3/3. 10:15 – 12:00

2014. szeptember 9.
hétfő
(kedd)

Sárközy külföldön, Gyarmati helyettesít.
S. hata jövő hedden, akkor az E elmarad.
Pótlás: ∀ előadás 7,5 perccel hosszabban lesz tartva.

Irodalom:
Freud – Gyarmati (E.):
Turán – Gyarmati (E.):
Sárközy:
Szalay (M.):
} Számelmélet

specmatos

Vizsga: majd Sárközy mondja (írásbeli)

— ∘ —

Természetes számok: $\mathbb{N} = \{ \overset{?}{0}; 1; 2; \dots \}$

Természetes számok
Számlálás
~~Egész számok~~
} alapfogalmak

Alaptulajdonságok rögzítése → axiómák → Peano-féle axiómarendszer
Ezek között a teljes indukció axiómája* (ami miatt a t.i. működik)
Ld. Fuchs: Algebra – számelmélet jegyzet.
Az axiómarendszer nem mondja meg, mik az egész számok, csak azt, mit lehet velük tenni.

Def. Azt mondjuk, hogy $a \in \mathbb{Z}$ osztható $b \in \mathbb{Z}$-vel, ha $\exists\, c \in \mathbb{Z}$, amelyre $a = bc$.
(Pl. 0 osztója 0-nak: $0 = 0 \cdot c \quad \forall c \in \mathbb{Z}$-re)
Jelölés: $b \mid a$

Tétel. (A maradékos osztás tétele): Ha $a, b \in \mathbb{Z}$, akkor $\exists!\, q, r \in \mathbb{Z}$, amelyekre $a = bq + r$, ahol $0 \leq r < |b|$

Def. Egy H halmazon definiált reláción a H elemeiből képzett rendezett párok egy S részhalmazát értjük.

(Pl. $(2;3) \notin S$, mert $2 \nmid 3$)

Def. Egy H halmazon definiált reláció reflexív, ha $\forall r \in H$-ra $(r;r) \in S$.
szimmetrikus, ha $(r;h) \in S \Rightarrow (h;r) \in S$
tranzitív, ha $(r_1;r_2) \in S \wedge (r_2;r_3) \in S \rightarrow (r_1;r_3) \in S$.

Példák:

– egyenlőség:	refl.	szimm.	tranz.
– kisebb:	–	–	tranz.
– oszthatóság:	refl.	–	tranz.

* Konstruktivizmus nem fogadja el az IDB-t és a T.I.-t.

Tétel. Egy x ~~pozitív~~ egész szám akkor és csak akkor osztója $\forall$ egész számnak, ha $x = \pm 1$.

B: $a|b \Leftrightarrow \exists c \in \mathbb{Z}: \quad b = ac$

$a = \pm 1$-re $\quad c = \pm b \quad \rightarrow \quad \forall$-nek osztója. ✓

Ha $a|b \quad \forall b \in \mathbb{Z}$, akkor $\quad a|1 \Rightarrow |a| \leq 1 \rightarrow a = \pm 1. \quad a \neq 0. \quad Q \in D.$

Def. Egy $e \in \mathbb{Z}$ egység $\Leftrightarrow \forall a \in \mathbb{Z}: \quad e|a.$

Következmény. Az egész számokon ± 1 egység.

A fenti def.-ben $\mathbb{Z}$ helyett lehet más is, pl. a Gauss-egészeken ± 1 és $\pm i$ egységek.

Tétel. $a|a$

B: Def. szerint $\quad a = 1 \cdot a \quad \rightarrow \quad a|a. \qquad Q \in D.$

Tétel. $a|b \quad \Rightarrow \quad -a|b, \; a|-b, \; -a|-b.$

B: $a|b \quad \Rightarrow \quad \exists c: \quad b = ac$

$b = (-a)(-c) \quad \Rightarrow \quad -a|b$

$(-b) = a \cdot (-c) \quad \Rightarrow \quad a|-b$

$(-b) = (-a) \cdot c \quad \Rightarrow \quad -a|-b \qquad Q \in D.$

Tétel. $a|b, \quad b \neq 0 \quad \Rightarrow \quad |a| \leq |b|$

B: $\exists c \in \mathbb{Z}: \quad b = ac$

$\Rightarrow \quad |b| = |a| \cdot |c|$

$c \neq 0$, mert $\quad b \neq 0$

$\Rightarrow |c| \geq 1 \quad \Rightarrow \quad |b| \geq |a| \cdot |c| \geq |a|. \qquad Q \in D.$

Tétel. $0|0$, de 0 esetében más egészet sem osztója.

B: $\exists c: \quad 0 = 0 \cdot c \quad \forall c \in \mathbb{Z}$-re. $\quad \Rightarrow \quad 0|0$

$0|a \quad \Leftrightarrow \quad a = 0 \cdot c \quad \Leftrightarrow \quad a = 0. \qquad Q \in D.$

Tétel: $a|b, \quad a|c, \quad d, e \in \mathbb{Z} \quad \Rightarrow \quad a|bd + ce$

B: $\exists b_0, c_0 \in \mathbb{Z}: \quad b = ab_0, \quad c = ac_0$

$bd + ce = ab_0d + ac_0e = a \cdot (b_0d + c_0e) \quad \Rightarrow \quad a|bd + ce \quad Q \in D.$

Tétel. Ha $a|b$ és $b|a$, akkor $\quad a = \pm b.$

B: $|a| \leq |b| \quad \wedge \quad |b| \leq |a| \quad \Rightarrow |a| = |b| \quad \Rightarrow \quad a = \pm b \qquad Q \in D.$

Def. Az $a \in \mathbb{Z}$ egységtöbbszöröseit a asszociáltjainak nevezzük.

Def. legnagyobb közös osztó

1. Az $a, b \in \mathbb{Z}$ - vel D l.n.k.o.-ja, ha
   1) $\begin{cases} - & D \mid a \\ - & D \mid b \end{cases}$ „kitüntetett közös osztó"
   2) $-\ d \mid a,\ d \mid b \Rightarrow d \mid D.$

2. Az $a, b \in \mathbb{Z}$ - vel D l.n.k.o.-ja, ha a közös osztók közül neki van a legnagyobb abszolút értéke.

Jelölje D_1 az 1. definíciban megadott l.k.o.-t,
D_2 a 2. —"— —"— —"—.

Megjegyzések. ① D_2 egyszerűsítő erejéig egyértelmű és létezik.
B: $d \mid a,\ d \mid b \Rightarrow d \le |a|$ $\Rightarrow$ létezés
D_2 és D_2' l.k.o. $\rightarrow$ ~~$D_2 \mid D_2'$ és $D_2' \mid D_2$~~ $\Rightarrow$ egyértelműség: ~~$D_2 = \pm D_2'$~~
$|D_2| = |D_2'| \Rightarrow D_2 = \pm D_2'$

② D_1 (ha létezik), egyértelmű egyszerűsítő erejéig
B: Indirekt: D_1, D_1' l.k.o. $\Rightarrow D_1 \mid D_1' \wedge D_1' \mid D_1 \Rightarrow |D_1| = |D_1'| \rightarrow$ egyértelmű

Tétel. Ha D_1 létezik, akkor $D_1 = \pm D_2$.

B: D_2 közös osztó: $D_2 \mid a,\ D_2 \mid b \Rightarrow D_2 \mid D_1$ per def. 1.
$\Rightarrow |D_2| \le |D_1|$
De D_2 abszt. értéke a lehető legnagyobb $\Rightarrow |D_2| = |D_1|$. $\square$ $D \in \mathbb{Q}$.

Kivételt jelent az $a = b = 0$ eset, mert ∞ sok közös osztójuk van
$\rightarrow D_1 = 0$
$\rightarrow D_2$ nem definiált

~~Tétel~~. D_1 létezése az eukl. alg. következménye lesz.

Euklidészi algoritmus.

$b \neq 0$, $a \in \mathbb{Z}$ - t osztjuk b-vel maradékosan: $a = b q_1 + r_1,\ 0 \le r_1 < |b|$
Ha $r_1 = 0 \rightarrow$ vége,
Ha $0 < r_1 < |b| \rightarrow$ folytatódik az eljárás
b-t osztjuk maradékosan r_1-gyel $b = r_1 q_2 + r_2 \quad 0 \le r_2 < r_1$
Ha $r_2 = 0 \rightarrow$ vége
Ha $0 < r_2 < r_1 \rightarrow$ folytatódik
r_1-gyet m. o. osztjuk r_2-vel $r_1 = r_2 q_3 + r_3 \quad 0 \le r_3 < r_2$
s.í.t.

$$|b| > r > r_1 > \dots > r_{n+1} = 0$$

$\{r_n\}$ sz. m. cs. a pozitív (nemnegatív) egészeken $\rightarrow$ monotonitása,
véges sok lépésben véget ér.
Felső becslés: legfeljebb $|b|$ lépésben véget ér. (Van jobb becslés: $\log_2 |b|$.)

Utolsó 2 lépés:
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_{n+1} + 0$$

Tétel. $r_n = D_1$ (tehát D_1 létezik)

Következmény. $\neg(a = b = 0)$ - ra $D_1 = D_2$ $\mathbb{Z}$-n.

B.
$$a = b q_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$r_2 = r_3 q_4 + r_4$$
$$\vdots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$

Bizonyítandó: 1) r_n közös osztó
2) $d|a,\ d|b \Rightarrow d|r_n$

1) Alulról felfelé haladunk:
$$r_n \mid r_{n-1}$$
$$r_n \mid r_{n-2}$$
$$r_n \mid r_{n-3}$$
$$\vdots$$
$$\left.\begin{array}{l} r_n \mid b \\ r_n \mid a \end{array}\right\} \checkmark$$

2) Felülről haladunk lefele:
$$d|a,\ d|b \Rightarrow d|r_1$$
$$d|b,\ d|r_1 \Rightarrow d|r_2$$
$$\vdots$$
$$d|r_{n-2},\ d|r_{n-1} \Rightarrow d|r_n \checkmark$$
QED.

2014. szeptember 23.
kedd

a és b lnko.-ja: $(a;b)$ → lényegében egyértelmű (± 1)

Definíció. Ha $(a;b) = 1$, akkor a és b viszonylagos törzsszámok (relatív prímek).

Tétel. $(a;b)$ felírható a és b egész együtthatós lineáris kombinációjaként:
$$\exists x, y \in \mathbb{Z}: \quad ax + by = (a;b)$$

B: $a = b = 0$ triviális
Ha $b \neq 0$ → euklidesz alg. alapján indukcióval igazoljuk, hogy r_k felírható a, b lin. komb.-jaként: $r_k = x_k a + y_k b$
$$r_1 = a - bq_1 = 1 \cdot a + (-q_1) \cdot b$$
$$r_2 = b - r_1 q_2 = b - q_2 \cdot (1 \cdot a + (-q_1) b) = (-q_2) \cdot a + (1 + q_1 q_2) b$$
Indukció: $r_{k-2} = x_{k-2} a + y_{k-2} b$ $(x_i, y_i \in \mathbb{Z})$
$$r_{k-1} = x_{k-1} a + y_{k-1} b$$
$$r_k = r_{k-2} + r_{k-1} q_k = (x_{k-2} a + y_{k-2} b) - q_k \cdot (x_{k-1} a + y_{k-1} b) =$$
$$= \underbrace{(x_{k-2} - q_k x_{k-1})}_{\in \mathbb{Z}} \cdot a + \underbrace{(y_{k-2} - q_k y_{k-1})}_{\in \mathbb{Z}} \cdot b$$
Tehát az utolsó $r_k \neq 0$ is felírható → $r_n = (a;b)$ is felírható. QED.

Összegezve: a lnko létezik, lényegében egyértelmű, a két def. ekvivalens (ha $\neg(a = 0 = b)$), meghatározható az eukl. algoritmussal és felírható a 2 szám lineáris kombinációjaként.

Prímszámok és felbonthatatlan számok

Def. Ha a 0-tól és egységtől különböző egész szám és $a = bc$ $(b, c \in \mathbb{Z})$-ből következik, hogy b és c közül az egyik egység, a másik a asszociáltja,
(átfogalmazás: a osztói az egységek és az asszociáltjai)
(átfogalmazás: a-nak csak triviális felbontása van)
akkor a-t felbonthatatlan számnak nevezzük.

Def. Ha p 0-tól és egységtől különböző egész és $p \mid bc \Rightarrow p \mid b \vee p \mid c$, akkor p prímszám.

Tétel. Ha p prím, akkor felbonthatatlan is $(p \in \mathbb{Z})$.
(ez nem csak egészekre igaz, hanem minden normális számkörben és általánosításban is)

B: $p = ab$ (1)
$\Rightarrow p \mid ab \Rightarrow p \mid a \vee p \mid b$.
Tfh. $p \mid a$. Másrészt $(1) \Rightarrow a \mid p$.
Tehát a és p asszociáltak: $a = p\varepsilon$ $/ \cdot b$
$\Rightarrow ab = p \varepsilon b$ $/ : p$
(1) $1 = \varepsilon b \Rightarrow b \mid 1 \Rightarrow b = \pm 1$ egység.
Q E D.

Tétel. Ha p felbonthatatlan, akkor p prím. $(p \in \mathbb{Z}\ !)$

B: $p \mid ab$
p felbonthatatlan $\Rightarrow$ osztói $1, p$ és asszociáltjaik
$(p, a) = \begin{cases} 1 \\ p \end{cases}$
$p \Rightarrow p \mid a \rightarrow$ kész ✓
$1 \Rightarrow 1 = xa + yp$ $/ \cdot b$
$b = x\underbrace{ab}_{p\mid} + y\underbrace{bp}_{p\mid} \Rightarrow p \mid b$ ✓
Q E D.

Következmény. p prím $\Leftrightarrow$ p felbonthatatlan $(p \in \mathbb{Z})$.

A SzAT-hoz kell, hogy ugyanazok legyenek. Ehhez kell, hogy a lin. komb. megjelenjen, tehát kell eukl. algoritmus, tehát kell maradékos osztás.

A számelmélet alaptétele és következményei

Tétel (számelmélet alaptétele, fundamental theorem of arithmetics)
Ha $a \neq 0$ és nem egység, akkor felbontható prímszámok / felbonthatatlan számok szorzatára, és ez a felírás tényezőiben (a tényezők sorrendjétől és egységtényezőktől eltekintve) egyértelmű.

B: 1) A felbonthatóság bizonyítása

Lemma: $a \neq 0$, $a = bc$ és b, c egyike sem egység, akkor $|b| < |a|$.

B: $a \neq 0 \Rightarrow b, c \neq 0$

$a = bc \Rightarrow \frac{a}{c} = b \Rightarrow \left|\frac{a}{c}\right| = \frac{|a|}{|c|} = |b|$ $\quad c \neq 0, \pm 1 \Rightarrow |c| \geq 2$

$\frac{|a|}{|c|} \leq \frac{|a|}{2} < |a| \Rightarrow |b| < |a|$. — L

Teljes indukció $|a|$ szerint.

