FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. március 30.

$A'(a,n)$	a ... ist Zeuge	$\forall a$	test
$a^{n-1} \equiv 1 \pmod n$	(Fermat)	CARMICHAEL-Zahl	FERMAT $p \leq 1/2$ v. $p = 1$
$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$	EULER-JACOBI	X	SOLOVAY-STRASSEN (1977) $p \leq 1/2$
$(a^t, a^{2t}, \ldots, a^{2^s \cdot t}) \equiv$ $\equiv (\ldots, -1, 1, \ldots, 1, 1) \pmod n$	ERÖS	X	MILLER-RABIN (1976) (1980) $p \leq 1/4$

$18q \mid (6q+1)\cdot(\underbrace{12q+1}_{-6q})\cdot(\underbrace{18q+1}_{\equiv 1}) - 1 \equiv$

$\equiv (1+6q)\cdot(1-6q)\cdot 1 - 1 \equiv$

$\equiv 1 - 36q^2 - 1 = 36q^2 \equiv 0 \pmod{18q}$

TÉTEL Euler-faktori-kritérium: $C = \{a \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n\} \subseteq \mathbb{Z}_n^*$

(valódi részcsop. $\mathbb{Z}_n^*$-ben.)

Biz: ha $a, b \in C$.

$$(ab)^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right) \equiv \left(\frac{ab}{n}\right) \pmod n$$ ✓

Köv: $|C| \le \frac{1}{2}|\mathbb{Z}_n^*|$, AGRAWAL, KAYAL, SAXENA (2002) polinomos idejű prímtesztje

p prím, $x^2 \equiv 1 \pmod p \Rightarrow x \equiv \pm 1 \pmod p$

n pH. $\Rightarrow n = 2^s \cdot t + 1$, $a \perp n$

(t pH.)

M-R-test: $(a^t, a^{2t}, a^{4t}, \dots, a^{2^s \cdot t}) \overset{?}{\equiv} (\dots, -1, 1, \dots, 1, 1) \pmod n$

($)^2$ ($)^2$ ($)^2$

PÉLDA $n = 341 = 2^2 \cdot 85 + 1$ $t = 85, s = 2, a = 2$

$2^{85} \equiv 32 \pmod{341}$

$2^{170} \equiv 1 \pmod{341}$

$2^{340} \equiv 1 \pmod{341}$

$(a^t, a^{2t}, a^{4t}) \equiv (32, 1, 1) \pmod{341}$

$32^2 \equiv 1$ pedig $32 \neq \pm 1$

$\Rightarrow 341$ összetett szám.

HF 18 Tanfolyis u-561-et a MR-tanfel.

PÉLDA: 2 olyan egész állítás: 2047, 3277, 4033, ...

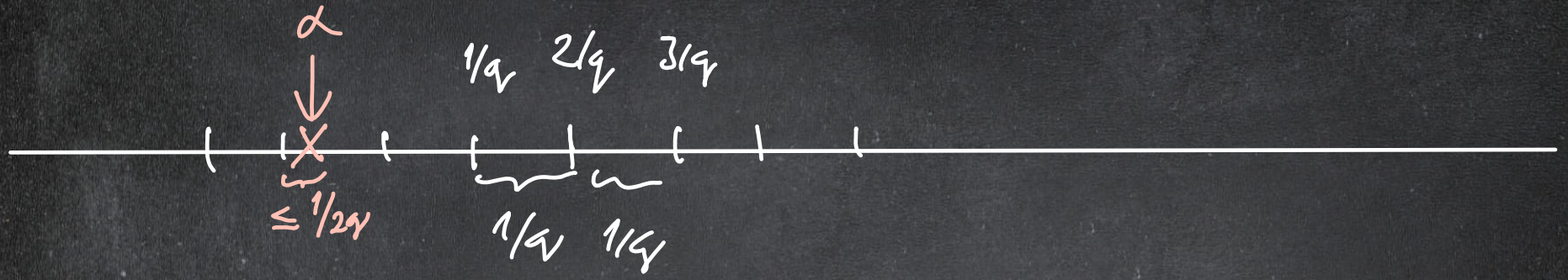
10^6-ig 46 db

DIOFANTOSZI APPROXIMÁCIÓ

$\alpha \in \mathbb{R}$ keressük $\frac{p}{q} \in \mathbb{Q}$ tört, amire $\left|\alpha - \frac{p}{q}\right|$ kicsi és q ne legyen túl nagy.

