matekdebrecen@gmail.com

matek2008

VIZSGAIDŐPONT

11.21. péntek 10-12 K/2

- feladatok GY jegy

- elm. E jegy

12.22. 14^{00}
! ↓ ki kell venni !

60p. 6 feladat 3 gy + 3 elm. – tétel – def.

2 feladat → először

1 feladat → most (tompacciás)

ELTE: Ambrus J.
Bolyai diff. c.

diff.-a → konkáv
szám → számok → konkáv
lagr. → lehet
konkáv diff.e. kétsor
számok → szám → nincs határ

Dr. Bérczes Attila

Fried-Gyarmati: Számelmélet (ELTE)

vizsga: írásbeli
tan: ea. (T, dij, pé.) + feladatok

Sárközi-Surányi (ELTE) első pár fejezet
Zöld összefoglaló + más középiskolai könyvek

időpont:

Számelméleti alapfogalmak:

1.1.1. Def.

$\forall\, b \in \mathbb{Z}$ az $a \in \mathbb{Z}$ osztójának van, ha $\exists\, q \in \mathbb{Z}$, amelyre
$a = bq$

jel.: $b \mid a$

$\forall$ 0 minden számmal osztható, hiszen $\forall\, b$ esetén $0 = b \cdot 0$

1.1.2. Def:

Ha egy szám $\forall$ számnak osztója $\Rightarrow$ EGYSÉG-nek nev.

1.1.3. Tétel:

Az egész számok körében 2 egység van, az 1 és -1.

Biz.

1.1.4. Tétel:

Ha ε és δ egységek és $b|a \Rightarrow \varepsilon b | \delta a$ is teljesül.

asszociáltak: ha pl. b egy egységszeresétől tekintem.

1.1.5.

- Minden a-ra $a|a$: a reflexív
- Ha $c|b$ és $b|a \Rightarrow c|a$
- $a|b \wedge b|a \Leftrightarrow$ ha a és b egymás asszociáltjai (egység szerese)
- $c|a \wedge c|b \Rightarrow c|a+b$, $c|a-b$ $\forall (k \in \mathbb{Z})$, $c|ka$,

$\wedge \forall r \in \mathbb{Z}, s \in \mathbb{Z}$ $c|\underbrace{ra+sb}$

egész együtthatós lineáris kombinációját.

Biz:

$\rightarrow$ Ha $a = \varepsilon b$ (ε egység) $\Rightarrow b|a$

$1 = \varepsilon r$ miatt $ra = b$, tehát $a|b$

$\leftarrow$ $a|b \wedge b|a$, azaz $q, s \in \mathbb{Z}$ -vel

$$b = aq \wedge a = bs \Rightarrow b = b(qs)$$

Ha $b = 0 \Rightarrow a = 0$, tehát $a = \varepsilon b$.

Ha $b \neq 0 \Rightarrow qs = 1$, azaz $s \wedge q$ is egység $\Rightarrow a = \varepsilon b$.

Maradékos osztás:

1.2.1 Tétel

$\forall a, b \neq 0 \ (\in \mathbb{Z})$ $\exists$ q és r, melyekre

$$a = bq + r \ \wedge \ 0 \leq r < |b| .$$

$q \wedge r$ egyértelműen meghatározott.

Biz: ! $b > 0$

$$0 \leq r = a - bq < b$$

pontosan akkor teljesül, ha

$$bq \leq a < b(q+1)$$

$$\Downarrow$$

$$q \leq a/b < q+1$$

Ha $b < 0 \Rightarrow$

$$0 \leq r = a + bq < |b| = -b$$

feltétel: $q \geq a/b > q-1$

[A maradék pozitív legyen!]

1.2.1.A Tétel

$\forall a$ és $b \neq 0 \ (\in \mathbb{Z})$ $\exists$ egyértelműen meghatározott $q, r \ (\in \mathbb{Z})$, melyekre

$$a = bq + r \quad \wedge \quad -\frac{|b|}{2} < r \leq \frac{|b|}{2}$$

Legyen r-ek a legkisebb abszolút értékű maradékai nemnulla.

Példa:

$$30 = (-8)\cdot(-3) + 6 = (-8)\cdot(-4) - 2$$

$a = 30 \qquad b = -8$

1.2.2. Tétel:

$\exists!\ t > 1$ rögzített egész.
$\forall A \in \mathbb{Z}^+$ egyértelműen felírható

$$A = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$$

ahol $0 \le a_i < t$ $\wedge$ $a_n \neq 0$.

Legnagyobb közös osztó:

1.3.1. Def:

a, b számok közös osztója a d, ha

1) $d \mid a$, $d \mid b$
2) ha $\forall c$-re $c \mid a$, $c \mid b \Rightarrow |c| \le |d|$

asszociáltaktól (egységszorzótól) eltekintve a közös egyértelmű.

Ha $a = b = 0 \Rightarrow \nexists$ közös, mert minden egész szám közös.

1.3.2 Def:

a, b kitüntetett közös osztója δ, ha

1) $\delta \mid a \wedge \delta \mid b$
2) $\forall c$-re $c \mid a, c \mid b \Rightarrow c \mid \delta$

kitüntetett közös osztót minden osztó osztja.

Ha $a = b = 0 \Rightarrow$ közös def. nemlet 0.