$a \neq 0, \pm 1 \Rightarrow |a| \geq 2$

$|a| = 2 \rightarrow a = \pm 2$ felbonthatatlan szám (HF) → 2 osztói lehetnek: $-2, -1, 0, 1, 2 \rightarrow \pm 2, \pm 1$ (Lemma miatt) per def igaz ✓

→ az a felbonthatatlan számok 1 tényezős szorzata ✓

Tfh. $n \in \mathbb{N}$, $n \geq 3$, n-nél kisebbekre igaz. Megmutatjuk, hogy $|a| = n$-re is.

Ha a felbonthatatlan ⇒ 1 tényezős szorzat, kész ✓

Ha a nem felbonthatatlan ⇒ $a = bc$ nemtriv felbontás

Lemma ⇒ $|b| < |a| = n$. és $|c| < |a| = n$.

⇒ indukciós feltevés alapján b és c felírhatók: $b = p_1 p_2 \cdots p_k$, $c = q_1 q_2 \cdots q_\ell$ } p_i, q_j felbontha-tatlan

$a = bc = (p_1 \cdots p_k)(q_1 \cdots q_\ell) = p_1 \cdots p_k q_1 \cdots q_\ell$ kívánt felbontás — I

2) Az egyértelműség bizonyítása

Tfh. $n = p_1 \cdots p_r = q_1 \cdots q_s$, ahol p_i, q_j prímek. $r \leq s$.

$\Rightarrow p_1 \mid n = q_1 \cdots q_s \Rightarrow p_1 \mid q_1 \cdot (q_2 \cdots q_s) \Rightarrow p_1 \mid q_1 \vee p_1 \mid (q_2 \cdots q_s)$

Ha $p_1 \mid q_1 \Rightarrow q_1 = \varepsilon p_1$, különben p_1 valódi osztója lenne q_1-nek, ami prím.

Ha $p_1 \mid q_2 q_3 \cdots q_s \Rightarrow p_1 \mid q_2 \vee p_1 \mid (q_3 \cdots q_s)$ ...

S.i.t. (t.i.) ⇒ véges sok lépésben véget érő eljárás.

$\exists q_j = p_1 \cdot \varepsilon$. Feltehető, hogy $j = 1$: $q_1 = \varepsilon_1 p_1$.

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = \varepsilon_1 p_1 \cdot q_2 \cdot \ldots \cdot q_s \quad / : p_1$

$p_2 \cdot \ldots \cdot p_r = \varepsilon_1 \cdot q_2 \cdot \ldots \cdot q_s$

Ugyanolyan típusú, mint az eredeti → folytatjuk az eljárást. feltehető, hogy $q_2 = \varepsilon_2 p_2$

$p_2 p_3 \cdots p_r = \varepsilon_1 \varepsilon_2 p_2 q_3 \cdots q_s$

S.i.t. ↘

$1 = \underbrace{\varepsilon_1 \cdot \ldots \cdot \varepsilon_r}_{\text{egység}} \cdot q_{r+1} \cdot \ldots \cdot q_s$

Ha $s > r \rightarrow q_{r+1} \mid 1$ ↯ nem lehet prím és egység.

$\Rightarrow s = r$, $p_i = \varepsilon_i q_i$ $\forall i = 1, \ldots, r$ Tehát tényezőben egyértelmű. — II

□

2014. szeptember 30.
kedd

Tétel. Minden 0-tól és ±1-től különböző $n \in \mathbb{Z}$ felírható $n = \pm q_1^{\alpha_1} \dots q_r^{\alpha_r}$ (1), ahol $q_1^{\alpha_1}, \dots, q_r^{\alpha_r}$ prímhatványok. A felbontás a $q_1^{\alpha_1}, \dots, q_r^{\alpha_r}$ sorrendjétől eltekintve egyértelmű.
($q_1, \dots, q_r$ különböző pozitív prímek)
($\alpha_1, \dots, \alpha_r$ pozitív egészek)

B: felbonthatóság az alaptételből triviális
egyértelműség következik az alaptétel egyértelműség részéből. (HF) □

Def. $n \in \mathbb{Z}$, $n \neq 0, \pm 1$ egy (1) előállítását n kanonikus alakjának nevezzük.

Tétel. $n \in \mathbb{Z}$, $n \neq 0, \pm 1$, n kanonikus alakja $n = \pm p_1^{\alpha_1} \dots p_r^{\alpha_r}$, akkor $d \in \mathbb{Z}$-re
$d \mid n \iff d = \pm p_1^{\beta_1} \dots p_r^{\beta_r}$, ahol $\forall i = 1, \dots, r \quad \{\alpha_i, \dots, 1, 0\} \ni \beta_i$. (ez nem d kan. alakja).

B: Következik a kanonikus alak létezéséből és egyértelműségéből. (HF) □

Tétel. Ha $a, b \in \mathbb{Z}$, $a, b \neq 0$, és $a = \pm p_1^{\alpha_1} \dots p_r^{\alpha_r}$ és $b = \pm p_1^{\beta_1} \dots p_r^{\beta_r}$ alakban felírhatók (nem kanonikus alak), ahol $p_1, \dots, p_r$ különböző pozitív prímek, $\alpha_1, \dots, \alpha_r$ és $\beta_1, \dots, \beta_r$ nemnegatív egészek, akkor

$$(a; b) = \pm \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}.$$

B: Következik az előző tételből (HF).

Def. Ha $a, b \in \mathbb{Z}$ és $\exists C \in \mathbb{Z}$; $a \mid C \wedge b \mid C$ és $a \mid c \wedge b \mid c \Rightarrow C \mid c$,
akkor C-t az a és b legkisebb közös többszörösének nevezzük.
$[a; b] = C$

Tétel. Bármely $a, b \in \mathbb{Z}$ $\exists [a; b]$ és előjeltől eltekintve egyértelmű,
továbbá $(a; b) \cdot [a; b] = \pm ab$.

Tétel. $\forall a, b \in \mathbb{Z}$, $a, b \neq 0$ előállítható mint fent $\rightarrow [a; b] = \pm \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$.
Ha $a = 0 \rightarrow [0, b] = 0$.

Bi: HF. □

Számelméleti függvények

Definíció. Számelméleti függvényen olyan függvényt értünk, melynek értelmezési tartománya $\mathbb{N}$.

Definíció. Ha az $f(n)$ számelméleti fgv.-re $(m;n) = 1$ esetén

(1) $f(m \cdot n) = f(m) \cdot f(n)$,

akkor $f(n)$-et multiplikatív sze. függvénynek nevezzük.

Ha (1) $\forall m, n \in \mathbb{N}$-re teljesül, akkor $f(n)$ totálisan /szigorúan/ szűkebb értelemben multipl.

Definíció. Ha a $g(n)$ sze. fgv.-re $(m;n) = 1$ esetén

(2) $g(m \cdot n) = g(m) + g(n)$

teljesül, akkor $g(n)$-t additív számelméleti függvénynek mondjuk.

Ha (2) $\forall m, n$-re teljesül, akkor $g(n)$ totálisan additív.

Turán a totálist használta, angolul a completely a standard megnevezés.

Példa:

$$\left.\begin{array}{ll} f(n) = 0 & \\ f(n) = 1 & \\ f(n) = n^c & c \in \mathbb{R} \end{array}\right\} \text{(totálisan) multiplikatív} \qquad \left.\begin{array}{ll} g(n) = 0 & \\ g(n) = c \log n & c \in \mathbb{R} \end{array}\right\} \text{(totálisan) additív}$$

Tétel. a) Ha $g(n)$ tetszőleges additív sze. fgv., akkor az $f(n) = e^{g(n)}$ sze. fv. multiplikatív.

b) Ha $\varphi(n)$ tetszőleges multipl. sze. fv., amire $\forall n$ $\varphi(n) > 0$, akkor a $\psi(n) = \log \varphi(n)$ sze. fv. additív.

B: a) $(m;n) = 1$

$$\left.\begin{array}{l} f(m \cdot n) = e^{g(m \cdot n)} = e^{g(m) + g(n)} = e^{g(m)} \cdot e^{g(n)} \\ f(m) f(n) = e^{g(m)} \cdot e^{g(n)} \end{array}\right\} \ominus$$

$\boxed{a}$

b) $(m;n) = 1$

$$\left.\begin{array}{l} \psi\, g(m \cdot n) = \log \varphi(mn) = \log(\varphi(m) \cdot \varphi(n)) = \log \varphi(m) + \log \varphi(n) \\ \psi(m) + \psi(n) = \log(\varphi(m)) + \log((\varphi(n))) \end{array}\right\} \ominus$$

$\boxed{b}$

$\square$

Tétel. a) Ha $f(n) \not\equiv 0$ multipl. sze. fv., akkor $f(1) = 1$

b) Ha $g(n)$ additív sze. fv., akkor $g(1) = 0$

B: a) $f(n) \not\equiv 0 \Rightarrow \exists m: f(m) \neq 0$

$f(m) = f(1 \cdot m) = f(1) \cdot f(m) \Rightarrow f(m) \cdot (1 - f(1)) = 0 \quad /: f(m) \neq 0$

$1 - f(1) = 0 \Rightarrow f(1) = 1$ $\boxed{a}$

b) Ugyanígy. $\boxed{b}$

$\square$

Tétel. $n > 1$, n kan. alakja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

a) Ha $f(n)$ multiplikatív, akkor $f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i})$.

b) Ha $f(n)$ tot. mult., akkor

$$f(n) = \prod_{i=1}^{r} f(p_i)^{\alpha_i}$$

c) Ha $g(n)$ additív, akkor $g(n) = \sum_{i=1}^{r} g(p_i^{\alpha_i})$

d) Ha $g(n)$ tot. additív, akkor

$$g(n) = \sum_{i=1}^{r} g(p_i) \cdot \alpha_i .$$

Következmény. Multiplikatív, ill. additív fgv. értékét a prímhatvány helyen vett értékek, tot. mult, ill. tot. add. fgv. értékét a prím helyen vett értékek egyértelműen meghatározzák.

B: a) $f(n) = f(p_1^{\alpha_1} \cdot (p_2^{\alpha_2} \cdots p_r^{\alpha_r})) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}(p_3^{\alpha_3} \cdots p_r^{\alpha_r})) \overset{t.i.}{=} \prod f(p_i^{\alpha_i})$ $\boxed{a}$

b) $f(p_i^{\alpha_i}) = f(p_i) \cdot f(p_i^{\alpha_i - 1}) \overset{t.i.}{=} f(p_i)^{\alpha_i} \rightarrow$ a)-val $\boxed{b}$

c) $g(n) = g(p_1^{\alpha_1}(p_2^{\alpha_2} \cdots p_r^{\alpha_r})) = g(p_1^{\alpha_1}) + g(p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \overset{t.i.}{=} \sum g(p_i^{\alpha_i})$ $\boxed{c}$

d) $g(p_i^{\alpha_i}) = g(p_i) + g(p_i^{\alpha_i - 1}) \overset{t.t.}{=} \alpha_i\, g(p_i) \rightarrow$ c)-vel $\boxed{d}$

$\square$

Tétel. a) Multiplikatív függvények szorzata multiplikatív.
b) Additív függvények összege additív.

B: a) $f(n)$, $g(n)$ mult., $h(n) = f(n)\,g(n)$ ne. fv.
$(m,n) = 1$ $\quad h(mn) = f(mn)\cdot g(mn) = (f(m)\,f(n))(g(m)\,g(n)) =$
$= f(m)\,g(m)\cdot f(n)\,g(n) =$
$= h(m)\cdot h(n)$ □

b) Ugyanilyen. □

Definíció. Legyen $\omega(n) = \begin{cases} 0, & \text{ha } n = 1 \\ r, & \text{ha } n = p_1^{\alpha_1}\cdots p_r^{\alpha_r} \text{ kan. alak.} \end{cases}$

(A különböző prímosztók száma.)

Definíció. Legyen $\Omega(n) = \begin{cases} 0, & \text{ha } n = 1 \\ \sum \alpha_i, & \text{ha } n = p_1^{\alpha_1}\cdots p_r^{\alpha_r} \text{ kan. alak.} \end{cases}$

(A multiplicitással számított prímosztók száma)

A jelölés nem teljesen egységes (ω: K, P szócsa volt régen), ma ez standard.

Tétel. $\omega(n)$ additív, $\Omega(n)$ totálisan additív.

B: HF □

Definíció. Legyen $f(n)$ tetsz. legyen számelméleti fv.
Legyenek $n \in \mathbb{N}$ pozitív osztói $(1 =)\ d_1 < d_2 < \dots < d_t (= n)$.
Ekkor a $\sum_{i=1}^{t} f(d_i)$ összeget $\sum_{d\mid n} f(d)$ -vel jelöljük, $\prod_{i=1}^{t} f(d_i) = \prod_{d\mid n} f(d)$.

A $\sum_{d\mid n} f(d)$ függvényt az f függvény összegzési függvényének nevezzük.

Tétel. Multiplikatív ne. fv. összegzési fv.-e is multiplikatív.

B: Legyen $f(n)$ multiplikatív, legyen $g(n) = \sum_{d\mid n} f(d)$.
Ha $f(n) \equiv 0 \Rightarrow g(n) \equiv 0$ mult. ✓
Ha $f(n) \not\equiv 0$: elég igazolni, hogy $g(1) = 1$ és
$n > 1$, n kan. al. $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ $\quad g(n) = g(p_1^{\alpha_1}\cdots p_r^{\alpha_r}) = \prod_{i=1}^{r} g(p_i^{\alpha_i})$,
mert ebből következik a multiplikativitás (HF).

$$g(1) = \sum_{d\mid 1} f(d) = f(1) = 1 \quad ✓$$

$$g(n) = g\left(p_1^{\alpha_1}\cdots p_r^{\alpha_r}\right) = \sum_{d\mid p_1^{\alpha_1}\cdots p_r^{\alpha_r}} f(d) = \sum_{\beta_1=0}^{\alpha_1}\sum_{\beta_2=0}^{\alpha_2}\cdots\sum_{\beta_r=0}^{\alpha_r} f\left(p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}\right) =$$

$$= \sum_{\beta_1=0}^{\alpha_1}\sum_{\beta_2=0}^{\alpha_2}\cdots\sum_{\beta_r=0}^{\alpha_r} f\left(p_1^{\beta_1}\right)\cdot f\left(p_2^{\beta_2}\right)\cdots f\left(p_r^{\beta_r}\right) = \prod_{i=1}^{r}\sum_{\beta_i=0}^{\alpha_r} f\left(p_i^{\beta_i}\right) =$$

$$= \prod_{i=1}^{r}\sum_{d\mid p_i^{\alpha_i}} f(d) = \prod_{i=1}^{r} g\left(p_i^{\alpha_i}\right) \quad ✓$$

□

Definíció. Az $n \in \mathbb{N}$ szám pozitív osztóinak száma $d(n)$ vagy $\tau(n)$,
összege $\sigma(n)$ (másképp $\sigma'(n)$).

