DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Veselo skaitļu teorija

15.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

1. Pirmskaitļi

Pirmskaitļi dabā - dažiem dzīvniekiem dzīves (attīstības) cikla ilgums (gados) ir pirmskaitlis, tas ir izveidojies evolūcijas rezultātā, lai labāk izvairītos no plēsējiem.

Ja kukaiņa dzīves cikla garums n ir salikts skaitlis, tad

- evolūcijas rezultātā lielāka iespēja ir parādīties vairākiem plēsējiem, kuru dzīves ciklu garumu ir n dalītāji, tādējādi dotās sugas kukaiņi būs vairāk apdraudēti;
- dažādas populācijas savā starpā vairāk konkurēs uz resursiem.

Evolūcijas rezultātā kukaiņu dzīves cikla ilgums konverģē uz pirmskaitli. Ir zināmi konkrēti piemēri - cikādēm dzīves ciklu garumi ir 7, 13 un 17 gadi.

1.1. Pirmskaitļu īpašības, hipotēzes un neatrisinātas problēmas

1.1.1. Fakti

Visi pirmskaitļi $p > 3$ apmierina nosacījumu

$$p \equiv \pm 1 \pmod 6.$$

1.1. teorēma. Eksistē patvaļīgi gari "pirmskaitļu tuksneši".

1.2. teorēma. (*Bertrana postulāts, Čebiševa teorēma*)

$$\forall n > n_0 \ \exists p : n < p < 2n - 2.$$

1.3. teorēma. Rinda $\sum_p \frac{1}{p}$ diverģē.

1.4. teorēma. (*Dirihlē teorēma par pirmskaitļiem aritmētiskās progresijās*) Ja $LKD(a, b) = 1$, tad aritmētiskā progresija

$$a, a + b, a + 2b+, \ldots$$

satur bezgalīgi daudz pirmskaitļu. Ekvivalents formulējums: eksistē bezgalīgi daudz pirmskaitļu p, kas apmierina nosacījumu

$$p \equiv a (\text{mod } b).$$

1.1. piezīme. Diezgan viegli ir pierādīt Dirihlē teorēmu speciālgadījumos, piemēram $p \equiv 1 (\text{mod } 2)$ vai $p \equiv 3 (\text{mod } 4)$.

Visi nepāra pirmskaitļi ir formā $p \equiv 1 (\text{mod } 2)$

Atzīmēsim, ka nepāra pirmskaitļiem ir iespējami tikai divi gadījumi:

$$p \equiv 1 (\text{mod } 4) \vee p \equiv 3 (\text{mod } 4).$$

Pieņemsim, ka eksistē galīgs skaits pirmskaitļu, kas apmierina nosacījumu

$$p \equiv 3 \equiv -1 (\text{mod } 4).$$

Apzīmēsim tos ar $p_1, ..., p_n$. Apskatīsim

$$N = 4p_1 ... p_n - 1.$$

Redzam, ka

- N dalās vismaz ar vienu pirmskaitli no kopas $p_1, ..., p_n$, jo pretējā gadījumā $N \equiv 1 (\mathrm{mod}\ 4)$,
- N nevar dalīties ne ar vienu pirmskaitli no kopas $p_1, ..., p_n$ pēc konstrukcijas.

1.1.2. Speciāla veida pirmskaitļi

Tiek pētītas vairākas pirmskaitļu sērijas. Pirmskaitļi ir vajadzīgi kriptogrāfijā.

Svarīgākās pirmskaitļu sērijas:

- *Fermā pirmskaitļi* $2^{2^n} + 1$ - $3, 5, 17, 257, 65537$;
- *Mersenna pirmskaitļi* $2^n - 1$ - 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, ..., pašlaik ir zināmi ap 26 pirmskaitļi;
- *Vagstafa pirmskaitļi* $\frac{2^n+1}{3}$ - 3, 11, 43, 683, 2731, 43691, 174763, 2796203,...;

1.1.3. "Pirmskaitļu teorēma"

Definēsim ar $\pi(x)$ pirmskaitļu skaitu, kas nepārsniedz x:

$$\pi(x) = \sum_{p \leq x} 1.$$

Definēsim

$$li(x) = \int_0^x \frac{dt}{\ln(t)}.$$

K.Gauss ap 1792.gadu izteica hipotēzi, kas tika pierādīta tikai 1896.gadā.