Ha $\exists \delta$ közös $\Rightarrow \delta$ csak a közös valamelyike lehet.

$$\left.\begin{array}{l} |\delta| \le |d| \\ d \mid \delta \Rightarrow |d| \le |\delta| \end{array}\right\} \Rightarrow |d| = |\delta| = \delta = d$$

1.3.3. Tétel:

$\forall$ két egész számnak $\exists$ közös-ja.

Ha $b \nmid a \Rightarrow q_i, r_i\ (\in \mathbb{Z})$-vel

$$a = bq_1 + r_1 \quad , 0 < r_1 < |b|$$

$$b = r_1 q_2 + r_2 \quad , 0 < r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \quad , 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n \quad , 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} \qquad (r_{n+1} = 0)$$

Az eljárás hetedik lépésben befejeződik véges sok lépésben, mert a

maradékok nemnegatív egészekből álló szigorúan csökkenő sorozatot alkotnak.

$$|b| > r_1 > r_2 > \dots$$

VÉGTELEN LEZÁRÁSS MÓDSZERE

Az utolsó nem nulla maradék lesz a keső.

Nagy! Euklidészi algoritmus !!! (kell!) Bizonyítással!

Pl: $(128, 24) = ?$

$128 : 24 = 5 \quad m : 8 \quad \rightarrow \quad 128 = 24 \cdot 5 + 8$

$128 \cdot 24 = 5$
$\quad 8$

$24 = 8 \cdot 3 + 0$

$(134; 24) =$

$134 = 24 \cdot 5 + 14$
$24 = 14 \cdot 1 + 10$
$14 = 10 \cdot 1 + 4$
$10 = 4 \cdot 2 + 2$
$4 = 2 \cdot 2 + 0$

} Ez a célszerűbb!

Folyamatban!

$134 = 24 \cdot 6 + (-10)$
$24 = 10 \cdot 2 + 4$
$10 = 4 \cdot 2 + 2$
$4 = 2 \cdot 2$

v. $24 = (-10)(-2) + 4$
$-10 = 4 \cdot (-3) + 2$

1.3.4. Tétel:

Ha $c > 0 \Rightarrow (ca, cb) = c(a, b)$

Biz:

1.3.5. Tétel:

Az $a \wedge b$ számok lineáris alakja előáll $\forall u, v \in \mathbb{Z}$ esetén

$(a, b) = au + bv$ alakban.

Biz.

$$14 = \underset{a}{134} - \underset{b}{24} \cdot 5$$

$$10 = 24 - 14 \cdot 1$$

$$4 = 14 - 10 \cdot 1$$

$$2 = 10 - 4 \cdot 2$$

$2 = 10 - 4 \cdot 2 = 10 - (14 - 10 \cdot 1) \cdot 2 = 10 - 14 \cdot 2 + 10 \cdot 2 =$

$= 10 \cdot 3 - 14 \cdot 2 = (24 - 14 \cdot 1) \cdot 3 - 14 \cdot 2 = 24 \cdot 3 - 14 \cdot 3 - 14 \cdot 2 =$

$= 24 \cdot 3 - 14 \cdot 5 = 24 \cdot 3 - (134 - 24 \cdot 5) \cdot 5 = 24 \cdot 3 - 134 \cdot 5 + 24 \cdot 25 =$

$= 24 \cdot (28) - 134 \cdot (5)$ a keresett együtthatók: 28 és -5

1.3.6. Tétel:

! $a, b, c \in \mathbb{Z}$ rögzített.

$ax + by = c$ diofantikus egyenletnek $\Leftrightarrow$ $\exists$ megoldása, ha

$(a, b) \mid c$.

Biz.

1.3.7. Def:

Az $a_1, a_2 \dots a_n$ számok relatív prímek, ha csupa 1.

1.3.8. Def:

Az $a_1, a_2 \dots a_n$ számok páronként relatív prímek, ha közülük semelyik kettőnek sincs egynél(től különböző) közös osztója,

azaz: $\forall\ 1 \le i \ne j \le n$ esetén $(a_i; a_j) = 1$.

$(2; 3; 6; 7) = 1$

rel. prím, de nem páronként rel. prímek.

1.3.9. Tétel:

Ha $c \mid ab$ és $(c, a) = 1 \Rightarrow c \mid b$.

Felbonthatatlan szám és prímszám:

1.4.1. Def

A p egynél(től) (± 0) különböző számot FELBONTHATATLAN SZÁM-nak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység.

Azaz: $p = ab \Rightarrow a$ v. b egység

„bizáró vagy"

1.4.2 Def:

A p egynél(től) és nullától különböző számot PRÍMSZÁMNAK nevezzük, ha csak úgy lehet osztója két egész szám

szorzatának, ha legalább az egyik tényezőnek osztója.

$p \mid ab \Rightarrow p \mid a$ v. $p \mid b$.

„megengedő vagy"

1.4.3 Tétel:

A egész számok körében p prím $\Leftrightarrow$, ha felbonthatatlan.

1.5.1. Tétel (A számelm. alaptétele)

$\forall$ 0-tól és egynél(től) különböző egész szám felbontható véges sok felbonthatatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve és az egység-tényezőktől eltekintve egyértelmű.

Kanonikus alak:

1.6.1 Tétel

$\forall\ n > 1 (\in \mathbb{Z})$ felírható

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i} \text{ alakban.}$$

...