Tétel. A $d(n)$ függvény multiplikatív, és $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ k.a.
$\Rightarrow d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$.

B: $d(n) = \sum_{d \mid n} 1$, tehát $d(n)$ az azonosan 1 sze. fv. összegzési fv.-e.

Az 1 multiplikatív $\Rightarrow$ $d(n)$ is multipl. ✓

$\Rightarrow d(n) = \prod_{i=1}^{r} d(p_i^{\alpha_i})$

$d(p_i^{\alpha_i}) = \alpha_i + 1$, mert osztói $1, p_i, \dots, p_i^{\alpha_i}$: $\alpha_i + 1$ db

$\Rightarrow d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$. □

Tétel. A $\sigma(n)$ fv. multiplikatív, és $n = \prod p_i^{\alpha_i}$ -re $\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$.

B: $\sigma(n) = \sum_{d \mid n} d$, tehát $\sigma(n)$ összegzési fv.-e az $f(n) = n$ fv.-nek, ami (totálisan) multiplikatív $\Rightarrow$ $\sigma(n)$ is multipl.:

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}) = \prod_{i=1}^{r} \sum_{d \mid p^{\alpha_i}} d = \prod_{i=1}^{r} \sum_{j=0}^{\alpha_i} p^j = \prod_{i=1}^{r} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}.$$ □

2014. 10. 07. kedd

Definíció. Ha valamely $n \in \mathbb{N}$ számra $\sigma(n) = 2n$,
akkor n egyenlő a nála kisebb osztóinak összegével,
akkor n-et tökéletes számnak mondjuk.

Pl. $\sigma(6) = 12$ $\rightarrow$ a 6 tökéletes.

Tétel. (Euklidesz) Ha p prím és $2^p - 1$ is prím (Mersenne-féle prím),
akkor $(2^p - 1) \cdot 2^{p-1}$ tökéletes szám.

Pl. $p = 2$ $\quad 2^p - 1 = 3$ $\quad \rightarrow \quad (2^p - 1) \cdot 2^{p-1} = 3 \cdot 2 = 6$

B: $\sigma\left(\underbrace{2^{p-1} \cdot (2^p - 1)}_{\text{rel. prímek}}\right) = \sigma(2^{p-1}) \cdot \sigma(2^p - 1) = \frac{2^p - 1}{2 - 1} \cdot (2^p - 1 + 1) = 2 \cdot (2^p - 1) \cdot 2^{p-1}$ ✓
Tehát def. szerint tök. szám. □

... Nem tudjuk, hogy van-e ∞ sok Mersenne-prím. Belátható időn belül nem biz.-ható.

Tétel. (Euler) Ha egy páros szám tökéletes szám, akkor szükségképpen
$2^{p-1} \cdot (2^p - 1)$ alakú, ahol p és $2^p - 1$ is prím.

B: Az előadáson nem bizonyítjuk, de elemien lejön.

Probléma. Nem tudjuk, hogy létezik-e páratlan tökéletes szám.
Valószínűleg nincsenek. Ismert, hogy ha legalább 7 prímosztója van,
nem lehet.

Ha van is ∞ sok, akkor is x-ig $o(x)$ van csak.

Definíció. $n = 1, 2, \dots$ esetén az $1 \le a \le n$, $(a, n) = 1$ feltételeket kielégítő a egész számok számát $\varphi(n)$-nel jelöljük. → Euler-féle φ-fgv.

Tétel. A $\varphi(n)$ függvény multiplikatív.

B. Később, még ebben a félévben.

Tétel. Ha $n > 1$ és n kanonikus alakja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, akkor

$$\varphi(n) = \left(\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \right) \cdot n = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right). \qquad \varphi(1) = 1.$$

B. Multiplikatív → elég $\varphi(p^\alpha)$-t kiszámolni $(1 \le a \le p^\alpha)$.
$(a, p^\alpha) = 1 \iff (a, p) = 1. \iff p \nmid a.$ ⇒ csak p többszörösei rosszak.
→ $p, 2p, \dots, p^{\alpha-1} \cdot p$ a rosszak

$$\Rightarrow \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

$$\Rightarrow \varphi(n) = \prod_{p \mid n} \varphi(p^\alpha) = \prod_{p \mid n} p^\alpha \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \qquad \square$$

Definíció. Legyen $n \in \mathbb{N}$. Ha nincs olyan $d > 1$, $d \in \mathbb{N}$, akkor n-et négyzetmentes számnak nevezzük.
(Azaz a kanonikus alakban $\forall$ kitevő pontosan 1.)
vagy $n = 1$.

Definíció. Legyen

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1 \\ (-1)^k, & \text{ha } n \text{ négyzetmentes és } n = p_1 p_2 \cdots p_k \text{ (különböző prímek)} \\ 0, & \text{ha } n \text{ nem négyzetmentes. } (\iff \exists\, d > 1 : d^2 \mid n) \end{cases}$$

Az így definiált $\mu(n)$ függvényt Möbius-függvénynek nevezzük.

Tétel. A $\mu(n)$ függvény multiplikatív.

B: $(m, n) = 1$
1) m és n is négyzetmentes

Tétel. A Möbius-függvény összegzési függvénye $M(n) = \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ha } n=1 \\ 0, & \text{ha } n>1 \end{cases}$.

(Itt $M(n)$ nem standard jelölés.)

B: $\mu(n)$ mult. $\Rightarrow$ $M(n)$ is multiplikatív. $\rightarrow$ elég prímhatványokra.

$$M(p^\alpha) = \sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^\alpha) =$$

$$= 1 + (-1) + 0 + \ldots + 0 = 0 \qquad (\alpha \geq 1)$$

$$M\left(\prod_{p|n} p^\alpha\right) = \prod_{p|n} M(p^\alpha) = \prod_{p|n} 0 = 0 \qquad (n > 1)$$

$$M(1) = \sum_{d|1} \mu(d) = \mu(1) = 1 \qquad (n = 1) \qquad \square$$

Def. Ha $g(n)$ számelméleti fv. összegzési fv.-e az $f(n)$ sze. fv.-nek, akkor $f(n)$ megfordítási függvénye $g(n)$-nek.

Tétel. (Möbius-féle inverziós formula) Bármely $g(n)$ sze. fv.-nek 1 és csak 1 $f(n)$ megfordítási fv.-e van, és ez a következő formulával számítható:

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right).$$

B: Nem bizonyítjuk. (Van elemi biz., de inkább analízis szükséges felhasználásával.)

Tétel: Multiplikatív fv. megfordítási fv.-e is az.

B: Nem bizonyítjuk.

Az $f(n)$ hogyan változik n függvényében?

$d(n) = 1 \rightarrow$ csak $n = 1$

$d(n) = 2 \rightarrow$ akkor, ha n prím (∞ sok helyen)

$n = 2^k \rightarrow d(n) = k+1 \rightarrow k = \log n / \log 2.$

$d(n) = \frac{1}{\log 2} \cdot \log n + 1 > \log 2 * \log n \rightarrow$ konstanssszor $\log n$

$n = 2^k 3^k \rightarrow d(n) = \left(\frac{\log n}{\log 6} + 1\right)^2 > \left(\frac{1}{\log 6}\right)^2 \cdot \log^2 n$

$\Rightarrow$ bmely fix ε-ra $d(n) > (\log n)^\varepsilon$ ∞ sok n-re

$\Rightarrow$ a függvény „ugrál": ∞ sokszor 2, ∞ sokszor „nagy".

Dirichlet: Általában egy $f(n)$ sze. fv. átlagértéke „simább", nem ugrál „úgy, mint f értékei.

Dirichlet-féle osztóprobléma: $\frac{1}{N} \sum_{n=1}^{N} d(n)$ becslése.

Tétel. $\Rightarrow \left| \sum_{n=1}^{N} d(n) - N \log N \right| < 2N$

$\left(\Rightarrow \left| \text{átlagérték} - \log N \right| < 2 \rightarrow \text{az átl. érték } \log N\text{-nel becsülhető} \rightarrow \text{nagyon sima.} \right)$

B. Tekintsük a következő $N \times N$-es mátrixot

	1	2	3	...	i	...	N
1	1	0	0	...			
2	1	1	0	...			
3	1	0	1	...			
⋮	⋮	⋮	⋮				
k	1				□		
⋮	⋮	⋮	⋮				
N	1						

□ → $\begin{cases} 1, \text{ha } i \mid k \\ 0, \text{ha } i \nmid k \end{cases}$

Két féle összeszámolás.

1) A k-adik sorban lévő 1-ek összege:

$$\sum_{i \mid k} 1 = d(k)$$

Sorok mentén összegezve:

$$\sum_{k=1}^{N} d(k)$$

2) Az i-edik oszlopban lévő 1-ek összege: az i-nek N-nél nem nagyobb többszörösei száma: $\left[\frac{N}{i}\right]$

Oszlopok mentén összegezve:

$$\sum_{i=1}^{N} \left[\frac{N}{i}\right]$$

$$\Rightarrow \sum_{k=1}^{N} d(k) = \sum_{i=1}^{N} \left[\frac{N}{i}\right]$$

Kellemetlen dolog: egészrész.

Megpróbáljuk, mekkora hibát ad az elhagyásra

$$\sum_{i=1}^{N} \left[\frac{N}{i}\right] = \sum_{i=1}^{N} \frac{N}{i} + \sum_{i=1}^{N} \left(\left[\frac{N}{i}\right] - \frac{N}{i} \right)$$

$$\sum_{k=1}^{N} d(k) - N \sum_{i=1}^{N} \frac{1}{i} = \sum_{i=1}^{N} \left(\left[\frac{N}{i}\right] - \frac{N}{i} \right)$$

$$(1): \left| \sum_{k=1}^{N} d(k) - N \sum_{i=1}^{N} \frac{1}{i} \right| = \left| \sum_{i=1}^{N} \left(\left[\frac{N}{i}\right] - \frac{N}{i} \right) \right| \leq \sum_{i=1}^{N} \left| \left[\frac{N}{i}\right] - \frac{N}{i} \right| < \sum_{i=1}^{N} 1 = N$$

Ismeretes, hogy $\log N < \sum_{i=1}^{N} \frac{1}{i} < 1 + \log N$ ($\frac{1}{x}$ alsó / felső int.-közelítés)

$$\left| \sum_{i=1}^{N} \frac{1}{i} - \log N \right| < 1$$

$$(2): \left| N \sum_{i=1}^{N} \frac{1}{i} - N \log N \right| < N$$

$$(1) \wedge (2): \left| \sum d(n) - N \log N \right| = \left| \left(\sum d(n) - N \sum_{i=1}^{N} \frac{1}{i} \right) + \left(N \sum_{i=1}^{N} \frac{1}{i} - N \log N \right) \right| \leq$$

$$\leq \left| \sum_{n=1}^{N} d(n) - N \sum_{i=1}^{N} \frac{1}{i} \right| + \left| N \sum_{i=1}^{N} \frac{1}{i} - N \log N \right| < 2N \qquad \square$$

Tehát $\sum d(n) \sim N \log N$. Megmutatható: $\left| \sum d(n) - N \log N + c_1 N \right| < c_2 \sqrt{N}$

Kongruenciák

Definíció. Legyen $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Ha $m \mid a-b$, akkor azt mondjuk, hogy a kongruens b-vel modulo m.

Jelölés: $a \equiv b \pmod{m}$

$a \equiv b \ (m)$

Az így definiált relációt kongruenciarelációnak nevezzük.

Ha $m \nmid a-b \rightarrow a \not\equiv b \ (m)$, a inkongruens b-vel mod m.

Tétel. $a \equiv b \ (m) \iff a$ és b m-mel osztva ugyanazon maradékot adják.

B: 1) $\Leftarrow$

$$\left.\begin{aligned} a &= q_1 m + r_1 \\ b &= q_2 m + r_1 \end{aligned}\right\} \Rightarrow a - b = m \cdot (q_1 - q_2) + 0$$

$$\Rightarrow m \mid (a-b) \quad \checkmark$$

2) $\Rightarrow$

$$\left.\begin{aligned} a &= q_1 m + r_1 \quad 0 \le r_1 < m \\ b &= q_2 m + r_2 \quad 0 \le r_2 < m \end{aligned}\right\}$$

$$m \mid (a-b) = (q_1 - q_2) \cdot m + (r_1 - r_2) \Rightarrow m \mid r_1 - r_2 \quad -m < r_1 - r_2 < m$$

$$\Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \quad \checkmark \qquad \square$$

2014. 10. 14.

Tétel. A kongruenciareláció a) reflexív
b) szimmetrikus
c) tranzitív.

B: c)

$$\left.\begin{aligned} a &\equiv b \ (m) \\ b &\equiv c \ (m) \end{aligned}\right\} \Rightarrow a \equiv c \ (m)$$

$$\left.\begin{aligned} m \mid a-b \\ m \mid b-c \end{aligned}\right\} \Rightarrow m \mid (a-b) + (b-c) = a-c \qquad \square$$

Definíció. Ha egy S reláció reflexív, szimmetrikus és tranzitív, akkor ekvivalenciarelációnak nevezzük.

Pl. $\mathbb{N}$-ben $=$ ekvivalenciareláció

$\mathbb{N}$-ben $<$ nem reflexív és nem szimetrikus, sőt antiszimetrikus, tranzitív

$\mathbb{N}$-ben $\mid$ reflexív, nem szimmetrikus, tranzitív

Tétel. A kongruenciareláció ekvivalenciareláció.

B: Az előző tétel szerint. $\square$

Tétel. Ha S valamely H halmazon definiált ekvivalenciareláció, akkor H egyértelműen felírható páronként közös elem nélküli részhalmazok, ún. ekvivalenciaosztályok egyesítéseként úgy, hogy $H \ni \xi, \ell$ akkor és csak akkor essék ugyanabba a részhalmazba (ekv. osztályba), ha ekvivalensek, vagyis kielégítik a relációt, azaz $(k; \ell) \in S$.

B: Nem bizonyítjuk.

Következmény. $\mathbb{Z}$ diszjunkt részhalmazokra (ekvivalenciaosztályokra) osztható úgy, hogy 2 egész szám akkor tartozik ugyanabba a részhalmazba, ha kongruensek egy adott számmal modulo m, más szóval korábbi tétel szerint m-mel osztva ugyanazt a maradékot adják.

Definíció. Ezeket az ekvivalenciaosztályokat modulo m maradékosztályoknak nevezzük. Az $a \in \mathbb{Z}$-t tartalmazó maradékosztályt a által reprezentált maradékosztálynak nevezzük, az a-t pedig e maradékosztály reprezentáns elemének mondjuk.

