Diszkrét matematika II

Számelmélet témakör jegyzete

Készült Burcsi Péter előadásai
és Harrison-Juhász Zsófia gyakorlatai alapján

Sárközi Gergő, 2021-22-1. félév
Nincsen lektorálva!

Tartalomjegyzék

1. Oszthatóság **3**
1.1. Definíció . . . 3
1.2. $\mathbb{Z}$-beli oszthatóság . . . 3
1.3. $\mathbb{N}$-beli oszthatóság . . . 3
1.4. Lineáris kombincáiós tulajdonság . . . 4

2. Legnagyobb közös osztó **5**
2.1. LNKO létezésének bizonyítása . . . 5
2.2. Bővített euklideszi algoritmus . . . 6
2.3. Euklideszi algoritmus a gyakorlatban . . . 7
2.4. Bővített euklideszi algoritmus a gyakorlatban . . . 7

3. Prímszámok **8**
3.1. Prím vs felbonthatatlan . . . 8
3.2. Felbonthatatlan = prím . . . 8
3.3. Számelmélet alaptétele . . . 9
3.4. Tétel: végtelen sok prím van . . . 9
3.5. Prímszámtétel . . . 10
3.6. Prímfelbontás kanonikus alakja . . . 10
3.7. Szám osztóinak száma . . . 10
3.8. LNKO kiszámítása prímtényezőkből . . . 10

4. Legkisebb közös többszörös **11**
4.1. Definíció . . . 11
4.2. Kiszámítása . . . 11
4.3. LNKO, LKKT kapcsolata . . . 11

5. Kongruencia **12**
5.1. Definíció . . . 12
5.2. Tulajdonságok . . . 12
5.3. Modulus tulajdonságai, gyakorlatról trükkök . . . 13
5.3.1. Ekvivalens átalakítás . . . 13
5.3.2. Gyorshatványozás . . . 13
5.4. Kínai maradéktétel . . . 14
5.4.1. Állítás . . . 14
5.4.2. Bizonyítás . . . 14
5.5. Euler-Fermat tétel . . . 15
5.5.1. Bevezetés . . . 15
5.5.2. Euler-féle φ függvény . . . 15
5.5.3. Euler-Fermat tétel . . . 15
5.5.4. Euler-féle φ függvény kiszámítása . . . 16
5.6. Egyváltozós lineáris kongruenciák . . . 17
5.6.1. Megoldási módszer . . . 17
5.6.2. Megoldás diofantikus egyenlet alapján . . . 17
5.7. Lineáris kongruencia rendszerek . . . 18
5.7.1. Kínai maradéktétellel, páronként relatív prímek esetén 18
5.7.2. Kínai maradéktétellel, nem relatív prímek esetén . . . 18
5.7.3. Behelyetessítős módszerrel . . . 18

6. Kétváltozós lineáris diofantikus egyenletek **19**

7. Számrendszerek **20**
7.1. Gyakorlati trükkök . . . 20

8. ZH 1-re összefoglaló jegyzet **21**
8.1. Kanonikus alak . . . 21
8.2. Oszthatóság . . . 21
8.3. Kongruencia . . . 21
8.4. Kis-Fermat tétel, Euler-Fermat tétel . . . 21
8.5. Kongruencia ekvivalens átalakításai . . . 22
8.6. Kétváltozós lineáris diofantikus egyenletek . . . 22
8.7. Kongruenciarendszerek, kínai maradéktétel . . . 22
8.8. Trükkök . . . 22

1. Oszthatóság

1.1. Definíció

- $a, b \in \mathbb{Z} : \exists c \in \mathbb{Z} : a * c = b \implies a|b$
  - TODO nem kétirányú a reláció?
- elnevezés: a osztója b-nek, b többszöröse a-nak, a osztja b-t
- példa: 3|21, 7|105
- 0|0

1.2. $\mathbb{Z}$-beli oszthatóság

- $\forall a : 1|a$
- $\forall a : a|a$ (reflexív)
- $\forall a : a|0$
- $\forall a : 0|a \implies a = 0$
- $\forall a, b, k : a|b \implies a * k|b * k$
- $\forall a, b : a|b \wedge a'|b' \implies aa'|bb'$
  - bizonyítás: $ak = b$ és $a'k' = b'$, tehát $aa' * kk' = bb'$
- $\forall a, b, k : k \neq 0 \wedge ak|bk \implies a|b$
- $\forall a, b, c : (a|b \wedge b|c) \implies a|c$ (tranzitív)