1.6.2 Tétel

Az $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ kanonikus alakú n számnak egy d pozitív egész $\Leftrightarrow$ osztója, ha d kanonikus alakja $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$, ahol $0 \le \beta_i \le \alpha_i$, $i = 1, 2 \dots r$.

1.6.3. Tétel:

Az $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ kanonikus alakú n szám

pozitív osztóinak a száma $d(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$.

1.6.4. Tétel

Az $a, b\ (\in \mathbb{Z}^+)$ kanonikus alakja

$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ és $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$, ahol $\alpha_i \geq 0$, $\beta_j \geq 0$.

Ekkor $(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_r^{\min(\alpha_r,\beta_r)}$

$\min(\alpha_i, \beta_i) \Rightarrow \alpha_i$ és β_i számok közül a kisebbiket jelenti,
ha $\alpha_i \neq \beta_i$ ill. a közös értéküket, ha $\alpha_i = \beta_i$

1.6.5. Def

Az a és $b\ (\in \mathbb{Z}^+)$ közül a $t \in (\mathbb{Z}^+)$, ha

- $a \mid k$, $b \mid t$ és

- ha $c > 0$, $a \mid c$, $b \mid c$ teljesül $\Rightarrow c \geq t$.

1.6.6. Tétel

$$!\ \cdot\ \cap\ !$$

$2 \mid 6$ ~~$4 \mid 8$~~

$5 \mid 30$ ~~$6 \mid 30$~~

$24 \mid a(a+1)(a+2) = A$

$6 \mid A$, $4 \mid A$ $\Rightarrow 12 \mid A$

$2^3 \mid A$, $3 \mid A$ $\Rightarrow 2^3 \cdot 3 \mid A$

Feladat:

$24 \mid a(a+1)(a+2) = A$ $\quad \forall a \in \mathbb{N}$ páros

$24 = 2^3 \cdot 3$

1) belátjuk, h. $3 \mid A$

$a, a+1, a+2$ (3 egymást követő szám) $\Rightarrow$ ezek valamelyikét biztosan osztja.

$\Downarrow$

szorzatukat is osztja

2) belátjuk, h. $2^3 \mid A$

$2 \mid a$

$2 \mid a+2$

$a, a+2$ két egymást követő páros szám $\Rightarrow$ egyikük osztható 4-gyel.

$\Downarrow$

$a \cdot (a+2)$ osztható 8-cal

$\Downarrow$

$2^3 \mid A$

$\Downarrow$

$2^3 \mid A$, $3 \mid A \Rightarrow 24 \mid A$.

$\Downarrow$

$[2^3\ 3]$

1.67. Tétel

$$(c, ab) = 1 \Leftrightarrow (c,a) = 1 \wedge (c,b) = 1$$

1.68. Tétel

Legendre-formula

A $n!$ kanonikus alakja:

$$n! = \prod_{p \le n} p^{a_p}, \text{ ahol } a_p = \sum_{\ell=1}^{\infty} \left[\frac{n}{p^\ell} \right].$$

FELADATOK

1) Biz. be, hogy

$$120 \mid a^5 - 5a^3 + 4a \qquad \forall a \in \mathbb{Z}$$

$$120 \mid a(a^4 - 5a^2 + 4) = a(a^2-1)(a^2-4) \Rightarrow$$

$$120 \mid a(a+1)(a+2)(a-1)(a-2)$$

$$120 \mid (a-2)(a-1)a(a+1)(a+2) = A$$

5 egymást követő szám szorzata

$120 = 2^3 \cdot 3 \cdot 5$

$5 \mid A$ ✓
$3 \mid A$ ✓
$2^3 \mid A$ ✓

$\Big\} \Rightarrow 120 \mid A$ ✓

Szöveget írni kérek!!!
2x-ben

8-cal

$$(a-2)(a-1)\,a\,(a+1)(a+2)$$

2^6

2 2 2

2 2 2

4-gyel 4-gyel

ha $a : 2$-vel osztható, de 4-gyel nem.

2)

$n \in \mathbb{N}$ páros.

$8 \mid n^2 - 1$

$8 \mid (n-1)(n+1)$

$2 \mid n-1$

$2 \mid n+1$

2 egymást követő páros szám: 1 osztható 4-gyel.

$n = 2\ell + 1 \qquad \ell \in \mathbb{N}$

$(2\ell+1)^2 - 1 = 4\ell^2 + 4\ell + 1 - 1 = 4 \cdot \underbrace{\ell(\ell+1)}_{2a \text{ alakú}}$

$\overset{1)}{\Rightarrow} 8 \mid n^2 - 1$

Időközben segít, ha a szám maradékos alakját felírjuk, és minden maradékosztályra megnézzük.

09. 20.
17[00]

Feladatok:

1) Bizonyítsuk be!

$\forall n \in \mathbb{N}$ $\quad 121 \mid n^2+3n+5$

2) Bizonyítsuk be!

$\forall a,b \in \mathbb{Z}$ $\quad 30 \mid ab(a^4-b^4) = ab(a^2+b^2)(a^2-b^2)$

$ab(a^2+b^2)(a+b)(a-b)$

3) Bizonyítsuk be!

$\forall n \in \mathbb{N}$ $\quad 19 \mid 2^{6n+2}+3$

4) Bizonyítsuk be!