Tétel. A mod m maradékosztályok száma m.

B: m-mel osztva a lehetséges maradékok: $0, 1, \dots, m-1$ $\longrightarrow$ ezek száma m. Annyi marad, ahány maradék. □

Tétel. $a \equiv b \ (m)$, $c \equiv d \ (m) \Rightarrow a+c \equiv b+d \ (m)$ (a kongruenciák összeadhatók).
(Speciálisan $c=d$-re: $a+c \equiv b+c \ (m) \rightarrow$ ugyanaz a szám hozzá is adható.)

B: $\left.\begin{array}{l} m \mid b-a \\ m \mid d-c \end{array}\right\} \longrightarrow m \mid (b-a)+(d-c) = (b+d)-(a+c)$ □

Tétel. $a \equiv b \ (m)$, $c \equiv d \ (m) \Rightarrow ac \equiv bd \ (m)$ (a kongruenciák összeszorozhatók, mindkét oldal szorozható ugyanazzal a számmal is)

B
$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= c\underbrace{(a-b)} + b\underbrace{(c-d)} \\ &\qquad m \mid \qquad\quad m \mid \end{aligned} \Rightarrow m \mid ac - bd$$ □

Következmény. $a \equiv b \ (m) \Rightarrow a^k \equiv b^k \ (m) \quad (\forall k \in \mathbb{N})$ (a kongruenciák hatványozhatók)

Következmény. $m \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$: $f(x) = a_n x^n + \dots + a_1 x + a_0$
$k \equiv l \ (m) \Rightarrow f(k) \equiv f(l) \ (m)$

B:
$$\begin{array}{lll} 1 \equiv 1 \ (m) & \xrightarrow{\cdot a_0} & a_0 \equiv a_0 \ (m) \\ k \equiv l \ (m) & \xrightarrow{\cdot a_1} & a_1 k \equiv a_1 l \ (m) \\ k^2 \equiv l^2 \ (m) & \xrightarrow{\cdot a_2} & a_2 k^2 \equiv a_2 l^2 \ (m) \\ \vdots & & \vdots \\ k^n \equiv l^n \ (m) & \xrightarrow{\cdot a_n} & a_n k^n \equiv a_n l^n \ (m) \\ \hline & & f(k) \equiv f(l) \ (m) \end{array}$$ □

Tétel. $ac \equiv bc \ (m) \Leftrightarrow a \equiv b \ \left(m/(m;c)\right)$

B:
1) $\Leftarrow$ $a \equiv b \ \left(\frac{m}{(m;c)}\right)$: $\frac{m}{(m;c)} \mid a-b \Rightarrow m \mid (m;c)\cdot(a-b) = (m;c)a - (m;c)b$

$\Rightarrow (m;c)\,a \equiv (m;c)\,b \ (m) \quad / \cdot \frac{c}{(m;c)} \ (\in \mathbb{Z})$

$ac \equiv bc \ (m)$ ✓

2) $\Rightarrow$ $ac \equiv bc \ (m)$ $\quad m \mid ac - bc = c(a-b)$

$\frac{m}{(m;c)} \mid \frac{c}{(m;c)}(a-b)$

↳ relatív prímek per def. $\Rightarrow \frac{m}{(m;c)} \mid a-b$

$\Rightarrow a \equiv b \ \left(\frac{m}{(m;c)}\right)$ ✓

Felhasználjuk, hogy $x \mid yz \ \wedge \ (x;y)=1 \Rightarrow x \mid z$. (HF) □

Következmény. $ca \equiv bc \ (m) \ \wedge \ (m;c) = 1 \ \Rightarrow \ a \equiv b \ (m)$

Jelölés. Az a által reprezentált maradékosztály fix modulusra: (a).
(Más változat: $\overline{a}$)

Definíció. Legyen $m \in \mathbb{N}$ adott modulus. $(a), (b)$ modulo m maradékosztályok.
a) $(a) + (b) \overset{def}{=} (a + b)$
b) $(a) \cdot (b) \overset{def}{=} (a \cdot b)$

Ezek a definíciók értelmesek. $a' \equiv a, \ b' \equiv b \ \rightarrow \ a' + b' \equiv a + b,$
$a' \cdot b' \equiv a \cdot b$.

Tehát a reprezentálás módjától a mo.-k függetlenek a def.-ben.

Tétel. A mod m maradékosztályok $+$-ra és $\cdot$-ra nézve (kommutatív, egységelemes), de összetett m esetén nem nullosztómentes) gyűrűt alkotnak.

B: $(a) + (b) = (a + b) = (b + a) = (b) + (a)$
$\rightarrow$ ugyanúgy $+, \cdot$ komm., asszociatív, van 0, van ellentett, disztrib.
$0: (0)$
$1: (1)$
$-(a): (-a)$ $\longrightarrow$ komm., egységelemes gyűrű

$m = ab, \quad 1 < a, b < m$
$(a)(b) = (ab) = (m) = (0) \ \rightarrow$ nem nullosztómentes

Ha m prím $\rightarrow$ később. $\square$

Definíció. Ha bizonyos $a_1, \dots, a_k \in \mathbb{Z}$ olyanok, hogy páronként különböző mod m mo.-kat reprezentálnak, ~~akkor~~ másrészt valamennyi mod m mo.-t reprezentálja ezek valamelyike ($\Rightarrow k = m$), akkor azt mondjuk, hogy $a_1, \dots, a_k$ teljes maradékrendszert alkotnak mod m.

Tétel. Bizonyos egész számok acsa. alkotnak teljes m.r.-t mod m, ha
a) páronként inkongruensek mod m;
b) számuk m.

B: HF (def-ből következik)

Tétel. ~~Bizonyos~~ Ha az $a_1, \dots, a_m$ számok t. m.r. mod m, továbbá $b, c \in \mathbb{Z}$, $(b; m) = 1$, akkor $ba_1 + c; \ ba_2 + c; \dots; ba_m + c$ is teljes m.r. mod m.

B: Elég belátni, hogy az előző tétel 2 feltétele teljesül.
b) nyilvánvaló.
a) $\lightning$ $i \neq j$, $ba_i + c \equiv ba_j + c \ (m)$
$ba_i \equiv ba_j \ (m) \quad (b; m) = 1$
$a_i \equiv a_j \ (m) \ \lightning$ $\square$

A relatív prímség amúgy szükséges is, nemcsak elégséges.

Tétel. $a \equiv b \pmod m \Rightarrow (a;m) = (b;m)$

B: $m \mid a-b \Rightarrow \exists t \in \mathbb{Z} : a-b = mt \Rightarrow b = a - mt$,
$a = b + mt$

$\Rightarrow (a;m) \mid b$, mert ugyis a-t és m-et is. $\Rightarrow (a;m) \mid (b;m)$, mert
$(b;m) \mid a \rightarrow (b;m) \mid (a;m)$ $(a;m) \mid m$ és $(a;m) \mid b$.

$\Rightarrow (a;m) = (b;m)$ (egymásnak osztói egyéig). □

Definíció. Ha valamely (a) mod m mo. elemeire $(a;m) = 1$ teljesül (ill implicite kivathatunk az előző tételre), akkor ezt a mo.-t redukált mo.-nak nevezzük.

Ha bizonyos $a_1, \dots, a_k$ páronként inkongruens számok olyanok, hogy redukált mo.-ot reprezentálnak, (azaz $(a_i;m) = 1$), másrészt $\forall$ redukált mo.-t reprezentál ezek közül pontosan 1, akkor azt mondjuk, hogy e számok redukált maradékrendszert alkotnak mod m.

Tétel. A mod m redukált mo.-ok száma $\varphi(m)$.

B: Triviális. (def.) □

Tétel. Bizonyos $a_1, \dots, a_k \in \mathbb{Z}$ akkor alkotnak mod m redukált mo.-t, ha
a) relatív prímek m-hez;
b) páronként inkongruensek;
c) számuk $\varphi(m)$.

B: Triviálisan. □

Tétel. Ha $a_1, \dots, a_{\varphi(m)}$ redukált m.o.-t alkotnak modulo m, és $(b;m) = 1$, akkor a $ba_1, \dots, ba_{\varphi(m)}$ számok is azt alkotnak.

B: Előző tétel feltételeit kell teljesíteni.
a) $(ba_i;m) = 1 \quad \forall i$
$p \mid (ba_i;m) \Rightarrow$
$\nexists$ $(ba_i;m) > 1 \rightarrow \exists p$ prím, hogy $p \mid ba_i$, $p \mid m$
$p \mid ba_i \rightarrow p \mid b \vee p \mid a_i$
Ha $p \mid b \wedge p \mid m$ $\lightning$
Ha $p \mid a_i \wedge p \mid m$ $\lightning$ ✓
b) $\nexists$ $i \neq j$ $ba_i \equiv ba_j \pmod m$ $(b;m) = 1$
$a_i \equiv a_j$ $\lightning$ ✓
c) Triviális. □

Tétel. $\varphi(n)$ multiplikatív.

B: Azt kell belátnunk, hogy $(a;b) = 1$-re $\varphi(ab) = \varphi(a)\varphi(b)$.
Az $1, 2, \dots, ab$ számok közt hány ab-hez — azaz mind a-hoz, mind b-hez — relatív prím van. $\rightarrow \varphi(ab)$
Kétféle leszámolás.

1 és a közti a-hoz relatív prímek:	$0a+r_1$	$0a+r_2$	. . .	$0a+r_{\varphi(a)}$
$a+1$ és $2a$ közti a-hoz r. prímek:	$1a+r_1$	$1a+r_2$	. . .	$1a+r_{\varphi(a)}$
$2a+1$ és $3a$ közti — " — :	$2a+r_1$	$2a+r_2$	. . .	$2a+r_{\varphi(a)}$
⋮				
$(b-1)a+1$ és ab közti — " — :	$(b-1)a+r_1$	$(b-1)a+r_2$	. . .	$(b-1)a+r_{\varphi(a)}$

Ezek az 1 és ab közti a-hoz relatív prímek.

Vedd, hogy b-hez is r. p. legyen → nézzük oszloponként!

$0a+r_i,\ 1a+r_i,\ \dots,\ (b-1)a+r_i$ teljes maradékrm., mert $0, 1, \dots, (b-1)$ t.m.r. mod b, és $(a,b)=1$.

→ $\forall$ oszlopban $\varphi(b)$ darab elem r.p. b-hez is.

⇒ 1 és ab között az a-hoz és b-hez is r.p.-ek száma $\varphi(a)\varphi(b) = \varphi(ab)$ □

Tétel. (Euler–Fermat-tétel): $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$.

B: Legyen $r_1, r_2, \dots, r_{\varphi(m)}$ redukált maradékrm. mod m.

Ekkor $ar_1, ar_2, \dots, ar_{\varphi(m)}$ r.m.rr., mert $(a,m)=1$.

→ sorrendtől eltekintve az első és a második rr. kongruensek.

$\Rightarrow r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \equiv (ar_1)\cdot(ar_2)\cdot\dots\cdot(ar_{\varphi(m)}) \pmod m$

$\Leftrightarrow r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \equiv a^{\varphi(m)} \cdot r_1 \cdot \dots \cdot r_{\varphi(m)} \pmod m$

r_i redukált maradékosz. → a szorzat relatív prím a modulushoz

$\Rightarrow 1 \equiv a^{\varphi(m)} \pmod m$ □

Következmény. ((Kis) Fermat-tétel): Ha p prím és $(a,p)=1$ (azaz $p \nmid a$), akkor $a^{p-1} \equiv 1 \pmod p$.

B: $m=p$ az EF-tételben → $(a;p)=1$ teljesül, $\varphi(p)=p-1 \Rightarrow a^{p-1} \equiv 1 \pmod p$. □

Másik alak: (nincs r.p. feltétel)

Következmény. Ha p prím, $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod p$.

B: Ha $(p;a)=1 \rightarrow a^{p-1} \equiv 1 \pmod p \Rightarrow a^p \equiv a \pmod p$ ✓

Ha $(p;a)>1 \rightarrow p \mid a \rightarrow a \equiv 0 \pmod p \Rightarrow a^p \equiv 0 \pmod p \overset{\text{tranz.}}{\Rightarrow} a^p \equiv a \pmod p$ ✓ □

Lineáris kongruenciák

Definíció. Lineáris kongruencián $ax \equiv b \pmod m$ alakú kongruenciát értünk, ahol $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, $a \not\equiv 0 \pmod m$, és aron $x \in \mathbb{Z}$-et keressük, amikre az imént kongr. teljesül. Ezeket a kongr. megoldásainak nevezzük.

Megjegyzés. x_1 megoldás $\wedge$ $x_1 \equiv x_2 \pmod m$ → $ax_1 \equiv b \pmod m$, $ax_2 \equiv ax_1 \pmod m$ } $\Rightarrow ax_2 \equiv b \pmod m$,

tehát x_2 is megoldás.

A megoldások korongos mod m maradékosztályok. Kérdés, hogy melyek.

→ elég venni egy TMR-t, és $\forall$ elemet végigpróbálni. → m lépésben kiderül.

Tétel. Az $ax \equiv b \pmod m$ kongruencia ekvivalens a mod m mo.-ek gyűrűjében felírt $(a)(x)=(b)$ egyenlettel.

B: Triviális.

Definíció. Az $ax \equiv b \pmod m$ l. kongr. x_1, x_2 megoldásait lényegesen különbözőnek mondjuk, ha $x_1 \not\equiv x_2 \pmod m$.

A kongr. megoldásszámán lényegesen különböző megoldásainak számát, azaz az $(a)(x) = (b)$ gyűrűbeli egyenlet megoldásainak számát értjük.

Tétel. Az (1): $ax \equiv b \pmod m$ akkor megoldható, ha $(a, m) \mid b$. Ha ez a feltétel teljesül, akkor a megoldásszám $(a; m)$, különben 0.

B: 1) megoldhatóság $\Rightarrow (a; m) \mid b$

Megoldható: $\exists x_1 : \quad ax_1 \equiv b \pmod m \iff m \mid (ax_1 - b)$

$\iff \exists y_1 : my_1 = ax_1 - b \iff \underbrace{ax_1}_{(a;m)\mid} - \underbrace{my_1}_{(a;m)\mid} = b \Rightarrow (a;m) \mid b$ ☐

2) $(a; m) \mid b \Rightarrow$ megoldható, és $(a; m)$ db mo. van.

$ac \equiv bc \pmod m \iff a \equiv b \left(\frac{m}{(m;c)}\right)$

Ha $c = (a; m) \longrightarrow \underbrace{\frac{a}{(a;m)}}_{a' \in \mathbb{Z}} x \equiv \underbrace{\frac{b}{(a;m)}}_{b' \in \mathbb{Z}} \left(\underbrace{\frac{m}{(a;m)}}_{m' \in \mathbb{Z}}\right) \iff (1)$

Tehát.