1.3. $\mathbb{N}$-beli oszthatóság

- minden igaz, amit felsoroltam $\mathbb{Z}$ alatt
- ha az alaphalmaz $\mathbb{N}$, akkor $a, b \in \mathbb{N} : (a|b) \Leftrightarrow (\exists c \in \mathbb{N} : a * c = b)$
  - TODO Ez $\mathbb{Z}$-ben is igaz, nem? lásd 1.4 lin komb bizonyítás
- $\forall a, b : (a|b \wedge b|a) \implies a = b$ (antiszimmetria)
  - $\mathbb{Z}$-ben nem igaz: $7|-7$ és $-7|7$
- reflexív, antiszimmetrikus és tranzitív: tehát részbenrendezés $\mathbb{N}$-ben

1.4. Lineáris kombincáiós tulajdonság

- Legyen:
  - $a \in \mathbb{Z}$
  - $b_1, b_2, ..., b_n \in \mathbb{Z}$
  - $\forall i : a | b_i$
- Akkor:
  - $a | \sum_{i=1}^{n} x_i * b_i \ (x_1, x_2, ..., x_n \in \mathbb{Z})$
- Bizonyítás:
  - $a | b_i \Leftrightarrow \exists k_i : a * k_i = b_i$
  - $\sum_{i=1}^{n} x_i * b_i = \sum_{i=1}^{n} x_i * a * k_i = a * \sum_{i=1}^{n} x_i * k_i$
- Következmények:
  - $a | b \wedge a | c \implies a | (k_1 * b + k_2 * c) \ (k_i \in \mathbb{Z})$

2. Legnagyobb közös osztó

- $a, b, d \in \mathbb{Z}$ ('d' 'a' és 'b' legnagyobb közös osztója, ha...)
- $d|a$ és $d|b$ (közös osztó)
- $\forall d' \in \mathbb{Z} : (d'|a \wedge d'|b) \implies d'|d$ (legnagyobb = minden másik osztja)
- Példa: 18, 30-nak 6 és -6 is LNKO

2.1. LNKO létezésének bizonyítása

- Tétel: $a, b \in \mathbb{Z} \implies \exists d : LNKO \wedge \exists x, y \in \mathbb{Z} : ax + by = d$
- Bizonyítás:
  - elég a,b $>$ 0-ra belátni
  - ha $0 < b < a$ akkor {a és b közös osztói} = {a-b és b közös osztói}
    - lineáris kombináció miatt igaz:
    - $(d|a \wedge d|b) \implies d|a - b = 1 * a - 1 * b$
    - $(d|a - b \wedge d|b) \implies d|a = 1 * (a - b) + 1 * b$
  - lépés: ({} jelezze a rendezetlen párt, ne a halmazt)
    - ha $a > b$ akkor $\{a, b\} \to \{a - b, b\}$
    - ha $b \geq a$ akkor $\{a, b\} \to \{b - a, a\}$
    - ez nem változtatja meg a közös osztókat
  - előbb-utóbb 0-hoz és egy pozitív számhoz jutunk
  - tehát létezik LNKO
  - $\exists s, t : d = (a - b) * s + b * t \implies \exists x, y : d = a * x + b * y$
    - megoldás: x=s, y=t-s

2.2. Bővített euklideszi algoritmus

- Bemenet: $a, b \in \mathbb{Z}^+$
- Kimenet: $d, x, y \in \mathbb{Z}$ (d az LNKO és $d = ax + by$)

```
function extended_gcd(a, b)
    (old_r, r) := (a, b)
    (old_s, s) := (1, 0)
    (old_t, t) := (0, 1)
    while r != 0 do
        quotient := old_r div r //egészrészes osztás
        (old_r, r) := (r, old_r - quotient × r)
        (old_s, s) := (s, old_s - quotient × s)
        (old_t, t) := (t, old_t - quotient × t)
    return (old_r, old_t, old_s) //t=x, s=y

//Extra: normál, nem bővített euklideszi algoritmus
function gcd(a, b)
    while b != 0
        t := b
        b := a mod b
        a := t
    return a
```

- d=LNKO: {a és b közös osztói} = {d osztói}
  - mert minden lépésnél d osztja r-t és old-r-t
- lineáris kombinációs rész, indukció:
  - (d osztja a-t és b-t, tehát a és b lineáris kombinációt is)
  - eredeti old-r = a = a*old-s + b*old-t
  - eredeti r = b = a*s + b*t
  - következő r is lineáris kombináció lesz

2.3. Euklideszi algoritmus a gyakorlatban

$a = b * q_1 + r_1$
$b = r_1 * q_2 + r_2$
$r_1 = r_2 * q_3 + r_3$
...
Ha $r_i = 0$, akkor $lnko(a, b) = r_{i-1}$
Ezt táblázatként a bővített algoritmus részeként láthatjuk.