5 $\nmid 3n^2+2n+1 = A$

(a) $n = 5k$

5 $\nmid 3 \cdot 25k^2 + 2 \cdot 5 + 1 = \not\phi$

(b) $n = 5k+1$

$A = 3 \cdot (25k^2+10k+1) + 2(5k+1) + 1 =$

$= 75k^2 + 30k + 3 + 10k + 2 + 1 = 75k^2 + 40k + 6$

(c) $n = 5k-1$

$A = 3 \cdot (25k^2-10k+1) + 2(5k-1) + 1 =$

$= 75k^2 - 30k + 3 + 10k - 2 + 1 = 75k^2 - 20k + 2$

(d) $n = 5k+2$

$A = 3 \cdot (25k^2+20k+4) + 2(5k+2) + 1 =$

$= 75k^2 + 60k + 12 + 10k + 4 + 1 = \not\phi$

(e) $n = 5k-2$

$A = 3(25k^2-20k+4) + 10k + 4 + 1$

$= 75k^2 - 60k + 12 + 10k + 4 + 1 = \not\phi$

5)

$n \in \mathbb{Z}$ $\qquad a^3-b^3=(a-b)(a^2+ab+b^2)$

$(n-3) \mid n^3-3$

6) $\frac{2a+3}{a-2} = \frac{2a-4+7}{a-2} = \frac{2a-4}{a-2} + \frac{7}{a-2} =$

$= 2 + \frac{7}{a-2} \in \mathbb{Z}$ $\qquad a-2 = \pm 1$ v $a-2 = \pm 7$

$a=3$ $\quad a=1$ $\quad a=9$ $\quad a=-5$

5) $\frac{n^3-3}{n-3} =$

$n^3 - 3 : n-3 = n^2+3n+9$

n^3-3n^2

$3n^2-3$

$3n^2-9n$

$9n-3$

$9n-27$

24

$\frac{(n-3)(n^2+3n+9)+24}{n-3} = n^2+3n+9 = \frac{24}{n-3}$

$n-3 = \pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 8; \pm 12; \pm 24$

7) Bizo.!

$\forall n \in \mathbb{N}$

$5 \mid 2^{4n+1}+3$

$n=1$-re

$5 \mid 2^{4\cdot1+1}+3$

$5 \mid 2^5+3 = 35$ ✓

($n=2$-re $\qquad 5 \mid 2^{4\cdot2+1}+3$ $\qquad 5 \mid 2^9+3 = 515$ ✓

$n=3$-ra $\qquad 5 \mid 2^{4\cdot3+1}+3$ $\qquad 5 \mid 2^{13}+3$ ✓)

Hip.: $n=k$-ra igaz.

$5 \mid \underbrace{2^{4k+1}+3}_{A}$

Bizonyítsuk: $n=k+1$-re.

$5 \mid 2^{4(k+1)+1}+3$

$5 \mid 2^4 \cdot (2^{4k+1}+3) - 2^4 \cdot 3 + 3 = 2^4 \cdot 5A - 3(16-1) = 5B$

$2^{4n+1}+3 = 2\cdot(2^4)^n+3 = 2\cdot(15+1)^n+3 =$

$= 2(5C+1)+3 = 10C+5$ $\quad :5$

↓ maradék 5-tel

8) Bizonyítsuk be! $x \in \mathbb{N}$

$(x-1)^3 + (x)^3 + (x+1)^3$ osztható

ⓐ a középső számmal

ⓑ 9-cel

$x^3 - 3x^2 + 3x - 1 + x^3 + x^3 + 3x^2 + 3x + 1 =$

$3x^3 + 6x = 3x(x^2+2)$

$3a \mid A$ $\Rightarrow$ $9a \mid A$ $\Rightarrow$ ha $3 \mid a \Rightarrow$ lehet $: 3a$

$9 \mid A$ $\Rightarrow$ $9a \nmid A$!

$\Rightarrow [3a; 9] \mid A$

ⓐ $3x \mid 3x(x^2+2)$ ✓

$9 \mid 3x(x^2+2)$

ha $3 \mid x$ ✓

ha $n = 1$. ✓

ha $n = 2$ ✓

9) Bizonyítsuk be!

$13 \mid 2^{70} + 3^{70}$

$2^{70} + 3^{70} = 4^{35} + 9^{35} = (4+9)(4^{34} - 4^{33} \cdot 9 + 4^{32} \cdot 9^2 + \dots + 9^{34}) =$

$= 13 \cdot A$

Ha n páratlan ($n \in \mathbb{N}$) $\Rightarrow a^n + b^n = (a+b)(a^{n-1} - a^{n-2} \cdot b + \dots + b^{n-1})$

$n \in \mathbb{N}$ $a^n - b^n = (a-b)(a^{n-1} + a^{n-2} b + \dots + b^{n-1})$

10) Bizonyítsuk be!

hogy az alábbi törtek egyetlen egész számra sem egyszerűsíthetők!

