}$.

Vandermonda identitāte: $C_{n+m}^k = \left(C_n^0 \cdot C_m^k\right) + \left(C_n^1 \cdot C_m^{k-1}\right) + \left(C_n^2 \cdot C_m^{k-2}\right) + \cdots + \left(C_n^0 \cdot C_m^k\right)$.

Binomiālo koeficientu īpašības:

- $C_n^k = C_n^{n-k} = \frac{n}{k} \cdot C_{n-1}^{k-1}$
- $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$
- $C_n^m \cdot C_m^{n-k} = C_n^k \cdot C_k^{n-m}$
- $C_n^0 + C_n^1 + C_n^2 + \cdots + C_n^{n-1} + C_n^n = 2^n$
- $(C_n^0)^2 + (C_n^1)^2 + (C_n^2)^2 + \cdots + (C_n^{n-1})^2 + (C_n^n)^2 = C_{2n}^n$

Luka teorēma: Ja p ir pirmskaitlis, un p-nārajā skaitļošanas sistēmā skaitļi M un N izskatās attiecīgi $\overline{m_k m_{k-1} \dots m_2 m_1}_p$ un $\overline{n_k n_{k-1} \dots n_2 n_1}_p$, tad $C_{n_1}^{m_1} \cdot C_{n_2}^{m_2} \cdot \ldots \cdot C_{n_k}^{m_k} \equiv C_N^M \pmod p$.

Kummera teorēma: Ja p ir pirmskaitlis, un C_n^k dalās ar p, tad maksimāla p pakāpe, ar kuru dalās C_n^k, ir vienāda ar pārnesumu skaitu, kas rodas, stabiņā saskaitot skaitļus $(k)_p$ un $(n-k)_p$ (indekss p apzīmē p-nāro skaitļošanas sistēmu).

Volstenholma teorēma: Ja $p > 3$ ir pirmskaitlis, tad $C_{2p}^p \equiv 2 \pmod{p^3}$

Dalīšanas pazīmes:

Pēdējie cipari:

Skaitlis X dalās ar 2^n, ja skaitlis $(X \bmod 10^n)$ dalās ar 2^n.
Skaitlis X dalās ar 5^n, ja skaitlis $(X \bmod 10^n)$ dalās ar 5^n.
Skaitlis X dalās ar 10^n, ja tā pēdējie cipari ir nulles.

Pēdējā cipara saīsinājums:

Skaitlis X dalās ar 7, ja skaitlis $\left((X \operatorname{div} 10) - 2 \cdot (X \bmod 10)\right)$ dalās ar 7.
Skaitlis X dalās ar 13, ja skaitlis $\left((X \operatorname{div} 10) + 4 \cdot (X \bmod 10)\right)$ dalās ar 13.
Skaitlis X dalās ar 17, ja skaitlis $\left((X \operatorname{div} 10) - 5 \cdot (X \bmod 10)\right)$ dalās ar 17.
Skaitlis X dalās ar 19, ja skaitlis $\left((X \operatorname{div} 10) + 2 \cdot (X \bmod 10)\right)$ dalās ar 19.
Skaitlis X dalās ar 31, ja skaitlis $\left((X \operatorname{div} 10) - 3 \cdot (X \bmod 10)\right)$ dalās ar 31.

Ciparu summa:

Skaitlis X dalās ar 3 vai 9, ja tā ciparu summa dalās attiecīgi ar 3 vai 9.
Skaitlis X dalās ar 11, ja tā cipāru uz nepāra vietām summas un tā cipāru uz pāra vietām summas starpība dalās ar 11.
Skaitlis X dalās ar patvaļīgu skaitļa a dalītāju k, ja $(a+1)$-nārajā skaitļošanas sistēmā skaitļa X ciparu summa dalās ar k.

Ciparu grupēšana:

Skaitlis X dalās ar 27, ja trīsciparu skaitļu, kuri tiek veidoti, grupējot skaitļa X ciparus pa 3, summa dalās ar 27.
Skaitlis X dalās ar 37, ja trīsciparu skaitļu, kuri tiek veidoti, grupējot skaitļa X ciparus pa 3, summa dalās ar 37.
Skaitlis X dalās ar 99, ja divciparu skaitļu, kuri tiek veidoti, grupējot skaitļa X ciparus pa 2, summa dalās ar 99.
Skaitlis X dalās ar 101, ja, summa dalās ar 101.
Skaitlis X dalās ar patvaļīgu skaitļa $(t^n - 1)$ dalītāju k, ja t-nārajā skaitļošanas sistēmā n-ciparu skaitļu, kuri tiek veidoti, grupējot [t-nārajā skaitļošanas sistēmā] skaitļa X ciparus pa n, summa dalās ar k.