2.4. Bővített euklideszi algoritmus a gyakorlatban

Kezdő értékek:
$r_{-1} = a$, $r_0 = b$
$x_{-1} = 1$, $x_0 = 0$
$y_{-1} = 0$, $y_0 = 1$

Minden $i \geq 1$ esetén:
$q_i = \lfloor r_{i-2}/r_{i-1} \rfloor$
$x_i = x_{i-2} - q_i * x_{i-1}$
$y_i = y_{i-2} - q_i * y_{i-1}$
$r_i = a * x_i + b * y_i$

i	q_i	r_i	x_i	y_i
-1	-	**a**	1	0
0	-	**b**	0	1
...	...	...	...	...
i	$\lfloor r_{i-2}/r_{i-1} \rfloor$	$r_{i-2} \mod r_{i-1}$	$x_{i-2} - q_i * x_{i-1}$	...
...	...	...	...	...
n-1	?	**lnko(a,b)**	**?**	**?**
n	?	**0**	...	...

i	q_i	r_i	x_i	y_i
-1	-	**86**	1	0
0	-	**31**	0	1
1	2	24	1	-2
2	1	7	-1	3
3	3	3	4	-11
4	2	**1**	**-9**	**25**
5	3	**0**	-	-

3. Prímszámok

3.1. Prím vs felbonthatatlan

- $f \in \mathbb{Z}$ felbonthatatlan (irreducibilis), ha $f \neq 0$, $f \neq \pm 1$ és f-nek a ± 1 és $\pm f$-en (triviális osztókon) kívül nincs más osztója
  - $f = a * b \implies (a = \pm 1) \vee (b = \pm 1)$
- $p \in \mathbb{Z}$ primszám (rendelkezik a prímtulajdonsággal), ha $p \neq 0$ és $p \neq \pm 1$ és $\forall a, b \in \mathbb{Z} : p|a * b \implies p|a \vee p|b$
  - nem prím példa: $15|3 * 5$, de $15 \not| 3$ és $15 \not| 5$

3.2. Felbonthatatlan = prím

- Cél: felbonthatatlanság $\Leftrightarrow$ prímtulajdonság
- Bizonyítás: p prím $\implies$ p felbonthatatlan
  - Indirekt, Tfh. (tegyük fel hogy) $p = a * b$ ($a \neq \pm 1$, $a \neq \pm p$)
  - $p|a * b \implies$ (mert prím) $p|a \vee p|b$
  - $p = a * b \implies a|p \wedge b|p$
  - $p|a \wedge a|p \implies p = \pm a$ (a helyett b-re ugyan ezek felírhatók)
  - ellentmondás
- Bizonyítás: f felbonthatatlan $\implies$ f prím
  - f-nek 4 osztója van: $\pm 1, \pm f$
  - kérdés, hogy igaz-e: $f|a * b \implies f|a \vee f|b$
  - ha $f|a * b$, de $f \not| a$:
    - f és a közös osztói: ± 1 (egyben LNKO)
    - LNKO $= 1 = x * f + y * a$ (lásd LNKO szekció)
    - /*b után: $b = b * x * f + b * y * a$
    - f osztja az első tagot: $f|b * x * f$
    - $f|a * b$ (kikötés), tehát f osztja a második tagot: $f|a * y * b$
    - tehát f osztja b-t is, hiszen b felírható olyan számok lineáris kombinációjaként, amiket f oszt

3.3. Számelmélet alaptétele

- Legyen $n \in \mathbb{Z}, n \neq 0, n \neq \pm 1$. Ekkor n lényegében (előjeltől és sorrendtől eltekintve) felirható prímszámok szorzataként.
- Bizonyítás: létezik felírás
  - Elég $n \geq 2$ esetben
  - Indukció: $n = 2$
  - Legyen $n > 2$. Minden n-nél kisebbhez létezik felírás
  - Ha n prím, akkor kész vagyunk
  - Ha n nem prím, akkor $\exists 1 < n_1, n_2 < n : n = n_1 * n_2$
    - De ekkor n felírható n_1 és n_2 szorzataként, szóval van felírás
- Bizonyítás: egyértelműség
  - Tfh. $n = p_1 * p_2 * ... * p_r = q_1 * q_2 * ... * q_s$ (p_i és q_i prímek)
  - p_1 prím és $p_1 | q_1 * q_2 * ... * q_s$ ezért $\exists l$ index, hogy $p_1 | q_l$
    - de q_l prím, azaz osztói: $\{\pm 1, \pm q\}$
    - p_1 nem lehet ± 1, mert prím
    - tehát $p_1 = \pm q_l$
  - Folytatva: $\frac{n}{p_1} = p_2 * ... * p_r = \pm q_1 * ... * q_{l-1} * q_{l+1} * ... * q_s = \pm \frac{n}{q_l}$
  - Azaz kisebb számmal folytatjuk, így előbb-utóbb végzünk és arra jutunk, hogy a két szorzat pontosan ugyanazokat a tényezőket tartalmazza (sorrendtől és előjeltől eltekintve)