ⓐ $\frac{a-1}{2a-1}$

ⓑ $\frac{2a+1}{3a+1}$

ⓒ $\frac{a^3+2a}{a^4+3a^2+1}$

ⓐ $\frac{a-1}{2a-1}$

Tfh: $b \mid a$, $b \mid a-1$ $\Rightarrow b \mid a-(a-1) \Rightarrow b \mid 1 \Rightarrow b = \pm 1$

ⓐ $\left.\begin{array}{l} b \mid a-1 \\ b \mid 2a-1 \end{array}\right\} b \mid 2a-1-2(a-1) \Rightarrow b \mid 1$

ⓑ $\left.\begin{array}{l} b \mid 2a+1 \\ b \mid 3a+1 \end{array}\right\} b \mid 3(2a+1)-2(3a+1) \Rightarrow b \mid 1$

ⓒ $b \mid a^3+2a$

$b \mid a^4+3a^2+1$

$$\frac{a^3+2a}{a^4+3a^2+1} = \frac{a(a^2+2)}{a^4+3a^2+1} = \frac{a(a^2+2)}{(a^2+2)(a^2+1)-1}$$

Tfh: p prím és $p \mid a(a^2+2) \Rightarrow$

$p \mid a$ v. $p \mid a^2+2$ (p prím, $p \neq \pm 1$)

I: $p \mid a \Rightarrow p \mid a^4+3a^2 \Rightarrow p \nmid a^4+3a^2+1$

II: $p \mid a^2+2 \Rightarrow p \mid (a^2+2)(a^2+1) \Rightarrow p \nmid (a^2+2)(a^2+1)+1 \Rightarrow$

$\Rightarrow p \mid a^4+3a^2+1$

11) Bizonyítsuk be!

$\forall n \in \mathbb{N}$

$6 \mid n \cdot (2n+1)(7n+1)$

a) $2 \mid n(2n+1)(7n+1)$

ha n páros ✓

ha n páratlan $2 \mid n(2n+1)(7n+1)$ ✓
($2n+1$: páros, $7n+1$: páros)

b) $3 \mid n(2n+1)(7n+1)$

$n = 3k$ ✓

$n = 3k+1$

$3 \mid (3k+1)(6k+2+1)(21k+7+1)$

$3 \mid 3k+3$ ✓

$n = 3k-1$

$3 \mid (3k-1)(6k-2+1)(\underbrace{21k-7+1}_{3 \mid 21k-6})$ ✓

Tehát: $6 \mid n(2n+1)(7n+1)$

→ Lehet 6-tal való osztási maradékkal is vizsgálni!

$6 \mid 14n^3+9n^2+n$ → Teljes indukcióval!

12) Bizonyítsuk be!

Ha a páratlan ($\in \mathbb{N}$) $\Rightarrow 2^{n+2} \mid a^{2^n}-1$

$n=1$ ✓ $\quad 2^3 \mid a^2-1$

$2^3 \mid (a-1)(a+1)$ ✓
($a-1$: páros, $a+1$: páros; v. valamelyik 4-gyel osztható)

Tfh:
$n = k$

Biz. $n = k+1$-re.

$$a^{2^{k+1}} - 1 = a^{2\cdot 2^k} - 1 = \left(a^{2^k}\right)^2 - 1 = \underbrace{\left(a^{2^k}-1\right)}_{2^{k+2}\cdot A}\underbrace{\left(a^{2^k}+1\right)}_{2B} =$$

$$= \underbrace{2^{k+3}}_{2^{k+2}\cdot 2} AB$$

$$a^{2^n} - 1 = \left(a^{2^{n-1}}+1\right)\left(a^{2^{n-1}}-1\right) = \left(a^{2^{n-1}}+1\right)\left(a^{2^{n-2}}+1\right)\left(a^{2^{n-2}}-1\right) =$$

$$= \left(a^{2^{n-1}}+1\right)\left(a^{2^{n-2}}+1\right)\cdots\left(a^{2^1}+1\right)\left(a^2-1\right)$$

$n-1$ db 2-es (2) (2) $\downarrow\ 2^3$ $\Rightarrow 2^{n+2}$ db 2-es összesen

1)

$$121 \nmid n^2+3n+5$$

$$n^2+3n+5 = \underbrace{(n+7)(n-4)}_{n^2+3n-28} + \underbrace{33}_{\text{osztható 11-gyel}}$$

$n+7$, $n-4$ — 11

$\Rightarrow$ vagy mind a kettő osztható 11-gyel, így az egész kifejezés is, vagy nem, $\Rightarrow$ a kif. sem.

I.

$$11 \mid \underbrace{n+7 \Rightarrow 11 \mid n-4}$$

$$121 \mid (n+7)(n+4) \Rightarrow 121 \nmid (n+7)(n-4) + 33 =$$

$$= n^2+3n+5$$

II

$$11 \nmid \underbrace{(n+7) \Rightarrow 11 \nmid (n-4)}$$

$\Downarrow$

$$11 \nmid (n+7)(n-4) \Rightarrow 11 \nmid (n+7)(n-4)+33 \Rightarrow$$

$$\Rightarrow 121 \nmid n^2+3n+5$$

2)

$$ab\left(a^4-b^4\right) = ab\left[\left(a^4-1\right)-\left(b^4-1\right)\right] =$$

$$= ab\left[\left(a^2+1\right)(a+1)(a-1) - \left(b^2+1\right)(b+1)(b-1)\right] =$$

$$= ab\left[\left(a^2-4\right)(a+1)(a-1) + 5(a+1)(a-1) - \right.$$

$$\left. - \left(b^2-4\right)(b+1)(b-1) - 5(b+1)(b-1)\right] =$$

$$= ab\left[(a+2)(a-2)(a+1)(a-1) + 5(a+1)(a-1) - \right.$$

$$\left. - (b+2)(b-2)(b+1)(b-1) - 5(b+1)(b-1)\right] =$$

$$= \Big[\underbrace{(a+2)(a-2)(a+1)(a-1)}_{120\,A}ab + \underbrace{5\underbrace{(a+1)(a-1)}_{5C}}_{30C}ab -$$

$$- \underbrace{(b+2)(b-2)(b+1)(b-1)}_{120\,B}ab - 5\underbrace{(b+1)(b-1)}_{5D}ab\Big]$$

$30D$

11.07.