$(1) \iff (1')$: $a' x \equiv b' \pmod{m'}$, ahol $(a'; m') = 1$.

Elegendő (1')-t megoldani. Ehhez tekintsük az $1, 2, \dots m'$ számokat: TMR mod m'.

$\longrightarrow (a'; m') = 1$ miatt $a', 2a', \dots, m'a'$ is TMR mod m'.

$\longrightarrow$ Pontosan 1 ezek közül kongruens b'-vel: $a' x_0 \equiv b' \pmod{m'}$

Tehát (1') megoldható, és pontosan 1 megoldása van: az x_0 maradékú.

x_0 megoldása (1)-nek is, mert ekvivalensek.

Tehát (1') összes megoldásai, és így (1) összes megoldásai:

$x_0, \ x_0 \pm m', \ x_0 \pm 2m', \ \dots, \ x_0 \pm (a; m) m', \dots$ azaz

$x_0, \ x_0 \pm \frac{m}{(a;m)}, \ x_0 \pm 2\frac{m}{(a;m)}, \ \dots, \ x_0 \pm ((a;m)-1) \cdot \frac{m}{(a;m)}, \ \underbrace{x_0 \pm (a;m)\frac{m}{(a;m)}}_{x_0 + m \equiv x_0}, \dots$

Hány és melyek ezek közül inkongruensek?

$x_0, \ x_0 + \frac{m}{(a;m)}, \ \dots, \ x_0 + ((a;m)-1)\frac{m}{(a;m)}$

inkongruensek $\longrightarrow (a; m)$ darab. ☐

Ezzel egy algoritmust is megadtunk. ☐

Tétel. Ha (1) megoldható és x_0 megoldás, akkor (1) összes megoldásai:

$$x_0 + 0, \ x_0 + \frac{m}{(a;m)}, \ x_0 + 2\frac{m}{(a;m)}, \ \dots, \ x_0 + ((a;m)-1)\frac{m}{(a;m)}.$$

Tétel. A mod p maradékosztályok a műveletre nézve (kommutatív) testet alkotnak, akkor p prím.

B: A mo.-ra gyűrűt alkotnak, kommutatív, egységelemes.

Annyit kell belátni, hogy lehet nem (0) elemmel osztani.

$(a)(x) = (b)$ megoldható, ha $(a) \neq (0)$, azaz $p \nmid a$, tehát $(a; p) = 1$.

$\iff (ax) = (b) \iff ax \equiv b \pmod m$ megoldható. Ez lin. kongruencia.

$(a; p) \mid b$ teljesül $\longrightarrow$ megoldható, és 1 megoldás van. ☐

Tétel. $(a; m) = 1$ esetén az (1) kongruencia megoldása: $x \equiv b a^{(\varphi(m)-1)} \pmod m$.

B: Behelyettesítés: $ax \equiv a \cdot b a^{\varphi(m)-1} = \underbrace{a^{\varphi(m)}}_{\text{EF: } \equiv 1, \ (a;m)=1} \cdot b \equiv b \pmod m$ ☐

Látjuk, hogy elég relatív prím modulusra nézni.

Lineáris diofantikus egyenlet

Lat.: diofantikus, gr: diophantosi.

Def. Diofantikus egyenleten $F(x_1, \dots, x_n) = 0$ egyenletet értünk, ahol $F \in \mathbb{Z}[x_1, x_2, \dots, x_n]$, mely egyenletnek egész megoldásait keressük.

Diophantosz felírt 23 db. egyenletet, és mindegyikre megadott egy megoldást.

Def. Lineáris db. egyenleten $a_1x_1 + \dots + a_nx_n = b$ alakú egyenletet értünk, ahol $\forall i$ $a_i \in \mathbb{Z}$, $b \in \mathbb{Z}$, és azon $x_1, \dots, x_n \in \mathbb{Z}$ -ket keressük, melyek kielégítik ezt az egyenletet.

A következőkben a kétismeretlenes diofantikus egyenleteket fogjuk tárgyalni:

$$ax + by = c.$$

Az n- ismeretlenes indukcióval visszavezethető 2ismeretlenesre.

11.04.

Tétel. Az $ax + by = c$ $(a, b \neq 0)$ (1) lin. diof. egyenlet megoldható akkor, ha $(a; b) \mid c$. Ha ez teljesül és x_0, y_0 megoldás, akkor az egyenlet összes megoldása

$$x = x_0 + \frac{b}{(a;b)}t \quad ; \quad y = y_0 \mp \frac{a}{(a;b)}t, \qquad t \in \mathbb{Z} \qquad (2).$$

B: 1) megoldható $\Rightarrow$ $(a;b) \mid c$.

$\exists x_0, y_0$: $\underbrace{ax_0}_{(a;b)\mid} + \underbrace{by_0}_{(a;b)\mid} = c.$ $\Rightarrow$ $(a,b) \mid c$ [1]

2) $(a,b) \mid c$ $\Rightarrow$ megoldható és a megoldások (2) szerintiek.

Teljesül:

$ax \equiv c \pmod b$: megoldható $\overset{(a;b)\mid c}{\Leftrightarrow}$ ha $\exists x_0$ hogy: $b \mid ax_0 - c$ $\Rightarrow$ $\exists u \in \mathbb{Z}$: $bu = ax_0 - c$

$\Leftrightarrow$ $ax_0 - bu = c$, tehát $x = x_0$ és $y = -u$ megoldás.

Ha x_0, y_0 és x_1, y_1 mo.:

$$\begin{aligned} ax_1 + by_1 &= c \\ -\ ax_0 + by_0 &= c \\ \hline a(x_1 - x_0) + b(y_1 - y_0) &= 0 \end{aligned}$$

$$a(x_1 - x_0) = b(y_0 - y_1)$$

$\Rightarrow b \mid a(x_1 - x_0)$ $\Rightarrow$ $\frac{b}{(a;b)} \mid \frac{a}{(a;b)} \cdot (x_1 - x_0)$ $\Rightarrow$ $\frac{b}{(a;b)} \mid (x_1 - x_0)$

($\frac{b}{(a;b)}$ és $\frac{a}{(a;b)}$ relatív prímek)

$\Rightarrow \exists t \in \mathbb{Z}$: $x_1 - x_0 = \frac{b}{(a;b)} \cdot t$ $\Rightarrow$ $x_1 = x_0 + \frac{b}{(a;b)} \cdot t$. ✓

$\underbrace{a(x_1 - x_0)}_{\frac{ab}{(a;b)}t} + b(y_1 - y_0) = 0$ $\Rightarrow$ $y_0 - y_1 = \frac{a}{(a;b)}t$ $\Rightarrow$ $y_1 = y_0 - \frac{a}{(a;a)}t.$ [2]

Tétel. Az $a_1x_1 + \dots + a_nx_n = b$ $(a_1, \dots, a_n \neq 0)$ lin. db. egyenlet megoldható $\Leftrightarrow$ $(a_1; \dots; a_n) \mid b$.

B: n szerinti indukció. Bázis: $n = 2$ fent.

$\dots$ $a_1x_1 + \dots + a_{n-1}x_{n-1} = (a_1; \dots; a_{n-1}) \cdot y.$

Lineáris Kongruenciarendszerek

Más név: szimultán kongruenciák.

Def. Lineáris kongruenciarendszeren
$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{m_k} \end{aligned}\right\} \quad (1)$$
alakú k-rendszert értünk, ahol $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$, $m_1, \dots, m_k \in \mathbb{N}$, $\forall i \quad a_i \not\equiv 0 \pmod{m_i}$.
Azon $x \in \mathbb{Z}$-ket keressük, melyekre e kongruenciák egyidejűleg teljesülnek.

A lin. kongr.-ot külön-külön megoldva (feltéve, hogy megoldhatók):
$$\begin{aligned} x &\equiv x_1 \pmod{m_1'} \\ x &\equiv x_2 \pmod{m_2'} \\ &\vdots \\ x &\equiv x_k \pmod{m_k'}. \end{aligned}$$
Ezért korlátozhatjuk az ilyen k-rendszerekre.

Legyen $k = 2$.

Tétel. Az
$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}\right\} \quad (2)$$
lin. k.r. megoldható $\Leftrightarrow (m_1; m_2) \mid a_1 - a_2$.
Ha és teljesül, akkor a megoldások egy maradékosztályt alkotnak mod $[m_1; m_2]$.

B: $x \equiv a_1 \pmod{m_1} \Leftrightarrow \exists y \in \mathbb{Z}: \; x = a_1 + m_1 y$. Ezek közül mik elégítik ki a 2. kongruenciát is?
$$a_1 + m_1 y \equiv a_2 \pmod{m_2}$$
$$m_1 y \equiv a_2 - a_1 \pmod{m_2}$$
Megoldhatóság feltétele: $\Leftrightarrow (m_1; m_2) \mid a_2 - a_1$. ✓
Ha a feltétel teljesül:
$$\frac{m_1}{(m_1; m_2)} y \equiv \frac{a_2 - a_1}{(m_1; m_2)} \quad \left(\frac{m_2}{(m_1; m_2)}\right) \quad \rightarrow \quad y \equiv y_0 \quad \left(\frac{m_2}{(m_1; m_2)}\right)$$
$$\Rightarrow \quad y = y_0 + z \frac{m_2}{(m_1; m_2)} \quad \overset{z \in \mathbb{Z}}{\Longrightarrow} \quad x = a_1 + m_1 y_0 + z \cdot \underbrace{\frac{m_1 m_2}{(m_1; m_2)}}_{[m_1; m_2]}$$
$\rightarrow$ és egy mod $[m_1; m_2]$ maradékosztály. □

Következmény. $(m_1; m_2) = 1$-re a (2) k.r. megoldható, és a megoldások egy maradékosztályt alkotnak modulo $m_1 m_2$.

Általános k-ra: feltételcsoport keresi, hasonló módszerrel.
Ha relatív prímek a modulusok:

Tétel. (Kínai maradéktétel) Ha $m_1, \dots, m_k$ páronként relatív prímek, akkor
$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$
megoldható és a megoldások mo. t alkotnak modulo $m_1 m_2 \cdots m_k$.

B: k szerinti indukcióval. Bázis: $k = 2$.

Tfh. k-ra igaz.

Bizonyítandó: $\left.\begin{array}{l} x \equiv a_1 \quad (m_1) \\ \vdots \\ x \equiv a_k \quad (m_k) \end{array}\right\}$

$x \equiv a_{k+1} \quad (m_{k+1})$ -ra igaz.

Indukciós feltevés szerint az első k megoldható és megoldásai:

$x \equiv x_0 \quad (m_1 m_2 \cdots m_k)$. ($x_0$ = állandó)

Kell: $\left.\begin{array}{l} x \equiv x_0 \quad (m_1 \cdots m_k) \\ x \equiv a_{k+1} \quad (m_{k+1}) \end{array}\right\}$ megoldása: 2 k-ból álló rendszer.

$(m_1 m_2 \cdots m_k ; \; m_{k+1}) = 1 \longrightarrow$ a $k = 2$ eset alkalmazható!

$\Rightarrow$ Megoldható és a megoldás maradéko. mod $m_1 \cdots m_k \cdot m_{k+1}$. ✓ □

Alkalmazások

I. Titkosírások, kriptográfia → XX. század elejétől

Fontos, hogy számelméleti eszközökkel jól lehet véletlent modellezni.

A transzformáláshoz kosszú kulcs kell, de azt nem jó küldeni.

→ rövidebbet küldeni, és azt „felfújni."

Rivest, Shamir, Adleman → RSA-algoritmus 1979 (ma már nem használják)

Adó: kifejezi az információt bitsorozatként (labeling)

A bitsorozathoz hozzárendel egy számot → 2-es számrendszerben véve az üzenet.

Feltehető, hogy 1 és 2^{300} közé esik. (64 vagy 128 szokás) → a.

Legyen p, q nagy, kb. ugyanakkora prímek: $p \times q$.

Legyen $m = pq$. Tekintünk 2 számot: e, f, melyekre $ef \equiv 1 \quad (\varphi(m))$

(f, $\varphi(m)$ titkos; $\varphi(m) = pq - p - q + 1$, p, q titkos; e publikálható, m publikálható)

a kódolása: $b = a^e$ mod m maradék (a legkisebb nemnegatív).

Vevő: $b^f \equiv (a^e)^f = a^{ef} \equiv a^{k\varphi(m)+1} = (a^{\varphi(m)})^k \cdot a \underset{\substack{(a;m)=1 \\ \text{feltehető}}}{\equiv} 1^k \cdot a \equiv a \quad (m)$

Miért megfejthetetlen? Csak f ismeretében lenne b meghatározható, ehhez viszont e és $\varphi(m)$ kellene, de $\varphi(m)$ titkos → tudni kéne a p-t és a q-t → $m (= pq)$ ismeretében meg kéne határozni p-t és q-t (faktorizálni m-et). Erre nincs jó faktorizáló algoritmus.

Prímeket gyártani polinomiálisan lehet.

2^{300}-ig mennek ma a gépek a felbontással kb.

II. Prímmodulusú kódolás

$$\begin{array}{rcl} 81 & \Rightarrow & 1010001 \\ +\ 107 & \Rightarrow & 1101011 \\ \hline 188 & \Leftarrow & 1\,0\,1\,1\,1\,1\,0\,0 \end{array}$$

A körethező jegyhez kell az előző jegy „maradéka" → lassú.

Program gyorsasága: bitoperációk száma nagyságrendileg

Bitoperáció: ami egy oszlopban történik

11.11. Gyorsítás: 2-es szr. helyett prímmodulusú kódolás alkalmazása.

$p_1 = 2, \quad p_2 = 3, \ldots, \quad p_k$

Az $1, 2, \ldots, p_1 \cdots p_k$ számokat egyértelműen meghülönbözteti, hogy az egyes prímek szerint milyen maradékot adnak (kínai maradéktétel)

$k = 3 \quad 2 \cdot 3 \cdot 5 = 30$ kicsi

$k = 4 \quad 2 \cdot 3 \cdot 5 \cdot 7 = 210$ már elég 4 prím

$81 \longleftrightarrow 81 \equiv 1 \ (2),\ 81 \equiv 0 \ (3),\ 81 \equiv 1 \ (5),\ 81 \equiv 4 \ (7) \rightarrow (1,0,1,4)$

$107 \longleftrightarrow 107 \equiv 1 \ (2),\ 107 \equiv 2 \ (3),\ 107 \equiv 2 \ (5),\ 107 \equiv 2 \ (7) \rightarrow (1,2,2,2)$

$x \longleftrightarrow x \equiv 0 \ (2),\ x \equiv 2 \ (3),\ x \equiv 3 \ (5),\ x \equiv 6 \ (7) \rightarrow (0,2,3,6)$

x-re lineáris kongruenciarendszer és $0 < x < 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$\rightarrow x \equiv 188 \ (210) \rightarrow x = 210$

$\Rightarrow$ A maradékosztályok számolása végezhető párhuzamosan $\rightarrow$ log gyorsaságú művelet

---

Magasabb fokú kongruenciák

Definíció: Magasabb fokú kongruencián

$$(1): \quad f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \equiv 0 \ (m)$$

alakú kongruenciát értünk, ahol $m, n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{Z}$, és olyan $x \in \mathbb{Z}$-t keressük, amelyek kielégítik (1)-et.