3.4. Tétel: végtelen sok prím van

- Tfh. összesen n prím van: $p_1, p_2, ..., p_n$
- $x = p_1 * p_2 * ... * p_n + 1$
- x felbontható prímekre, hiszen minden szám felbontható prímekre
- $x - 1$ osztható az összes prímmel, tehát x nem osztható egyikkel sem (ellentmondás)

3.5. Prímszámtétel

- $\lim_{x\to\infty} \frac{\pi(x)}{x/ln(x)} = 1$, ahol $\pi(x) = 1 \leq p < x$ prímek száma
- Jelentés: prímek száma nagyjából $\frac{x}{ln(x)}$
- Random szám x körül: $1/ln(x)$ eséllyel prím
  - $ln(x)$ arányos x számjegyeinek számával

3.6. Prímfelbontás kanonikus alakja

- Prímfelbontás kanonikus alakja: $n = p_1^{\alpha_1} * p_2^{\alpha_2} * ...$ (ahol p_i különböző)
- n osztói pontosan azok az $m = p_1^{\beta_1} * p_2^{\beta_2} * ...$ számok ahol $\forall i : 0 \leq \beta_i \leq \alpha_i$
- Bizonyítás:
  - m-nek lenne más prímosztója q
  - $q|m \wedge m|n \implies q|n \implies$ q n egy tényezője, ellentmondás

3.7. Szám osztóinak száma

- $n = p_1^{\alpha_1} * p_2^{\alpha_2} * ...$ szám pozitív osztóinak száma: $(\alpha_1 + 1) * (\alpha_2 + 1) * ...$
- mert β_i-re ennyi lehetőség van

3.8. LNKO kiszámítása prímtényezőkből

- $n = p_1^{\alpha_1} * p_2^{\alpha_2} * ...$ és $m = p_1^{\beta_1} * p_2^{\beta_2} * ...$ és $\alpha_i = 0$, $\beta_i = 0$ is meg van engedve
- $LNKO(n, m) = p_1^{min(\alpha_1,\beta_1)} * p_2^{min(\alpha_2,\beta_2)} * ...$

4. Legkisebb közös többszörös

4.1. Definíció

- Legyen $n, m \in \mathbb{Z}$ és $t = LKKT(n, m) \in \mathbb{Z}$
- Ekkor $n|t \wedge m|t$ és $\forall t' : (n|t' \wedge m|t') \implies t|t'$
- Kettő LKKT van, normáls esetben a pozitívra gondolunk

4.2. Kiszámítása

- Ha $n = p_1^{\alpha_1} * p_2^{\alpha_2} * ...$ és $m = p_1^{\beta_1} * p_2^{\beta_2} * ...$
- Ekkor $LKKT(n, m) = p_1^{max(\alpha_1,\beta_1)} * p_2^{max(\alpha_2,\beta_2)} * ...$

4.3. LNKO, LKKT kapcsolata

- $LNKO(a, b) * LKKT(a, b) = a * b$
- Tehát LKKT-t ki lehet számítani a két szám szorzatából és LNKO-ból

5. Kongruencia

5.1. Definíció

- $m, a, b \in \mathbb{Z}$ esetén $a \equiv b \pmod{m} \Leftrightarrow m|a-b$
- Másik jelölés: $a \equiv b$ (m)

5.2. Tulajdonságok

- reflexív: $\forall a : a \equiv a \pmod{m}$
- szimmetrikus: $\forall a, b : a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$
  - $m|a-b \Leftrightarrow m|b-a$ (mindkettő lineáris kombináció)
- tranzitív: $\forall a, b, c : a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}$
  $\implies a \equiv c \pmod{m}$
  - $m|a-b \wedge m|b-c \implies m|a-c$ (mert $a-c = (a-b)+(b-c)$)
- reflexív, szimmetrikus, tranzitív: ekvivalencia reláció
  - mod m szerinti osztályok: m szerinti (modulo m) maradékosztályok

5.3. Modulus tulajdonságai, gyakorlatról trükkök

- $a + b \mod m = (a \mod m + b \mod m) \mod m$
- $a * b \mod m = (a \mod m) * (b \mod m) \mod m$
- $a^x \mod m = (a \mod m)^x \mod m$
- Kis-fermat tétel: $a^p \mod p = a^1 \mod p$ (ahol p prím)
  - Átfogalmazva: $a^{p-1} \mod p = 1$
  - Következmény: $a^x \mod p = a^{(x \mod (p-1))} \mod p$