Kongruenciák

D

$m \mid a-b$

$a \equiv b \pmod m$ $\quad m$: modulus

$m \mid a-b \iff m \mid b-a$ ezért

Pl.: $a \equiv b \pmod m \iff b \equiv a \pmod m$

$11 \equiv 3 \ (3)$

$32 \equiv -1 \ (11)$

$21 \not\equiv 6 \ (10)$

T: i) $\forall a$-ra $a \equiv a \ (m)$ } reflexivitás.

ii) $a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$ } szimm.

iii) $a \equiv b \ (m) \wedge b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$ tranzitív ✓ } ekvivalenciareláció.

iv) $a \equiv b (m) \wedge c \equiv d (m) \Rightarrow a+c \equiv b+d (m) \wedge a-c \equiv b-d (m)$

v) $a \equiv b (m), c \equiv d (m) \Rightarrow ac \equiv bd (m)$

vi) $a \equiv b (m) \Rightarrow a+c \equiv b+c \ (m), a-c \equiv b-c \ (m)$

vii) $a \equiv b (m) \Rightarrow ac \equiv bc \ (m)$

viii) $a \equiv b (m) \Rightarrow a^k \equiv b^k \ (m)$

ix) $a \equiv b \ \ldots$

P1 P3

A kongruencia a rac. számokra nincs definiálva!

T: $ac \equiv bc \ (m) \wedge (c,m) = 1 \Rightarrow a \equiv b \ (m)$

T: $d = (c,m)$

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

$[a \cdot c \equiv b \cdot c \ (mc) \Rightarrow a \equiv b \ (m)] \qquad (c,m) = 1$

$\rightsquigarrow$ od 6-ra 2-nek nincs inverze

Maradékosztályok

2.2.1 Def $\quad \bar{a}$ $(a)_m$ → maradékosztály

$(a)_m = c_{(m)} \iff a \equiv c \pmod{\ }$

Vagy mogyoróval a halmaz, v. nincs közös eleme.

2.2.2. Def.:

Pl $\{33; -5; 11; -11; -8\} \pmod 5$ → teljes maradékrendszer $\pmod 5$

2.2.3. T

2.2.4 T **2.2.5 T**

2.26 D, 2.2.8 D

Példa! TK-ból

triviális maradékr. (mod 12)

$\{1, 5, 7, 11\}$

2. Gr. Tétel: páros maradékkal

kiszámítható kongr.

lin kongr.: $14x \equiv 21 \pmod{35}$ /:7

$(14; 21) = 7 \mid 35$

$2x = 3 \pmod 5$ $/ \cdot 2^{\varphi(5)-1}$

$2^{\varphi(5)} \cdot x \equiv 2^{\varphi(5)-1} \cdot 3 \pmod 5$

$x \equiv 2^3 \cdot 3 \quad (5)$

$x \equiv 4 \quad (5)$

$(4)_{35}$; $(9)_{35}$ $(14)_{35}$ $(19)_{35}$ $(24)_{35}$ $(29)_{35}$ $(34)_{35}$

11.08.

2.6.2 kínai maradéktétel

(B12) ⇒ konstruktív bizo.

1. pl

$2x \equiv 3 \quad (5)$

$3x \equiv 5 \quad (7)$

$5x \equiv 7 \quad (8)$

szimm. kongr. r.

$2x \equiv 3 \quad (5) \qquad (2,5) = 1 \mid 3$

$2^{\varphi(5)} x \equiv 2^{\varphi(5)-1} \cdot 3 \quad (5)$

$x \equiv 2^{4-1} \cdot 3 \quad (5)$

$x \equiv 2^3 \cdot 3 \quad (5)$

$x \equiv 4 \quad (5)$

$3x \equiv 5 \quad (7) \qquad (3,5) = 1 \mid 7$

$x \equiv 3^{\varphi(7)-1} \cdot 5 \quad (7)$

$x \equiv 3^{6-1} \cdot 5 \quad (7)$

$x \equiv 3^5 \cdot 5 \quad (7)$

$x \equiv 9 \cdot 9 \cdot 15 \quad (7)$

$x \equiv 4 \quad (7)$

$5x \equiv 7 \quad (8) \qquad (5,7) = 1 \mid 8$

$x \equiv 5^{\varphi(8)-1} \cdot 7 \quad (8)$

$x \equiv 5 \cdot 7 \quad (8)$

$\varphi(8) = 8 \cdot (1 - \frac{1}{2})$

$\varphi(6) = 6 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 2$

$\varphi(n) = n \cdot \prod_{p \mid n} (1 - \frac{1}{p})$

$x \equiv 5^{4-1} \cdot 7 \quad (8)$

$x \equiv 25 \cdot 5 \cdot 7 \quad (8)$

$x \equiv -5 \quad (8)$

$x \equiv 3 \quad (8)$

$x \equiv 4 \quad (5)$

$x \equiv 4 \quad (7)$

$x \equiv 3 \quad (8)$

$M = 5 \cdot 7 \cdot 8 = 280$

$M_1 = 7 \cdot 8 = 56$

$M_2 = 5 \cdot 8 = 40$

$M_3 = 5 \cdot 7 = 35$

$M_1 \cdot b_1 \equiv 1 \quad (5)$

$56 \cdot b_1 \equiv 1 \quad (5)$

$b_1 \equiv 1 \quad (5)$

$40 \cdot b_2 \equiv 1 \quad (7)$

$5 b_2 \equiv 1 \quad (7)$

$b_2 \equiv 5^{\varphi(7)-1} \cdot 1 \quad (7)$

$b_2 \equiv 5^5 \quad (7)$

$b_2 \equiv -2^5 \quad (7)$

$b_2 \equiv 3 \quad (7)$

$a_1 = 5$

$a_2 = 7$

$a_3 = 8$

φ!