1.5. teorēma. (*pirmskaitļu teorēma*)

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1 \text{ vai } \lim_{x \to \infty} \frac{\pi(x)}{li(x)} = 1.$$

PIERĀDĪJUMS Ļoti grūts. Vienādība seko no Lopitāla teorēmas.
■

1.2. piezīme. Īstenībā tika pierādīts vairāk:

$$|\pi(x) - li(x)| < C_1 x e^{-C_2\sqrt{ln(x)}}.$$

Vēlāk tika pierādīts, ka $\pi(x) - li(x)$ bezgalīgi bieži maina zīmi. Nav zināms neviens x, kuram $\pi(x) - li(x) > 0$.

1.3. piezīme. Hipotēze:

$$\pi(x) = li(x) + O(\sqrt{x} ln(x)).$$

1.1.4. Pirmskaitļu virknes

Pirmskaitļu pāri $(p, p+2)$ sauc par *dvīņu pirmskaitļiem.*

Hipotēze: dvīņu pirmskaitļu ir bezgalīgi daudz.

Hipotēzes: pirmskaitļu virkņu

- $(p, p+4)$,

- $(p, p+6)$,
- $(p, p+2, p+6)$,
- $(p, p+4, p+6)$,
- $(p, p+2, p+6, p+8)$,
- $(p, p+2, p+6, p+8, p+12)$,

ir bezgalīgi daudz.

1.1.5. Goldbaha hipotēze

Hipotēze (*stiprā Goldbaha hipotēze*): katrs pāra skaitlis $n > 2$ ir izsakāms divu pirmskaitļu summas veidā (1742.gads). (Pārbaudīta līdz 10^{18}).

Hipotēze (*vājā Goldbaha hipotēze*): katrs nepāra skaitlis $n > 7$ ir izsakāms trīs pirmskaitļu summas veidā (1742.gads). (Ir pierādīta pietiekoši lieliem n.)

1.2. Rīmana ζ-funkcija

1.2.1. Definīcija

Rīmana ζ-funkcija tiek definēta ar vienādību

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

1.2.2. Vienkāršākās īpašības

1.6. teorēma.

1. Ja $s > 1$, tad $\zeta(s)$ konverǧē.
2. Ja $s \leq 1$, tad $\zeta(s)$ diverǧē.

PIERĀDĪJUMS
Izmantojam pozitīvu rindu konverǧences Košī integrālo pazīmi -

$$\int_1^{+\infty} x^{-s} dx < \infty \iff s > 1. \blacksquare$$

1.7. teorēma. $s > 1 \implies \zeta(s) = \prod_p \frac{1}{1-p^{-s}}$.

PIERĀDĪJUMS Ievērosim, ka

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \ldots$$

Definēsim

$$P_k(s) = \prod_{i=1}^{k} \frac{1}{1-p_i^{-s}}.$$

Redzam, ka

$$P_k(s) = \sum_{n \in D_k} \frac{1}{n^s},$$

kur kopa D_k satur visus naturālos skaitļus, kas dalās tikai ar pirmajiem k pirmskaitļiem.

$n \notin D_n \implies n > p_k$.

$$|P_k(s) - \zeta(s)| = \sum_{n \notin D_k} \frac{1}{n^s} \leq \sum_{n > p_k} \frac{1}{n^s} = \zeta(s) - \sum_{n \leq p_k} \frac{1}{n^s}.$$

Redzam, ka

$$k \to \infty \implies \zeta(s) - \sum_{n \leq p_k} \frac{1}{n^s} \to 0.\blacksquare$$

1.2.3. Rīmana problēma

Rīmana problēma

$\zeta(s)$ visām nullēm, kas nav uz reālas ass, reāla daļa ir vienāda ar 1/2.