Megjegyzés: Ha x_1 megoldás és $x_1 \equiv x_2 \Rightarrow x_2$ is megoldás, mert $f(x_1) \equiv f(x_2) \ (m)$,

$f(x_1) \equiv 0 \rightarrow f(x_2) \equiv 0$. □

Tehát a megoldások maradékosztályok. $\rightarrow$ Elég végigpróbálni az m maradékosztályait $\rightarrow$ véges algoritmus létezik. (Algebrában 4-nél magasabb fokú egyenletre nincs.)

Ha nem próbálgatni akarunk $\rightarrow$ kísérlet az algebrai egyenletekhez. $\rightarrow$ redukció, ipar. eszköz.

Redukciós eljárások

Tétel: Legyen $m > 1$, $m \in \mathbb{N}$. Legyen m kan. alakja $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Legyen $f(x) = a_0 x^n + \dots + a_{n-1} x + a_n \in \mathbb{Z}[x]$.

Ekkor az $f(x) \equiv 0 \ (m)$ kongruencia ekvivalens az

$$\left.\begin{array}{ll} f(x) \equiv 0 & (p_1^{\alpha_1}) \\ \vdots & \\ f(x) \equiv 0 & (p_r^{\alpha_r}) \end{array}\right\} \quad (3)$$

kongruenciarendszerrel abban az értelemben, hogy x adsa. megoldása (2)-nek, ha egyidejűleg kielégíti a (3)-beli kongruenciák mindegyikét.

B: $(2): \ f(x) \equiv 0 \ (m) \Leftrightarrow m \mid f(x) \Leftrightarrow \forall i \ p_i^{\alpha_i} \mid f(x) \Leftrightarrow \forall i \ f(x) \equiv 0 \ (p_i^{\alpha_i})$. □

Következmény: Az $f(x) \equiv 0 \ (m)$ kong. megoldása az $f(x) \equiv 0 \ (p^\alpha)$ prímhatvány modulusú kongruenciák megoldására, majd lineáris k. rendszer megoldására redukálható:

$f(x) \equiv 0 \ (p_i^{\alpha_i}) \rightarrow x \equiv x_i \ (p_i^{\alpha_i})$ rendszer.

Tétel: Legyenek $m, n \in \mathbb{N}$; $a_0, \dots, a_n \in \mathbb{Z}$, $a_0 \not\equiv 0 \ (m)$. Jelöljük a mod m maradékosztályok gyűrűjét $\mathbb{Z}_m$-mel és legyen $F(x) = (a_0) x^n + (a_1) x^{n-1} + \dots + (a_{n-1}) x + (a_n) \in \mathbb{Z}_m[x]$.

Ekkor az (1) kongruencia ekvivalens (4): $F(x) = (0)$ $\mathbb{Z}_m[x]$-beli egyenlettel, amennyiben $x = x_0$ adsa. megoldás, ha $x = (x_0)$ megoldása (4)-nek.

B: Triv a megjegyzés alapján.

Definíció: Az (1) kongruencia x_1, x_2 megoldásait lényegesen különbözőnek mondjuk, ha $x_1 \not\equiv x_2 \ (m)$.

Definíció: Az (1) megoldásszámán (1) lényegesen különböző megoldásainak számát (vagyis (4) megoldásszámát) értjük.

Tétel: Az $f(x) \equiv 0 \ (p^\alpha)$ kongruencia megoldása visszavezethető $f(x) \equiv 0 \ (p)$ megoldására, majd ezt követően $\alpha - 1$ db lineáris kongruencia megoldására.

B: N.B. (számolós), helyette példa

Példa. Oldjuk meg az $f(x) = x^3 - x^2 - 1 \equiv 0 \pmod{27}$ kongruenciát!

Megoldás: ① $27 \mid f(x) \Rightarrow 3 \mid f(x)$. Ez mely x-ekre teljesül?

② Ezek közül melyekre teljesül $9 = 3^2 \mid f(x)$ is?

③ Ezek közül melyekre teljesül $27 = 3^3 \mid f(x)$ is?

① → Teljes mod 3 m.m. mely elemeire teljesül $f(x) \equiv 0 \pmod 3$?

$$f(0) \equiv -1 \not\equiv 0 \pmod{27}$$

$$f(\pm 1) = (\pm 1)^3 - (\pm 1)^2 - 1 = \begin{cases} -1 \not\equiv 0 \pmod 3 \\ -3 \equiv 0 \pmod 3 \end{cases}$$

$$\rightarrow x \equiv -1 \pmod 3 \Rightarrow x = 3y - 1$$

② $f(3y-1) \equiv 0 \pmod 9$

$$f(3y-1) \equiv (3y-1)^3 - (3y-1)^2 - 1 \equiv -1 + 6y - 1 - 1 \equiv 0 \pmod 9$$

$$6y \equiv 3 \pmod 9$$

$$2y \equiv 1 \pmod 3$$

$$-y \equiv 1 \pmod 3$$

$$y \equiv -1 \pmod 3$$

$$x = 9z - 4 \Leftarrow y = 3z - 1 \Leftarrow$$

③ $f(9z-4) \equiv 0 \pmod{27}$

$$f(9z-4) = (9z-4)^3 - (9z-4)^2 - 1 \equiv (-4)^3 + 72z - 16 - 1 \equiv 0 \pmod{27}$$

$$-64 + 72z - 16 - 1 \equiv 0 \pmod{27}$$

$$-10 + (-9z) - 16 - 1 \equiv 0 \pmod{27}$$

$$-9z - 27 \equiv 0 \pmod{27}$$

$$x = 27t - 4 \Leftarrow z = 3t \Leftarrow z \equiv 0 \pmod 3$$

$$\Downarrow$$

$$\boxed{x \equiv -4 \pmod{27}}$$

Mostantól szorítkozhatunk csak prím modulusú kongruenciákra.

Prím modulusú magasabb fokú kongruenciák

Tétel. (Főtétel) Egy prím modulusú n-edfokú kongruencia megoldásszáma $\leq n$.

B: $f(x) = a_0 x^n + \ldots + a_n \equiv 0 \pmod p$ ekvivalens $F(x) = (a_0) x^n + \ldots + (a_n) = (0)$ $\mathbb{Z}_p[x] \ni F(x)$

p prím → $\mathbb{Z}_p$ test. Algebrában főtétel: test feletti n-edfokú algebrai egyenletnek legfeljebb n gyöke van.

Definíció. Ha két magasabb fokú kongruencia megoldásai azonosak, akkor a 2 kongruenciát ekvivalensnek mondjuk. ($\sim$)

Cél: alacsonyabb fokú polinomot találni, ami ekvivalens.

Tétel: Egy p modulusú magasabbfokú kongruencia ekvivalens egy max. $p-1$-edfokú kongruenciával, és ez utóbbi meg is konstruálható.

B: $f(x) = a_0 x^n + \ldots + a_n \equiv 0 \pmod p$, $a_0 \not\equiv 0$

Osszuk $f(x)$-et $x^p - x$-szel!

$f(x) = (x^p - x)\, q(x) + r(x)$ q, r egész eh.-s polinomok, mert $x^p - x$ főegyütthatója 1 és egész eh.-s.

$r(x) \not\equiv 0$ vagy $\operatorname{gr} r \leq p-1$.

$f(x) \equiv 0 \quad (p) \qquad f(x) = (x^p - x)\, q(x) + r(x)$

$x = a$ megoldás: $f(a) \equiv 0\ (p) \iff f(a) = \underbrace{(a^p - a)}_{\equiv 0 (p)} \cdot q(a) + r(a) = r(a) \equiv 0 \quad (p)$

KF

Tehát $f(x) \equiv 0\ (p) \iff r(x) \equiv 0\ (p)$.

$f \sim r$. □

Tétel. (Wilson-tétel) Ha p prímszám, akkor $(p-1)! \equiv -1 \quad (p)$.

B: Fokszámtétellel.

(Csak prímekre igaz: $(m-1)! \equiv -1 \quad (m) \iff m$ prím $\rightarrow$ nem praktikus, de a legtégebbi prímteszt.)

11. 18.

Tekintsük $f(x) = (x^{p-1} - 1) - (x-1)(x-2)\cdots(x-(p-1))$

Fermat-tétel miatt $i = 1, 2, \dots, p-1$-re $x^{p-1} - 1 \equiv 0 \Rightarrow$ ezek gyökök

Tehát legalább $p-1$ gyök van.

Fokszámtétel $\Rightarrow$ gr f létezik és $\geq p-1$ vagy $f \equiv 0$. gr f = deg f

f legmagasabb fokú tagja x^{p-1}, ami kiesik $\Rightarrow$ gr $f \leq p-2$

$\Rightarrow f(x) \equiv 0 \Rightarrow \forall$ együttható $\equiv 0\ (p) \rightarrow$ ez a konstans tagra is igaz

$-1 + (-1)^p \cdot (p-1)! \equiv 0 \quad (p)$

$p > 2$: $-1 \equiv (p-1)! \quad (p)$ ✓ $\qquad p = 2$: $-1 + 1 \equiv 0 \quad (2)$

$-1 \equiv 1! \quad (2)$ ✓ □

Binom Kongruenciák

Definíció. Binom kongruencián $a x^k \equiv b \quad (m)$ kongruenciát értünk.

Továbbiakban $m = p$.

Megjegyzés. $a x^k \equiv b \quad (p)$. Legyen $y = x^k \rightarrow$ lin. kong. y-ra $\rightarrow y \equiv y_0 \quad (p)$

$\rightarrow x^k \equiv y_0 \quad (p)$. Tehát a eliminálható, szorítkozhatunk erre.

$x^k \equiv a \quad (p)$

Ha $a \equiv 0 \rightarrow p \mid x$ kell és elég $\rightarrow x \equiv 0 \quad (p)$.

Feltehető, hogy $a \not\equiv 0\ (p)$.

Tétel. Az $x^k \equiv 1 \quad (p)$ kongruencia N megoldásszáma $(k; p-1)$.

B: Tfh. $k \mid p-1$. $(k; p-1) = k$. Bizonyítandó $N = k$.

Fokszámtétel $\Rightarrow N \leq k$.

Tekintsük az $x^{p-1} - 1 \equiv 0 \quad (p)$ kongruenciát! $x = 0$ nem mo., de az összes redukált maradék megoldás (KF szerint). $\Rightarrow$ megoldásszáma $p-1$.

Szorzattá alakítás: $(x^k - 1)(x^{p-1-k} + x^{p-1-2k} + \dots + 1) \equiv 0 \quad (p)$

Ennek megoldásszáma $= p-1 \leq N +$ fokszám a 2. tényezőben $= N + p - 1 - k$

$\Rightarrow k \leq N \qquad \Rightarrow N = k$. ✓

Legyen $d = (k, p-1)$.

Áll. $x^k \equiv 1 \quad (p) \iff x^d \equiv 1 \quad (p)$

Ebből következik, hogy $N = d$, mert $x^d \equiv 1$-nek a fentiek szerint d megoldása van

B: 1) $\overleftarrow{\ }$ $x^d \equiv 1 \quad (p)$ Hatv. $\frac{k}{d} \in \mathbb{Z}$ hatványra $\Rightarrow x^k \equiv 1 \quad (p)$ ✓

2) $\overrightarrow{\ }$ Lemma. $k \in \mathbb{N}$, p pozitív prím $\Rightarrow \exists\, u, v > 0$, $uk - v(p-1) = (k; p-1) = d$. (3)

B: ~~Tudjuk, hogy~~ kisőbb

$\underbrace{x^k \equiv 1 \quad (p)}_{\rightarrow x \not\equiv 0 (p) \Rightarrow x^{p-1} \equiv 1 (p)} \Rightarrow x^{uk} \equiv 1 \quad (p) \Rightarrow x^{v(p-1)+d} \equiv 1 \quad (p) \Rightarrow (x^{p-1})^v \cdot x^d \equiv 1 \quad (p)$

$1^v \cdot x^d \equiv 1 \quad (p)$ ✓

B (lemma): Van mo., mert $(k;p-1) \mid (k;p-1)$. Kellene, hogy poz. legyenek.
$\exists\, u_0$ megoldás a maradékosztályban, hogy $u_0 > d\ (>0)$.
$\Rightarrow u_0 k > u_0 > d$.
$v_0 \cdot (p-1) + d = u_0 \cdot k > d \Rightarrow v_0 (p-1) > 0 \Rightarrow v_0 > 0$. ✓ □

Eddig volt: $x^k \equiv 0 \quad (p)$,
$x^k \equiv 1 \quad (p)$. Áttérünk az általános esetre: $x^k \equiv a \ (p)$. $(a \not\equiv 0)$ (4)

Def. Ha $(a,p)=1$ és (4) megoldható, akkor a-t k-adik hatványmaradéknak mondjuk.

Tétel. a acsa k-adik hatványmaradék mod p, ha $a^{\frac{p-1}{(k,p-1)}} \equiv 1 \ (p)$;
Ha ez a feltétel teljesül, akkor (4) megoldásszáma $(k;p-1)$.

B: 1) a k-adik hvm. mod $p \Rightarrow a^{\frac{p-1}{(k,p-1)}} \equiv 1 \ (p)$.
$\exists$ (4)-nek x_0 megoldása: $x_0^k \equiv a \ (p)$. $x_0 \not\equiv 0$, mert $a \not\equiv 0$, mert $(a,p)=1$.
Emeljük $\frac{p-1}{(k;p-1)}$. hatványra:

$$\left(x_0^k\right)^{\frac{p-1}{(k;p-1)}} \equiv a^{\frac{p-1}{(k;p-1)}} \ (p).$$

$$\underbrace{\left(x_0^{p-1}\right)^{\frac{k}{k;p-1}}}_{1 \ (KF)} \equiv a^{\frac{p-1}{(k;p-1)}} \ (p)$$

✓

2) $a^{\frac{p-1}{(k;p-1)}} \equiv 1 \ (p) \Rightarrow a$ k-adik hvm. mod p. És a megoldásszám $(k;p-1)$.
N.B. □

Rend

$(a,p)=1 \Rightarrow \exists\, k \in \mathbb{N}: \ a^k \equiv 1 \ (p)$. (5) Ez igaz a Kis Fermat-tétel miatt: $k=p-1$ ilyen.
„Jó" kitevő: (5) teljesül rá.