$\varphi(p) = p - 1$ ha p prím

$\varphi(n) = n \cdot \prod_{p \mid n} (1 - \frac{1}{p})$

$35 \cdot b_3 \equiv 1 \quad (8)$

$3\, b_3 \equiv 1 \quad (8)$

$b_3 \equiv 3^{\varphi(8)-1} \cdot 1 \quad (8)$

$b_3 \equiv 3^3 \quad (8)$

$b_3 \equiv 27 \quad (8)$

$b_3 \equiv 3 \quad (8)$

Hogy a k. m-t. szerint:

$x \equiv \overset{a_1 \cdot M_1 \cdot b_1}{4 \cdot 56 \cdot 1} + 4 \cdot 40 \cdot 3 + 3 \cdot 35 \cdot 3 \quad (\mathrm{mod}\ 280)$

$x \equiv 179 \quad (280)$

Az eljárás a modulusszal páros számért relatív prímekre fell bontható!
Így nem alkalmazható az tétel.

$19 \mid 2^{6n+2} + 3$

$2^{6k} = 64^n \equiv (9 \cdot 7 + 1)^n = \sum_{i=0}^{n} (9 \cdot 7)^{n-i} \cdot \binom{n}{i} = 9\ell + 1$

$2^{6n+2} + 3 = 2^{4 \cdot 2^{6n}} + 3 = 2^{4 \cdot (9\ell+1)} + 3 =$

$= 2^4 \cdot 2^{4 \cdot 9\ell} + 3 = 16 \cdot 2^{4 \cdot 9 \cdot k} + 3 = 16 \cdot \left(2^{4 \cdot 9 \cdot \ell} - 1\right) + 16 + 3 =$

$= \underbrace{16 \cdot \left(4^{4 \cdot 9 \cdot \ell} - 1\right)}_{19\,\ell} + 19$

Be kell látni: $19 \mid 2^{4 \cdot 9\ell} - 1$

$2^{4 \cdot 9\ell} - 1 = \left(2^{2 \cdot 9 \cdot \ell} - 1\right)\left(2^{2 \cdot 9\ell} + 1\right) =$

$= \left(2^{9\ell+1}\right)\underbrace{\left(2^{9\ell} - 1\right)\left(2^{2 \cdot 9\ell} + 1\right)}_{19\,|\ \checkmark} = \left(2^{9\ell} + 1\right) \cdot L =$

ha $\ell \to$ plan:

$= \left(2^9 + 1\right) \cdot (\ldots) \cdot L$

ha $\ell \to$ páros

$a^\ell - b^\ell$

$2^{4 \cdot 9 \cdot \ell} - 1 = \left(2^{2 \cdot 9k} - 1\right)\left(2^{2 \cdot 9\ell} + 1\right) = \underbrace{\left(2^{18} - 1\right)}_{\left(2^9+1\right)\left(2^9-1\right)}(\ldots)$

$\cdot \left(2^{2 \cdot 9 \cdot \ell} + 1\right)$

$19 \mid\ \checkmark$

- Kong. hl.
- Euklidészi alg.
- oszthatóság tulajdonságai

Számelméleti fgv-ek

D. 6.1.1.
D. 6.1.2.
D: 6.1.3

n osztóinak száma

$$d(n)=\sum_{d|n} 1 = \prod_{i=1}^{s}(\alpha_i+1) \qquad n=\prod_{i=1}^{s} p_n^{\alpha_i} \qquad p_i \neq p_j \text{ ha } i\neq j$$

Hányszor találod olyan számot, amely osztja az n-et, összeadások egyet.

$$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s} \Bigg\} \; d=p_1^{\beta_1}\cdots p_s^{\beta_s} \quad 0\le\beta_i\le\alpha_i$$
$$d|n$$

MULTIPLIKATÍV, de nem totálisan multiplikatív

D.: 6.1.4.

D.: 6.1.5. Példák

T: 6.16.

T: 6.17. , 6.18.

Nev. számelméleti fgv.

D.: 6.2.1.

$\sigma(n)$: n pozitív osztóinak összege

$$\sigma(n)=\sum_{d|n} d$$

T.: 6.2.2.

n kanonikus alakja: $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r} \Rightarrow$

$$\sigma(n)=\prod_{i=1}^{r}(1+p_i+p_i^2+\cdots+p_i^{\alpha_i})=\prod_{i=1}^{r}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

D 6.2.3.