5.3.1. Ekvivalens átalakítás

- Legyen a kongruencia $a \equiv b \mod m$
- $c \neq 0$-val szorozni a-t, b-t és m-t
- Legyen $c \neq 0$ és $gcd(m, c) = 1$, ekkor a, b beszorozható c-vel (m marad)
- Legyen $c \neq 0$, hogy $c|a$ és $c|b$, ekkor a és b leosztható c-vel, m pedig leosztható $gcd(m, c)$-vel

5.3.2. Gyorshatványozás

($n^x \mod m$): az x szám felírása 2-es számrendszerben és $n^{(2^k)} \mod m$ értékekhez táblazatot készíteni ($k \in \mathbb{N}_0$). Itt a következő érték mindig az előző érték négyzete, mod m. Ekkor az n kettő hatványokra emelt mod m értékeiből összerakni az n^x értéket: $n^x \mod m = (\prod n^{(2^k)} \mod m) \mod m$

Példa Legyen a feladat $2019^{10} \mod 7$
10 a kettes számrendszerben: 1010
Tehát $2019^{10} = 2019^{2^3} * 2019^{2^1}$
Tudjuk, hogy $2019^{10} \mod 7 = (2019^{2^3} \mod 7) * (2019^{2^1} \mod 7)$
A táblázatban számoljuk ki $2019^{(2^k)} \mod 7$ értékeket
Tudjuk, hogy $2019^{(2^k)} \mod 7 = (2019 \mod 7)^{(2^k)} \mod 7$
Tudjuk, hogy $2019^{(2^{k+1})} \mod 7 = (2019^{(2^k)} \mod 7)^2 \mod 7$
Táblázatból kiolvasva: $2019^{10} \mod 7 = (2 * 2) \mod 7$

k	0	1	2	3
$2019^{(2^k)} \mod 7$	3	2	4	2

5.4. Kínai maradéktétel

5.4.1. Állítás

- Legyen $m_1, m_2, ..., m_n$ tetszőleges 1-nél nagyobb egészek, melyek páronként relatív prímek
  - páronként relatív prím: $i \neq j \implies LNKO(m_i, m_j) = 1$
- Ekkor
  - az alábbi szimultán kongruenciarendszer megoldható minden $a_1, a_2, ..., a_n$ egészek esetén
  - az x-ek maradékosztályt alkotnak modulo $M = m_1 * m_2 * ... * m_n$
- $x \equiv a_1 \mod m_1$
  $x \equiv a_2 \mod m_2$
  ...
  $x \equiv a_n \mod m_n$

5.4.2. Bizonyítás

- Legyen $n = 2$ (ha nagyobb, akkor indukcióval megoldható)
- $LNKO(m_1, m_2) = 1 = m_1 * x_1 + m_2 * x_2$
- $A = a_2 * m_1 * x_1 + a_1 * m_2 * x_2$
  - $A \equiv 0 + a_1 * m_2 * x_2 \mod m_1$
  - $1 = m_1 * x_1 + m_2 * x_2 \implies 1 \equiv m_1 * x_1 + m_2 * x_2 \mod$ bármi
  - $1 \equiv m_1 * x_1 + m_2 * x_2 \equiv m_2 * x_2 \mod m_1$
  - $A \equiv a_1 * m_2 * x_2 \equiv a_1 \mod m_1$
- $A \equiv a_1 \mod m_1$ és $A \equiv a_2 \mod m_2$
- Ezért $x \equiv A \mod m_1 * m_2$
- Be kell látni: A és A' is jó $\implies A \equiv A' \mod m_1 * m_2$
  - $A' \equiv A \equiv a_1 \mod m_1 \implies m_1 | A - A'$
  - $A' \equiv A \equiv a_2 \mod m_2 \implies m_2 | A - A'$
  - Ezekből következik: $m_1 * m_2 | A - A'$ (m_1, m_2 relatív prímek)

5.5. Euler-Fermat tétel

5.5.1. Bevezetés

- $ax \equiv ax' \mod m$ és $(a,m)=1$ akkor $x \equiv x' \mod m$
  - Bizonyítás: $ax \equiv ax' \mod m$
  - $\Leftrightarrow m|ax - ax' = a(x-x')$
  - $\implies$ (mert $(a,m)=1$) $\implies m|(x-x')$
  - $\Leftrightarrow x \equiv x' \mod m$
- Általánosabban: $ax \equiv ax' \mod m \implies x \equiv x' \mod \frac{m}{(a,m)}$

5.5.2. Euler-féle φ függvény

- $\varphi(m) = |\{x = 1, ..., m \mid (x,m) = 1\}|$
  - azaz 1 és m közötti, m-mel relatív prím számok száma
- Példa: $\varphi(10) = 4$, mert: 1,3,7,9