Def. $(a,p)=1$-re a legkisebb $k \in \mathbb{N}$ jó kitevőt az a rendjének nevezzük mod p.
Jelölés: $o_p(a)$, röviden $o(a)$. $(\exp a)$

Tétel. $(a,p)=1 \quad a^k \equiv 1 \ (p) \iff o_p(a) \mid k$.

B: 1) $o_p(a) \mid k \Rightarrow a^k = \left(a^{o_p(a)}\right)^{\frac{k}{o_p(a)}} \equiv 1^{\frac{k}{o_p(a)}} \equiv 1 \ (p)$ ✓

2) $a^k \equiv 1 \ (p)$. Osszuk el k-t $o_p(a)$-val maradékosan!
$k = q \cdot o(a) + r \quad 0 \le r < o(a)$
$a^k = a^{q\,o(a)+r} = (a^{o(a)})^q \cdot a^r \equiv 1 \cdot a^r \equiv 1 \ (p) \rightarrow r < o(a)$ és jó kitevő vagy 0.
$\Rightarrow r = 0 \Rightarrow o(a) \mid k$. □

Következmény. $o_p(a) \mid p-1$.
B: $p-1$ jó kitevő KF szerint. □

Tétel. $(a,p)=1$-re $a^k \equiv a^l \ (p) \iff k = l \ (o_p(a))$ $(k,l \geq 0)$.

B: Feltehető, hogy $k \geq l$. Oszthatunk a^l-nel: $a^{k-l} \equiv 1 \ (p)$
$\iff o_p(a) \mid k-l \iff k \equiv l \ (o_p(a))$ □

Tétel. p prím, $k \in \mathbb{N} \rightarrow 1 \le a \le p-1$, $o_p(a) = k$ tulajdonságú a-k száma
$$\begin{cases} 0, & \text{ha } k \nmid p-1 \\ \varphi(k), & \text{ha } k \mid p-1. \end{cases}$$

B: Lemma: $\varphi(n)$ összegzési fv.-e $\sum_{d|n} \varphi(d) = n$.

B: φ multiplikatív $\to \sum \varphi(d)$ is multiplikatív. Az $f(n) = n$ is multipl.
Mindkét oldalon multipl. fv. áll. $\to$ Elég a prímhatvány helyeket nézni.

$$\sum_{d|p^\alpha} \varphi(d) = \varphi(1) + \varphi(p) + \dots + \varphi(p^\alpha) = 1 + (p-1) + (p^2-p) + \dots + (p^\alpha - p^{\alpha-1}) = p^\alpha$$

$$f(p^\alpha) = p^\alpha.$$ □

k-ra vonatkozó teljes indukció.
$k = 1$: $1 | p-1 \to \varphi(1) = 1$ ilyen a van. Nyilvám ilyen a csak az $a = 1$: ✓
Tfh. $k-1$-ig igaz $\to$ k-ra is igaz.
1) $k \nmid p-1 \Rightarrow \nexists a: O_p(a) = k$, mert $O_p(a) | p-1$ teljesüljön kell. ✓
2) $k | p-1 \to$ bbl. $\varphi(k)$ van.
Tehát hány $1 \le a \le p-1$ redukált maradék van, hogy $O_p(a) = k$.

$$|\{a: 1 \le a \le p-1, O_p(a) = k\}| = |\{a: 1 \le a \le p-1, k \text{ jó kitevő}\}| - \underbrace{|\{a: 1 \le a \le p-1, \exists \text{ kisebb jó kitevő}\}|}_{d = O_p(a) | k,\ d < k} =$$

$$= \underbrace{(k; p-1)}_{\text{binomkr. megoldásszáma}} - \sum_{\substack{d|k \\ d<k}} \underbrace{|\{a: 1 \le a \le p-1, O_p(a) = d\}|}_{\text{alkalmazható az ind. feltevés}} =$$

$$= \underbrace{k}_{\substack{(k;p-1) = \\ k, \text{ mert} \\ k|p-1.}} - \sum_{\substack{d|k \\ d<k}} \varphi(d) = \underbrace{\sum_{d|k} \varphi(d)}_{\text{lemma}} - \sum_{\substack{d|k \\ d<k}} \varphi(d) = \varphi(k).$$ □

2014. 11. 25.

Def. #1 Ha $(g,p) = 1$ és $O_p(g) = p-1$, akkor g-t primitív gyöknek mondjuk mod p.

Tétel. Ha g primitív gyök mod p és $k, l \in \{0,1,2,\dots,\}$ akkor $g^k \equiv g^l \ (p)$
$\iff k \equiv l \ (p-1)$.

B: Előzőekben: $a^k \equiv a^l \iff k \equiv l \ (O_p(a))$, és itt $O_p(g) = p-1$. □

Def. #2 Ha $g, g^2, \dots, g^{p-1}$ redukált maradékrendszer mod p, akkor g primitív gyök mod p.

Tétel. A két definíció ekvivalens.

B: 1. #1 $\Rightarrow$ #2.
$g, g^2, \dots, g^{p-1} \to$ számuk $p-1 = \varphi(p)$ ✓
$(g,p) = 1 \Rightarrow g, g^2, \dots, g^{p-1} \not\equiv 0 \ (p)$ ✓
$g^k \not\equiv g^l \ (p)$ az előző tétel miatt. ✓

2. #2 $\Rightarrow$ #1
$g, \dots, g^{p-1}$ r.m.r. $\Rightarrow (g,p) = 1$
$g^{p-1} \equiv 1$ (Fermat) $g, g^2, \dots \not\equiv g^{p-1} \Rightarrow O_p(g) = p-1$. □

Tétel. $\forall p$ prímszámhoz $\exists$ primitív gyök mod p és a lényegesen különbözők száma $\varphi(p-1)$.

B: Korábbi tétel szerint $\varphi(k)$ darab lényegesen különböző a létezik: $O_p(a) = \cancel{\varphi}(k)$-val.
$\to O_p(a) = p-1$, a számuk $\varphi(p-1)$. □

A definíciók ekvivalenciája miatt ha g pr. gy. mod p, $(a,p) = 1$-re $\exists!\ k \in \mathbb{N}$
$g^k \equiv a \ (p)$ és $1 \le k \le p-1$.

Definíció. Ha g primitív gyök modulo p és $(a,p)=1$, akkor azt az egyértelmű k-t, amelyre $1 \le k < p-1$, $g^k \equiv a \ (p)$ az a szám g alapú indexének vagy g alapú diszkrét logaritmusának nevezzük.

Jelölés: $\overset{g}{\operatorname{ind}}_p a$, rögzített p-re $\overset{g}{\operatorname{ind}}\, a$, rögzített g-re $\operatorname{ind} a$. modulo p.

Tétel. $(a,p)=(b,p)=1$, k nemnegatív egészre: (logaritmikus azonosságok)

1) $\operatorname{ind}(ab) \equiv \operatorname{ind}(a) + \operatorname{ind}(b) \quad (p-1)$

2) $\operatorname{ind}(a^k) \equiv k \operatorname{ind}(a) \quad (p-1)$

B: 1) $g^{\overset{g}{\operatorname{ind}}_p a} \equiv a \ (p)$, $g^{\overset{g}{\operatorname{ind}}_p b} \equiv b \ (p)$ $\longrightarrow$ $g^{\operatorname{ind} a + \operatorname{ind} b} \equiv ab \ (p)$

$g^{\overset{g}{\operatorname{ind}}_p (ab)} \equiv ab \ (p)$ A kongruenciarelációk tranzitív $\Rightarrow$ $g^{\operatorname{ind}(ab)} \equiv g^{\operatorname{ind} a + \operatorname{ind} b} \ (p)$

Korábbi tétel $\Rightarrow$ $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \ (p-1)$ $\hookrightarrow o_p(g)$

2) 1)-ből indukcióval. □

Az index alkalmazható binomkongruenciák megoldására: (1) $x^k \equiv a \ (p)$. $(a,p)=1$.

$\Leftrightarrow$ $g^{\operatorname{ind} x^k} \equiv g^{\operatorname{ind} a} \ (p)$.

$\Leftrightarrow$ $\overset{g}{\operatorname{ind}}\, x^k \equiv \overset{g}{\operatorname{ind}}\, a \quad (p-1)$

$\Leftrightarrow$ (2) $k \overset{g}{\operatorname{ind}}\, x \equiv \overset{g}{\operatorname{ind}}\, a \quad (p-1)$ $\longrightarrow$ lineáris kongruencia $\overset{g}{\operatorname{ind}}$ x-ben.

Tetszőleges vagy alkalmas g-hez indextáblázatot és visszahelyező-táblázatot készítünk.

Tétel. Ha $(a,p)=1$, akkor a k-adik hatványmaradék mod p $\Leftrightarrow$ $(k,p-1) \mid \overset{g}{\operatorname{ind}}\, a$ (g primitív gyöktől független: ha az egyikre teljesül, mindre teljesül).

Ha ez a feltétel teljesül, a megoldások száma $(k,p-1)$.

B: (1) megoldható $\Leftrightarrow$ (2) megoldható $\Leftrightarrow$ $(k,p-1) \mid \overset{g}{\operatorname{ind}}\, a$. És ha ez teljesül, a megoldások száma $(k,p-1)$. □

Kvadratikus maradékok

most $x^k \equiv a \ (p)$-t vizsgáljuk $k=2$-re $\longrightarrow$ „gyökvonás".

Definíció. Ha $(a,p)=1$ és $x^2 \equiv a \ (p)$ megoldható, akkor a-t p-s maradéknak mondjuk mod p.

Ha $(a,p)=1$ és (1) nem oldható meg, akkor a kvadratikus nemmaradék mod p.

(Ha $a \equiv 0 \ (p)$, akkor sem ebbe, sem abba a csoportba nem soroljuk be.)

Tétel. $p>2$, $(a,p)=1$-re a akkor kvadratikus maradék mod p, ha $a^{\frac{p-1}{2}} \equiv 1 \ (p)$.

B: A k-adik hatványmaradékságra vonatkozó tételt $k=2$-re specializáljuk: a másodikat hatványmaradék, akkor p-s m. $\Leftrightarrow$ $a^{(p-1)/(2,p-1)} \equiv 1 \ (p)$. $(2,p-1)=2$

$\Leftrightarrow$ $a^{(p-1)/2} \equiv 1 \ (p)$. □

Tétel. $p>2$-re az $1, 2, \dots p-1$ számok közt mind a p-s m.-ek, mind a p-s nemm. száma $\frac{p-1}{2}$.

B: Korábbi tétel: a k-adik kvm.-ek száma $\frac{p-1}{(k,p-1)}$. $\longrightarrow$ $\frac{p-1}{(2,p-1)} = \frac{p-1}{2}$ db p-s m. □

Tétel. $p>2$, $(a,p)=1$ esetén a kv. m. $\Leftrightarrow$ ~~kka~~ tetszőleges g-re $\operatorname{ind}_g a$ páros.

B: a k-adik hvm. mod p $\Leftrightarrow$ $(k; p-1) \mid \operatorname{ind} a$. $\quad (k; p-1) = (2; p-1) = 2$. □

Tétel. (Euler-lemma) $p>2$, $(a,p)=1$ esetén

$$a^{\frac{p-1}{2}} \equiv \begin{cases} +1, & \text{ha } a \text{ kv. m. mod } p \\ -1, & \text{ha } a \text{ kv. nm. mod } p \end{cases} \quad (p)$$

B: Korábbi tétel szerint $a^{\frac{p-1}{2}} \equiv 1$ $\Leftrightarrow$ a kv. m. mod p. Bizonyítandó még, hogy a kv. nm.-re vonatkozó állítás is igaz.

$(a; p) = 1 \Rightarrow$ Fermat: $a^{p-1} \equiv 1 \quad (p)$

$$a^{p-1} - 1 \equiv 0 \quad (p) \qquad p-1 \text{ páros}$$

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \quad (p)$$

a kv. nm. $\Rightarrow$ $a^{\frac{p-1}{2}} - 1 \not\equiv 0$ (p). $\Rightarrow$ $a^{\frac{p-1}{2}} + 1 \equiv 0 \quad (p)$

$\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv -1 \quad (p)$, ha a kv. nemmaradék. □

„És ezzel maradéktalanul igazoltuk a tételt."

Ez kog nagyságrendben dönti el, hogy valami kv. m.-e.

Definíció. p tetszőleges prím, $(a,p)=1$. Ekkor az $\left(\frac{a}{p}\right)$ Legendre-szimbólum értéke

$+1$, ha a kv. m. mod p,

-1, ha a kv. nm. mod p.

($a \equiv 0$ (p)-re a Legendre-szimbólum értéke nincs definiálva. Újabban előfordul, hogy $\left(\frac{0}{p}\right)=0$-t is definiálják, de ez még nem általánosan elfogadott.)

Tétel. $(a,p) = (b;p) = 1$, $a \equiv b$ (p) esetén: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

B: $a \equiv b$: $x^2 \equiv a \quad (p)$ megoldható $\Leftrightarrow$ $x^2 \equiv b \quad (p)$ megoldható. □

Tétel. $(a,p) = 1$ $\left(\frac{a^2}{p}\right) = +1$.

B: $x^2 \equiv a^2 \quad (p)$ megoldható, mert $x = \pm a$ megoldás. □

Következmény. $\left(\frac{1}{p}\right) = +1$. □

Tétel. $p>2$, $(a,p) = 1$ esetén $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p)$.

B: Euler-lemma átfogalmazása. □

Tétel. $(a,p) = (b,p) = 1$-re $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$: a Legendre-szimbólum multiplikatív.

B: Ha $p=2$ $\rightarrow$ triviális.

Ha $p>2$:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \quad (p)$$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p)$$

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \quad (p)$$

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv (ab)^{\frac{p-1}{2}}$$

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad (p)$$

Mindkét oldal $+1$ vagy -1,

$p>2 \Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Tétel. $p>2$ esetén $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, azaz $x^2 \equiv -1 \quad (p)$ megoldható $\Leftrightarrow$ $p \equiv 1 \quad (4)$.

Ha $p=2$, akkor $\left(\frac{-1}{2}\right) = +1$.

B: Euler-lemma következménye szerint $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \quad (p)$. mindkét oldalon $+1$ vagy -1 áll és a modulus >2 $\rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

□

Tétel. (Gauss-lemma). Legyen $p>2$, $(a,p)=1$. Jelöljük az $a, 2a, \dots, \frac{p-1}{2}a$ számok mod p legkisebb nemnegatív maradékai ~~számait~~ közül a $\frac{p}{2}$-nél nagyobbak számát m-mel. Ekkor $\left(\frac{a}{p}\right) = (-1)^m$.

B: N.B. (kb. 1 óra hosszú)

Ez elég gyors eljárás a kvadratikus maradékság eldöntésére.

2014. XII. 2.

Tétel. $p>2$-re $\left(\frac{-1}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Azaz $\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{ha } p = 8k \pm 1 \\ -1, & \text{ha } p = 8k \pm 3 \end{cases}$.