$\mu(n)$ Möbius-fgv.

$$\mu(n)=\begin{cases}1, & \text{ha } n=1\\ (-1)^r, & \text{ha } n=p_1\cdots p_r \text{ ahol } p_j\text{-k különb. prímek}\\ 0, & \text{ha } \exists \text{ prím, melyre } p^2|n\end{cases}$$

T.: 6.24.

$$\sum_{d|n}\mu(d)=\begin{cases}1, & \text{ha } n=1\\ 0, & \text{ha } n>0\end{cases}$$

D.: 6.25.

χ(ekv) $w(n)$: n diff. (poz.) prímosztóinak száma

ν(ső) ...

D.: 6.26.

T.: 6.27.

T: 6.28.

D: 6.31. TÖKÉLETES SZÁM

T.: 6.32.

D: 6.51. Összegzési fgv.

D: 6.52. megfordítási fgv.

T.: 6.5.3 Möbius-f. megfordítási formula

T: 6.5.4 $\emptyset$

T.: 6.6.1. számelméleti fgv.-ek konvolúciója

T.: 6.6.2.

$3x \equiv 1 \quad (4)$
$6x \equiv 1 \quad (7)$
$8x \equiv 1 \quad (9)$
$10x \equiv 1 \quad (11)$

$(4;7;9;11) = 1$

$-x \equiv 1 \quad (4)$
$-x \equiv 1 \quad (7)$
$-x \equiv 1 \quad (9)$
$-x \equiv 1 \quad (11)$

$x \equiv -1 \quad (4) \iff 4 \mid x+1$
$x \equiv -1 \quad (7) \iff 7 \mid x+1$
$x \equiv -1 \quad (9) \iff 9 \mid x+1$
$x \equiv -1 \quad (11) \iff 11 \mid x+1$

$4 \cdot 7 \cdot 9 \cdot 11 \mid x+1$

$2772 \mid x+1$

$x \equiv -1 \quad (2772)$

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

$a^{\varphi(m)-1} \cdot a \equiv 1 \pmod{m}$

$3x \equiv 1 \quad (4)$
$2x \equiv 3 \quad (5)$
$5x \equiv 2 \quad (7)$
$7x \equiv 8 \quad (9)$

$(4;5;7;9) = 1$

$3x \equiv 1 \quad (4) \qquad / \cdot 3^{\varphi(4)-1}$

$\varphi(4) = 4 \cdot \left(1 - \frac{1}{2}\right) = 2$

$x = 1 \cdot 3^{2-1} \quad (4)$

$x \equiv -1 \quad (4)$

$2x \equiv 3 \quad (5)$
$-3x \equiv 3 \quad (5) \qquad / \cdot (-3)$
$x \equiv -1 \quad (5)$

$\text{mert } (-3;5) = 1$

$5x \equiv 2 \quad (7)$
$-2x \equiv 2 \quad (7) \qquad / : (-2)$
$x \equiv -1 \quad (7)$

$7x \equiv 8 \quad (9)$
$-2x \equiv 8 \quad (9) \qquad / : (-2)$
$x \equiv -4 \quad (9)$
$x \equiv 5 \quad (9)$

Csak akkor lehet f-tel oszthatóan, ha $(a,m) = 1$.

$f(9) = 9 \cdot \left(1 - \frac{1}{3}\right) = 6$

$x \equiv -1 \quad (4)$
$x \equiv -1 \quad (5)$
$x \equiv -1 \quad (7)$
$x \equiv 5 \quad (9)$

$M = 4 \cdot 5 \cdot 7 \cdot 9 = 1260$
$M_1 = 5 \cdot 7 \cdot 9 = 315$
$M_2 = 4 \cdot 7 \cdot 9 = 252$
$M_3 = 4 \cdot 5 \cdot 9 = 180$
$M_4 = 4 \cdot 5 \cdot 7 = 140$

$M_1 \cdot b_1 \equiv 1 \quad (4)$
$315\, b_1 \equiv 1 \quad (4)$
$-b_1 \equiv 1 \quad (4)$
$b_1 \equiv -1 \quad (4)$

$4 \cdot 7 \cdot 9\, b_2 \equiv 1 \quad (5)$

$(-1) \cdot (2) \cdot (-1)\, b_2 \equiv 1 \quad (5)$
$2\, b_2 \equiv 1 \quad (5)$
$b_2 \equiv 3 \quad (5)$

$4 \cdot 5 \cdot 9 \cdot b_3 \equiv 1 \quad (7)$
$(-3)(-2)\, 2\, b_3 \equiv 1 \quad (7)$
$-2\, b_3 \equiv -6 \quad (7)$
$b_3 \equiv 3 \quad (7)$

$4 \cdot 5 \cdot 7 \cdot b_4 \equiv 1 \quad (9)$
$4 \cdot (-4) \cdot (-2)\, b_4 \equiv 1 \quad (9)$
$32\, b_4 \equiv 1 \quad (9)$
$-4\, b_4 \equiv -8 \quad (9)$
$b_4 \equiv 2 \quad (9)$

$/ \cdot 2^{\varphi(5)-1}$

$$x \equiv (-1) \cdot 5 \cdot 7 \cdot 9 \cdot (-1) + (-1) \cdot 4 \cdot 7 \cdot 9 \cdot (-2) +$$

$$+ (-1) \cdot 4 \cdot 5 \cdot 9 \cdot 3 + 5 \cdot 4 \cdot 5 \cdot 7 \cdot 2 \quad (4 \cdot 5 \cdot 7 \cdot 9)$$

$$x \equiv 1679 \quad (1260)$$

$$x \equiv 419 \quad (1260)$$