5.5.3. Euler-Fermat tétel

- $(a,m) = 1 \implies a^{\varphi(m)} \equiv 1 \mod m$
  - Máshogy: $a^x \equiv a^{x \mod \varphi(m)} \mod m$
- Bizonyítás:
  - Legyen $a_1, a_2, ..., a_{\varphi(m)}$ mindegyike egy különböző szám $\{0, 1, ..., \varphi(m)-1\}$-ből (melyek relatív prímek m-hez)
  - $a*a_1, a*a_2, ..., a*a_{\varphi(m)}$ páronként különböznek mod m
    - $a*a_i \equiv a*a_j \implies a_i \equiv a_j \implies$ ellentmondás
  - tehát a $a_1, ..., a_{\varphi(m)}$ és a $a*a_1, ..., a*a_{\varphi(m)}$ maradékosztályok ugyan azok, legfeljebb más sorrendben
    - redukált maradékrendszerek, ezeket viszont nem vettük
  - $\implies a_1 * ... * a_{\varphi(m)} \equiv (a*a_1) * ... * (a*a_{\varphi(m)}) \mod m$
  - $\implies a_1 * ... * a_{\varphi(m)} \equiv a^{\varphi(m)} * (a_1 * ... * a_{\varphi(m)}) \mod m$
  - $\implies 1 \equiv a^{\varphi(m)} \mod m$
- Példa: $7^4 \equiv 1 \mod 10$

5.5.4. Euler-féle φ függvény kiszámítása

- Állítás:
  - Legyen $m = p^\alpha$ valami p prímre, $\alpha \geq 1$
  - Akkor $\varphi(m) = p^\alpha - p^{\alpha-1} = (p-1) * p^{\alpha-1} = \frac{p-1}{p} * m$
  - Példa: $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$
- Bizonyítás:
  - $LNKO(p^\alpha, a) = 1 \Leftrightarrow p \not| a$
  - $\varphi(p^\alpha) = |\{a = 1, ..., p^\alpha \mid p \not| a\}| = p^\alpha - p^{\alpha-1}$
    - Mert p-vel $p^{\alpha-1}$ pozitív szám osztható (ami $\leq p^\alpha$)
    - Más megközelítés: minden p-edik szám kiesik, azaz $p^{\alpha-1}$ darab
- Állítás: φ multiplikatív
  - Legyen a, b relatív prímek
  - $\varphi(a * b) = \varphi(a) * \varphi(b)$
- Bizonyítás:
  - $x \equiv a_1 \mod a$ és $x' \equiv a_1 \mod a$ esetén: $lnko(x, a) = lnko(x', a)$
  - Tehát x relatív prím $a * b \Leftrightarrow x$ relatív prím a és b
  - Ez kell: $x \equiv a_1 \mod a$ és $x \equiv b_1 \mod b$
    - ahol $lnko(a, a_1) = 1$ és $lnko(b, b_1) = 1$
  - a_1-ből $\varphi(a)$ db van, stb.
  - Kínai maradéktétel miatt biztos van megoldás
- Következmény:
  - Ha $n = p_1^{\alpha_1} * p_2^{\alpha_2} * ... * p_r^{\alpha_r}$ (kanonikus alak)
  - Akkor $\varphi(n) = \Pi_{k=1..r}(p^{\alpha_k} - p^{\alpha_k - 1}) = n * \Pi_{k=1..r}(1 - \frac{1}{p_k})$
  - Példa: $\varphi(100 = 2^2 * 5^2) = (2^2 - 2^1)(5^2 - 5^1) = 2 * 20 = 40$

5.6. Egyváltozós lineáris kongruenciák

- $a * x \equiv b \mod m$ ahol a, b, m adott
- ha x megoldás, akkor minden $x' \equiv x \mod m$ is

5.6.1. Megoldási módszer

- $ax \equiv b \mod m$
- Átírva: $\exists y \in \mathbb{Z} : ax - b = my$, azaz $ax + my = b$
- LNKO(a,m) kiszámítása: $as + mt = d = (a, m)$
- $(a, m) \nmid b \implies$ nincs megoldás
- $(a, m) \mid b \implies x \equiv s * \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$
  - $(\frac{a}{(a,m)}, \frac{m}{(a,m)}) = 1 = \frac{a}{d} * s + \frac{m}{d} * t$
  - $\implies \frac{a}{(a,m)} * s = 1 - \frac{m}{(a,m)} * t$
  - $\implies \frac{a}{(a,m)} * s = 1 - \frac{m}{(a,m)} * t \equiv 1 \mod \frac{m}{(a,m)}$
  - $\implies \frac{a}{(a,m)} * (s * \frac{b}{(a,m)}) \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$
- x' megoldás $\Leftrightarrow x \equiv x' \mod \frac{m}{(a,m)}$