$\alpha = \sqrt{2} = 1{,}4142\ldots$

$\frac{p}{q} = \frac{141}{100}$ $\quad \frac{p}{q} = \frac{17}{12} = 1{,}416$ $\quad \frac{p}{q} = \frac{99}{70} = 1{,}4142\ldots$



DIRICHLET APPROXIMÁCIÓS TÉTELE $\forall \alpha \in \mathbb{R}\ \forall n \in \mathbb{N}\ \exists \frac{p}{q} \in \mathbb{Q} : \left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}$

és $1 \le q \le n$.

Biz: $\{0\alpha\}, \{1\alpha\}, \dots, \{n\alpha\} \in [0,1) = [0, 1/n) \cup [1/n, 2/n) \cup \dots \cup [(n-1)/n, 1]$

$n+1$ db szám — n db szelet

szelet-elv $\Rightarrow \exists\, 0 \le i < j \le n : \left|\{i\alpha\} - \{j\alpha\}\right| < \frac{1}{n}$

$$\left.\begin{aligned} i\alpha &= [i\alpha] + \{i\alpha\} \\ j\alpha &= [j\alpha] + \{j\alpha\} \end{aligned}\right\} \Rightarrow \left|\{i\alpha\} - \{j\alpha\}\right| = \left|\underbrace{(i-j)}_{q}\alpha - \underbrace{([i\alpha] - [j\alpha])}_{p}\right| < \frac{1}{n}$$

$1 \le q \le n$

Tehát $|q\alpha - p| < \frac{1}{n} \Rightarrow |\alpha - \frac{p}{q}| < \frac{1}{nq}$. ∎

DEF $\frac{p}{q} \approx \alpha$ <u>jó közelítés</u>, ha $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

TÉTEL $\alpha \notin \mathbb{Q} \Rightarrow$ van ∞ sok jó közelítése.

Biz. $\forall n: \exists \frac{p_n}{q_n} \in \mathbb{Q}: |\alpha - \frac{p_n}{q_n}| < \frac{1}{nq_n}$ és $q_n \in n$

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{nq_n} \leq \frac{1}{q_n} \leq \frac{1}{n} \to 0$$

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$$

Mivel tört sok véges számnak közelítő alakja $\frac{p_n}{q_n}$ sorozatelem

Hc $\frac{p_{n_1}}{q_{n_1}} = \frac{p_{n_2}}{q_{n_2}} = \ldots = s \in \mathbb{Q}$

$$\left.\begin{array}{l} \frac{p_{k_1}}{q_{k_1}}, \frac{p_{k_2}}{q_{k_2}}, \ldots \to \alpha \\ \;\; \| \qquad \| \\ \;\; s \qquad s \qquad \to s \end{array}\right\} \Rightarrow \alpha = s \text{ és } \alpha \notin \mathbb{Q}. \blacksquare$$

TÉTEL $\alpha \in \mathbb{Q} \Rightarrow$ csak véges sok jó közelítése van.

Biz: $\alpha = \frac{a}{b} \in \mathbb{Q}$. Tfh. $\frac{p}{q}$ jó közelítés, de $\frac{p}{q} \neq \alpha$.

$$\frac{1}{q^2} > \left|\alpha - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq-bp}{bq}\right| = \frac{|aq-bp|}{bq} \geq \frac{1}{bq}$$

($\alpha - \frac{p}{q} \neq 0$)

$\Rightarrow q < b \Rightarrow$ csak véges sok lehetőség van q-ra

Minden q-hoz csak véges sok p lesz jó.

$\Rightarrow$ csak véges sok jó $\frac{p}{q}$ közelítés van. $\blacksquare$

HF19 Keressünk egy CF összeget, jól közelítőt $\alpha = \frac{4}{7}$-hez.

HF20 $f: x \mapsto \frac{ax+b}{cx+d}$ $\quad g: \frac{ex+f}{gx+h}$

$$x \mapsto f(g(x)) = \frac{?x + ?}{?x + ?}$$

Próbáljuk meg ezt „népiesen" értelmezni.