B: Gauss-lemma $a=2$-re: $(2,p)=1$.

$1\cdot 2,\ 2\cdot 2,\ \dots,\ \frac{p-1}{2}\cdot 2$ $\rightarrow$ ($a=2$-re) ezek maradéka önmaga

$m = (\text{összes}) - (\text{kicsi}) = \frac{p-1}{2} - \left[\frac{p/2}{2}\right] = \frac{p-1}{2} - \left[\frac{p}{4}\right]$

$$m = \begin{cases} 4k - 2k = 2k, & \text{ha } p = 8k+1 \\ (4k-1) - (2k-1) = 2k, & \text{ha } p = 8k-1 \\ (4k+1) - (2k) = 2k+1, & \text{ha } p = 8k+3 \\ (4k-2) - (2k-1) = 2k-1, & \text{ha } p = 8k-3 \end{cases} \Rightarrow (-1)^m = \left(\frac{2}{p}\right) = \begin{cases} +1 \\ +1 \\ -1 \\ -1 \end{cases}$$

Megmutatjuk, hogy a kétféle megfogalmazás ekvivalens.

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k\pm 1)^2-1}{8}} = (-1)^{8k^2 \pm 2k} = +1$$

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k\pm 3)^2-1}{8}} = (-1)^{8k^2 \pm 6k + 1} = -1.$$

Tétel. (Kvadratikus reciprocitási tétel.) Legyenek $p,q>2$ prímek. Ekkor

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

(Ezzel iterálva bármely Legendre-szimbólum gyorsan kiszámítható.)
(polinomiális időben)

Másképp $\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{ha } p \text{ és } q \text{ közül legalább az egyik } 4k+1 \text{ alakú} \\ -\left(\frac{q}{p}\right), & \text{ha egyik sem } 4k+1 \text{ alakú} \end{cases}$.

B: NB. (pl. Gauss-lemmával lehet, de van sok másik. Sárközy egy barátja gyűjti őket. 40 éve már 49-nél járt.)

A $+1, -1$ véletlenszerűen váltakoznak $\rightarrow$ véletlenszám-generálás.

Ide kapcsolódik: Jacobi-szimbólum.

Eddig tartott a standard bevezető számelmélet kurzus.

Prímszámelmélet

Konvenció. Most csak pozitív prímekre szorítkozunk.

Tétel (Euklidész) Végtelen sok prímszám létezik.

B: Az euklideszi gondolatmenettel.

$\nexists$ véges sok prím létezik: legyenek ezek $p_1 = 2,\ p_2 = 3,\ \dots,\ p_k$.

$A \overset{\text{def}}{=} p_1 p_2 \cdots p_k + 1$.

$A \geq 2 + 1 > 1 \Rightarrow$ az alaptétel szerint A felírható prímek szorzataként

$\Rightarrow \exists\, q_i$ prímosztója, $q_i \mid A$.

A bármely p_i-vel osztva 1 maradékot ad $\Rightarrow \forall i\ p_i \neq q_i$, mert q_i-vel osztva 0 a maradék.

$\Rightarrow$ találtunk egy további prímet $\lightning$ $\square$

Ebből lehetne becslés, de nem elég erős.

Lehetne pl. a Fermat-számokkal is bizonyítani (vagy gyakorlatok), de ez is gyenge becslés.

Definíció. Az x-nél nem nagyobb (pozitív) prímek száma $\pi(x)$.

Tétel. $\exists\, c_1, c_2$ pozitív állandók, hogy $x \geq 2$-re

(1) $\quad c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x}$

(x-ig „sok", $c_1 \frac{x}{\log x}$ prím van, de a számokra csak ennyi, $\log x$-ed része prím.)

B: Kombinatorikus számelméleti eszközökkel.

Elég igazolni, hogy alkalmas c_1, c_2-vel elég nagy x-re teljesül.

(mert ekkor c_1 csökkentésével, c_2 növelésével kisebb x-ekre is igazzá tehető.)

1. lemma. Ha $n \in \mathbb{N}$, p prím, melyre $n < p \leq 2n$, akkor

$$p \mid \binom{2n}{n}.$$

B: $p \mid n! \binom{2n}{n} = \frac{(2n)!}{n!} = (2n)(2n-1)\cdots(n+1) \Rightarrow$ valamelyik tényező épp p.

$(p; n!) = 1$, mert $p > n$.

$$\Rightarrow p \mid \frac{n!\binom{2n}{n}}{n!} = \binom{2n}{n}.$$

1

2. lemma. $n \in \mathbb{N}$: $\binom{2n}{n} < 4^n$.

B: $\binom{2n}{n} < \binom{2n}{0} + \binom{2n}{1} + \dots + \binom{2n}{n} + \dots + \binom{2n}{2n} = (1+1)^{2n} = 4^n$

2

3. lemma. Tetszőleges $n \in \mathbb{N}$, $n > 1$ számra $\pi(2n) - \pi(n) = \sum_{n < p \leq 2n} 1 < \log 4 \frac{n}{\log n}$.

B: 1. lemma $\Rightarrow \prod_{n<p\leq 2n} p \mid \binom{2n}{n} \Rightarrow$ (2): $\prod_{p} p \leq \binom{2n}{n} < 4^n$

(3): $\prod_{n<p\leq 2n} p > \prod_{n<p\leq 2n} n = n^{\pi(2n)-\pi(n)}$

(2) és (3): $n^{\pi(2n)-\pi(n)} < 4^n$. $\log$ monoton nő

$\log\left(n^{\pi(2n)-\pi(n)}\right) < \log(4^n)$

$(\pi(2n) - \pi(n)) \cdot \log n < n \log 4$

$$\pi(2n) - \pi(n) < \log 4 \frac{n}{\log n}.$$

3

Legyen $u, v > 0$ úgy, hogy $\quad 2^u \le \sqrt{x} < 2^{u+1}$,
$\quad 2^{v-1} \le \sqrt[4]{x} \le 2^v$.

A 3. lemma szerint:

$$\pi(x) \underset{\pi \text{ monoton}}{\le} \pi(2^v) = \sum_{k=1}^{v} \left(\pi(2^k) - \pi(2^{k-1})\right) + \underbrace{\pi(1)}_{0} = \sum_{k=u+1}^{v} \left(\pi(2^k) - \pi(2^{k-1})\right) + \underbrace{\sum_{k=1}^{u} \left(\pi(2^k) - \pi(2^{k-1})\right)}_{\pi(2^u) \le \pi(\sqrt{x}) \le \sqrt{x}}$$

$$< \sum_{k=u+1}^{v} < \log 4 \frac{2^{k-1}}{\log 2^{k-1}} + \sqrt{x} \le \sum_{k=u+1}^{v} \log 4 \frac{2^{k-1}}{\log 2^u} + \sqrt{x} \le$$

$$\le \frac{3 \log 4}{\log x} \sum_{k=u+1}^{v} 2^{k-1} + \sqrt{x} < \frac{6 \log 4}{\log x} \cdot x + \sqrt{x} < 12 \frac{x}{\log x} + \frac{x}{\log x} = 13 \frac{x}{\log x}.$$

Ez volt a felső becslés, az alsó hasonlóan kijönne (NB). □

Mennyire éles ez a becslés?

Definíció. Azt mondjuk, hogy $f(x)$ aszimptotikusan egyenlő $g(x)$-szel ($x \to \infty$ esetén), ha

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

Az 1800-as évek végén Hadamard (fr.), de la Vallée Poussin bizonyította:

Tétel (Prímszámtétel): $x \to \infty$ esetén $\pi(x) \sim \frac{x}{\log x}$.

A Riemann-sejtésből kijönne.
A prímszámtételre az 1940-es években Erdős és Selberg adtak az eredeti analitikus bizonyításnál is bonyolultabb elemi bizonyítást. Sajnos ebből sem jött ki a Riemann-sejtés, pedig sokan remélték, hogy ha erre megyünk az elemi, abból kijön.

A prímek eloszlása

Először: olyan tételek keresése, hogy bizonyos speciális alakú számok között ∞ sok prím létezik.
Fermat először: $2^{2^n} + 1 \to$ téves, $n = 5$. Kérdés (nyitott): a Fermat-számok között van-e ∞ sok prím.
Mersenne: van-e ∞ sok $2^p - 1$ alakú Mersenne-prím?

Tétel. Végtelen sok $4k-1$ alakú prím létezik.
B: Lemma. Ha $n = 4k-1$ alakú természetes szám, akkor van $4m-1$ alakú prímosztója.
B: Ha n-nek $\nexists$ $4m-1$ alakú prímosztója $\Rightarrow n = p_1 \cdots p_l$. Mindegyik $p_i \neq 2$
$\Rightarrow \forall p_i$ 1 maradékot ad 4-gyel osztva $\Rightarrow p_1 \cdots p_l \equiv 1 \ (4)$ ↯ □

Tfh. csak véges sok $4k-1$ alakú prím $\exists$: $p_1 = 3, p_2 = 7, \ldots, p_n$.
$A \overset{\text{def}}{=} 4p_1 p_2 \cdots p_n - 1$. A lemma szerint A-nak van $4m-1$ alakú prímosztója: q_r.
De A $p_1, \ldots, p_n$-nel osztva -1 maradékot ad. $\to q_r \neq p_1, \ldots, p_n$. ↯ □

12. 9.

Tétel. Végtelen sok $4k+1$ alakú prím létezik.
B: Lemma. Ha $u \in \mathbb{N}$, p prím, $p \mid 4u^2 + 1$, akkor p $4l+1$ alakú.
B: $4u^2 + 1$ pth. $\Rightarrow p$ pthan. $1 + 4u^2 \equiv 0 \ (p)$, $4u^2 \equiv -1 \ (p)$, $(2u)^2 \equiv -1 \ (p)$.
$2u = x \longrightarrow x^2 \equiv -1 \ (p)$ megoldható $\Rightarrow \left(\frac{-1}{p}\right) = +1 \Rightarrow p = 4l+1$ tanult tétel. □

Tfh. csak véges sok $4k+1$ alakú prím $\exists$: $p_1 = 5, p_2 = 13, \ldots, p_n$.
$A \overset{\text{def}}{=} 4u^2 + 1$, $u = p_1 \cdots p_n \to A$-nak van $4k+1$-es prímosztója, de $A \bmod p_i = 1$.
(SZAT és lemma) □

Elemileg még belátható: $\exists$ $ak \pm 1$ alakúból ∞ sok.

Tétel. (Dirichlet tétele): $a \in \mathbb{N}$, $b \in \mathbb{Z}$, $(a,b) = 1$ $\Rightarrow$ $\exists$ ∞ sok $ak + b$ alakú prím.
B: NB. $\square$

Az $(a,b) = 1$ szükséges is: $d = (a,b) > 1 \longrightarrow d \mid ak + b \quad \forall k \in \mathbb{N}$
$\Rightarrow$ legfeljebb 2 esetben lesz $ak+b$ prím (ha d prím és $ak+b = \pm d$).

A Dirichlet-tétel átfogalmazható: $f(n) = an + b \in \mathbb{Z}[n]$ ∞ sok prímet állít elő alkalmas $n \in \mathbb{N}$-ekre.

Igaz-lehet-e magasabb fokú polinomokra?
Sejtés. ∞ sok n^2+1 alakú prím van. $\longrightarrow$ igen plauzibilis, hogy igaz
Iwaniec. $\exists$ ∞ sok n^2+1 alakú prím szám van, ami max. 2 prím szorzata.
(Iwaniec szerint ez a legnehezebb tétele.)
Egyetlen olyan másodfokú polinom sincs, amiről konkrétan tudjuk, hogy ∞ sok prímet állít elő.

Prímdifferenciák

Legyen az n-edik prímszám p_n, az n-edik prímdifferencia $d_n = p_n - p_{n-1}$

Tétel. Tetszőlegesen nagy $k \in \mathbb{N}$-et megadva $\exists n$, hogy $d_n > k$.
B: Levezethető lenne $\frac{\pi(x)}{x} \to 0$-ból (egzisztencia bizonyítás).
Konstruktív bizonyítás:
$k! + 2$, $k! + 3$, ..., $k! + k$ mindegyike összetett: $k! + i$-re $(2 \le i \le k)$
$\longrightarrow$ $i \mid k! + i$ és $i \neq k! + i$. i valódi osztó.
Ha $p_{n-1} < k! + k < p_n$ $\longrightarrow$ $d_n \geq (k! + k + 1) - (k! + 1) = k$. $\square$

Sejtés. $n \in \mathbb{N}$: n^2 és $(n+1)^2$ közt van prím.
Más változatban: n^2 és $n^2 + n$ közt van prím.
} reménytelen változat: $\forall \varepsilon$ $\forall n > n_0(\varepsilon)$: n és $n + n^{\varepsilon}$ közt van prím.
Tudjuk már: $n^2 + n^{1,05}$ között van (Pintz – Iwaniec)
∞ sok n-re n és $n + c \log n$ között van prím.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...
$d_2 = 1$, az nyilván nem lesz még egyszer

Definíció. $d_n = p_n - p_{n-1} = 2$ $\Rightarrow$ p_n és p_{n-1} ikerprímek.
Sejtés. $\exists$ ∞ ikerprím.
Erdős: ∞ n-re $d_n < (1-\varepsilon) \log n$.
Nemrég Pintzék: $O(\sqrt{\log n})$.
Zhang pár éve: $d < 300$ ∞ sokszor. Azóta ezt nyomják lefele: most kp. 60-nál járnak.
$\longrightarrow$ ezek mostanában felgyorsítatták a stagnáló prímszámelméletet.

Prímösszegek

Sejtés. (Goldbach):
a) $\forall$ 2-nél nagyobb ps szám felírható 2 prím összegeként.
b) $\forall$ 5-nél nagyobb pt szám felírható 3 prím összegeként.

a) a nehezebb: a) $\Rightarrow$ b).
Tétel (Vinogradov, kb. 1940): $\exists$ n_0: $\forall$ n_0-nál nagyobb pt szám felírható 3 prím összegeként.
Vgr. bizonyította ~~előtt~~ rendesen. Korábban Hardy és Littlewood az általánosított Riemannból kihozták.
n_0 iszonyú nagy.

Tétel. (Vaughan, '70-'80-as évek)

$\forall$ 1-nél nagyobb ptl szám felírható max. 5 prím összegeként.

Most már közelében vagyunk a páratlan Goldbachnak. A páros messze, csak részeredmények.

Tétel. (Rényi, '50-es évek)

$\forall$ 2-nél nagyobb ps felírható 2 szám összegeként, melyek közül az egyik prím, a másik majdnem prím, azaz $\exists$ c állandó, hogy legfeljebb c faktora van (multiplicitással): $p+q = 2n$, p prím, $\Omega(q) \leq c$.

Chen: $c = 2$-re levitte.