5.6.2. Megoldás diofantikus egyenlet alapján

- $ax \equiv b \mod m \Leftrightarrow \exists y \in \mathbb{Z} : ax + my = b$
- megoldjuk a diofantikus egyenletet
- $x_t = x_0 + \frac{m}{(a,m)}t \quad (t = 0, 1, ..., (a, m) - 1)$
- megoldások: $[x_0] \cup [x_1] \cup ... \cup [x_{(a,m)-1}]$
  - $\{x_0 + mk \mid k \in \mathbb{Z}\} \cup \{x_1 + mk \mid k \in \mathbb{Z}\} \cup ...$
  - $[x] = \{x' \in \mathbb{Z} \mid x' \equiv x \mod m\}$
- egyszerűsítés: ha megoldható, akkor ekvivalens: $\frac{ax}{(a,m)} \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$

5.7. Lineáris kongruencia rendszerek

5.7.1. Kínai maradéktétellel, páronként relatív prímek esetén

- Legyen i kongruenciánk: $x \equiv c_i \mod m_i$
- m_i páronként relatív prímek
- $i-1$ lépésben oldjuk meg: mindig 2 kongruenciából csinálunk 1 újat
  - Legyen ez a kettő kongruencia $i = 1$ és $i = 2$
  - $x \equiv c_2 * m_1 * x_1 + c_1 * m_2 * x_2 \mod m_1 * m_2$
  - Ahol x_1 és x_2 innen jön: $m_1 * x_1 + m_2 * x_2 = 1$ (mindig megoldható)
  - Végül egyetlen kongruencia marad: $x \equiv ? \mod \prod m_i$

5.7.2. Kínai maradéktétellel, nem relatív prímek esetén

- Legyen i kongruenciánk: $x \equiv c_i \mod m_i$
- Ha bármelyik m_j és m_k nem relatív prímek, akkor bontsuk őket szét 2 vagy több kongruenciára, hogy azok legyenek, vagy egymás hatványai.
  - Példa: $x \equiv 4 \mod 15$ és $x \equiv 4 \mod 10$
  - Elsőből: $x \equiv 4 \mod 5$ és $x \equiv 4 \equiv 1 \mod 3$
- Ezek után ha bármelyik $m_j | m_k$ (pl. $2|2$ vagy $2|4$)
  - vagy ellentmondanak egymásnak és nincs megoldás
  - vagy nem mondanak ellen egymásnak, m_j eldobható
- Ezek után relatív prímek m_i-k és megoldhatók a fenti módszerrel

5.7.3. Behelyetessítős módszerrel

- Legyen i kongruenciánk: $a_i * x \equiv c_i \mod m_i$
- $i-1$ lépésben oldjuk meg: mindig 2 kongruenciából csinálunk 1 újat
  - Legyen ez a kettő kongruencia $i = 1$ és $i = 2$
  - Elsőből kifejezzük x-et: $x \equiv y \mod m$ (ahol y és m ismert)
  - Felírjuk egyenletként: $x = y + k * m \ \ (k \in \mathbb{Z})$
  - Behelyettesítjük másodikba: $a_2 * (y + k * m) \equiv c_2 \mod m_2 \ (k \in \mathbb{Z})$
  - Megoldjuk k-ra: $k \equiv ? \mod ?$
- Végül egyetlen kongruencia marad: $x \equiv ? \mod ?$

6. Kétváltozós lineáris diofantikus egyenletek

- $ax + by = c$ ahol $a, b, c, x, y \in \mathbb{Z}$ és $x, y =?$
- $(a, b)|c \Leftrightarrow$ megoldható
- Bővített euklideszi algoritmus: $ap + bq = (a, b)$
  - megszorozva $\frac{c}{(a,b)}$-vel:
  - $x_0 = p * \frac{c}{(a,b)}$
  - $y_0 = q * \frac{c}{(a,b)}$
  - $ax_0 + by_0 = c$
- $ax_t + by_t = c$
  - $x_t = x_0 + \frac{b}{(a,b)}t$
  - $y_t = y_0 - \frac{a}{(a,b)}t$
- Ha csak pozitív megoldások érdekelnek:
  $x_t > 0 \wedge y_t > 0$ egyenletrendszert meg kell oldani

7. Számrendszerek

7.1. Gyakorlati trükkök

- Számrendszer váltás: a számot folyamatosan leosztjuk az új bázissal. A maradékot feljegyezzük. Ha nullához értünk, akkor végeztünk: a maradékot fordított sorrendben (utoljára feljegyzett van a legtöbbet érő helyiértéken) kiolvassuk.

8. ZH 1-re összefoglaló jegyzet

8.1. Kanonikus alak

- Legyen $n = p_1^{a_1} * p_2^{a_2} * ...$ és $m = p_1^{b_1} * p_2^{b_2} * ...$
- n osztóinak száma: $(a_1 + 1) * (a_2 + 1) * ...$
- $\varphi(p^a) = p^a - p^{a-1}$ és $\varphi(x * y) = \varphi(x) * \varphi(y)$
- $LNKO(n, m) = gcd(n, m) = (n, m) = p_1^{min(a_1,b_1)} * p_2^{min(a_2,b_2)} * ...$
- $LKKT(n, m) = lcm(n, m) = [n, m] = p_1^{max(a_1,b_1)} * p_2^{max(a_2,b_2)} * ...$
- LNKO, LKKT összefüggés: $n * m = (n, m) * [n, m]$

8.2. Oszthatóság

- $a, b \in \mathbb{Z} : \exists c \in \mathbb{Z} : a * c = b \implies a|b$
- $\forall a : 1|a \ \wedge \ a|0$ viszont $0|a \implies a = 0$
- $a|b \wedge a|c \implies a|(k_1 * b + k_2 * c)$ (lineáris kombinációs tulajdonság)
- $\mathbb{N}$-ben részbenrendezés: reflexív, tranzitív és antiszimmetrikus
  - $\mathbb{Z}$-ben nem antiszimmetrikus: $7|-7$ és $-7|7$
- Bővített euklideszi algoritmus: $gcd(a, b) = a*x+b*y$ (q,r,x,y táblázat)

8.3. Kongruencia

- $m, a, b \in \mathbb{Z} : a \equiv b \mod m \ \Leftrightarrow \ m|a - b$
- Ekvivalencia reláció: reflexív, szimmetrikus, tranzitív
- $a * +b \equiv a \mod m * +b \mod m$ és $a^x \equiv (a \mod m)^x \ (mod\ m)$

8.4. Kis-Fermat tétel, Euler-Fermat tétel

- Kis-Fermat tétel: p prím $\implies a^{p-1} \equiv 1 \mod p$
- Euler-Fermat tétel: $(a, m) = 1 \implies a^{\varphi(m)} \equiv 1 \mod m$

8.5. Kongruencia ekvivalens átalakításai

- $a \equiv b \mod m$
- $c \neq 0$: $ac \equiv bc \mod mc$
- $gcd(m, c) = 1$ és $c \neq 0$: $ac \equiv bc \mod m$
- $c \neq 0$ és $c|a$ és $c|b$: $\frac{a}{c} \equiv \frac{b}{c} \mod \frac{m}{(m,c)}$

8.6. Kétváltozós lineáris diofantikus egyenletek

- $ax + by = c$ ahol x, y ismeretlen
- $(a, b)|c \Leftrightarrow$ megoldható
  - Bővített euklideszi algoritmus: $ap + bq = (a, b)$
  - $a * (p * \frac{c}{(a,b)}) + b * (q * \frac{c}{(a,b)}) = c = a * x_0 + b * y_0$
  - $x_t = x_0 + \frac{b}{(a,b)}t \quad$ és $\quad y_t = y_0 - \frac{a}{(a,b)}t$
- Kongruenciából: $ax \equiv n \mod m \implies \exists y : ax + my = n$
  - Megoldás: $[x_0] \cup [x_1] \cup ...$ ahol $0 \leq t < (a, m)$
  - Egyszerűsítés: $\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$ (ekkor csak $t = 0$)

8.7. Kongruenciarendszerek, kínai maradéktétel

- Legyen i db kongruenciánk: $x \equiv c_i \mod m_i$
- Ha m_i páronként relatív prímek: megoldható, kettesével
  - $x \equiv c_2 * m_1 * x_1 + c_1 * m_2 * x_2 \mod m_1 * m_2$
  - Ahol x_1 és x_2 innen jön: $m_1 * x_1 + m_2 * x_2 = 1$ (mindig megoldható)
- Egyébként bontsuk kanonikus formára az m_i-ket: vagy ellentmondás lesz vagy elhagyható m_1 ha $m_1|m_2$ (pl. $2|4$).

8.8. Trükkök

- Gyorshatványozás: $a^{12} = a^8 * a^4$ és $a^8 \equiv (a^4 \mod m)^2 \mod m$
  Azaz mindig csak az előző eredményt kell négyzetre emelni.
- $(a, m) = 1 \implies a^{b^c} \equiv a^n \mod m$ és $n \equiv b^c \mod \varphi(m)$