Diszkrét Matematika 2.
Programtervező informatikus A. szakirány
Definíciók és tételek (Bebizonyítással kértek is)
2022-2023. tanév 1. félév

Petrányi Bálint

2022. december 2.

Tartalomjegyzék

*A *. hivatalosan nincsenek benne a kérdések között*

Tételek

Számelméleti alapok

1. Oszthatóság az egész számok körében.

Az a egész osztja a b egészet: $a \mid b$, ha létezik olyan c egész, mellyel $a \cdot c = b$, azaz $b \setminus a$ szintén egész.

2. Egységek

Ha egy szám bármely másiknak osztója, akkor egységnek nevezzük.

3. Asszociált számok

Két szám asszociált, ha egymás egységszeresei.

*. Triviális osztó

Egy számnak az asszociáltjai és az egységek a triviális osztói.

4. Felbonthatatlan (irreducibilis) számok

Ha egy nem-nulla, nem-egység számnak a triviális osztóin kívül nincs más osztója, akkor felbonthatatlanak (irreducibilis) nevezzük

5. prímszámok

Egy nem-nulla, nem-egység p számot prímszámnak nevezünk, ha $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$

*. Prímek és Felbonthatatlan kapcsolat

Minden Prímszám felbonthatatlan

6,1. Maradékos osztás tétele (nemnegatív) egészek körében. (Maradék létezésére tétel)

Tetszőleges $a, b \neq 0$ egész számokhoz egyértelműen léteznek q, r egészek hogy

$$a = bq + r \quad \text{és} \quad 0 \leq r < |b|$$

6,2. Maradékos osztás tétele (nemnegatív) egészek körében. (Tényleges tétel)

Legyenek a, b egész számok ($b \neq 0$). Legyen $a = b \cdot q + r (0 \leq r < |b|)$
Ekkor

- $a \bmod b = r$;
- $q = \lfloor a \setminus b \rfloor$, ha $b > 0$, és $q = \lceil a \setminus b \rceil$, ha $b < 0$

7. Legnagyobb közös osztó

Az a és b legnagyobb közös osztója a d szám: $d = (a, b) = \text{lnko}(a, b)$, ha $c \mid a$ és $c \mid b \Rightarrow c \mid d$

8. Legkisebb közös többszörös

Az a és b legkisebb közös többszörös a m szám: $m = [a,b] = \text{lkkt}(a,b)$ ha $a \mid c$ és $b \mid c \Rightarrow m \mid c$

9. Bővített euklideszi algoritmus

Minden a,b egész számok esetén léteznek x,y egészek hogy $(a,b) = x \cdot a + y \cdot b$

10. A számelmélet alaptétele

Minden nem-nulla, nem egység egész szám sorrendtől és asszociáltaktól eltekintve egyértelműen felírható prímszámok szorzataként.

11. Kanonikus prímtényezős alak.

Egy n nem-nulla egész szám kanonikus alakja:

$$n = \pm\, p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i},\ \text{ahol } p_1, p_2, ..., p_\ell \text{ pozitív prímek, } \alpha_1, \alpha_2, ..., \alpha_\ell \text{ pozitív egészek.}$$

12. Osztók számának ($\tau(n)$ számelméletfüggvény)

Egy $n > 1$ egész esetén legyen $\tau(n)$ az n pozitív osztóinak száma és $n = p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_\ell^{\alpha_\ell}$ kanonikus alakkal. Ekkor

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot ... \cdot (\alpha_\ell + 1)$$

13. Euler-féle φ függvénynek a kiszámítása a kanonikus alakból.

Legyen m prímtényezős felbontása $m = p_1^{e_1} p_2^{e_2} ... p_\ell^{e_\ell}$ Ekkor:

$$\varphi(m) = \prod_{i=1}^{\ell} \left(p_i^{e_1} - p_i^{e_i - 1}\right) = m \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right)$$

14. Prímek száma (Euklidész-tétel)

Végtelen sok prím van.

15. Prímek száma (Dirichlet-tétel)

Ha a, d egész számok, $d > 0, (a,d) = 1$, akkor végtelen sok $ak + d$ alakú prím van.

16. Eratoszthenész szitája

Keressük meg egy adott n-ig az összes prímet. Soroljuk fel 2-től n-ig az egész számokat. Ekkor 2 prím. A 2 (valódi) többszörösei nem prímek, ezeket húzzuk ki. A következő szám 3 szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket húzzuk ki..
Ismételjük az eljárást $\sqrt{n}$-ig. A ki nem húzott számok mind prímek.

17. Kongruenciák: $a \equiv b \pmod m$ definíciója.

Legyenek a, b, m egészek, akkor $a \equiv b \mod m$ (a és b kongruensek), ha $m \mid a - b$, és $a \not\equiv b \mod m$ (a és b inkongruensek), ha $m \nmid a - b$

18. Kongruenciák: $a \equiv b \pmod m$ tulajdonságai.

Minden a, b, c, d és m egész számára igaz

1. $a \equiv a \mod m$ reflexív
2. $a \equiv b \mod m, m' \mid m \Rightarrow a \equiv b \mod m'$
3. $a \equiv b \mod m \Rightarrow b \equiv a \mod m$ szimmetrikus
4. $a \equiv b \mod m, b \equiv c \mod m \Rightarrow a \equiv c \mod m$ tranzitív
5. $a \equiv b \mod m, c \equiv d \mod m \Rightarrow a + c \equiv b + d \mod m$
6. $a \equiv b \mod m, c \equiv d \mod m \Rightarrow ac \equiv bd \mod m$

19. Lineáris kongruenciák megoldása

Legyenek a,b,m egész számok, $m > 1$. Ekkor az $ax \equiv b \mod m$ megoldható $\Leftrightarrow (a, m) \mid b$ Ez esetben pontosan (a, m) darab inkongruens megoldás van $\mod m$

20. Lineáris diofantikus egyenletek

lineáris diofantikus egyenletek: $ax + by = c$, ahol a,b,c egészek.
Ez ekvivalens az $ax \equiv c \mod b$, $by \equiv c \mod a$ kongruenciákkal.
Az $ax + by = c$ pontosan akkor oldható meg, ha $(a, b) \mid c$, és ekkor a megoldások megkaphatóak a bővített euklideszi algoritmussal

21. Szimultán kongruenciák

Szeretnénk olyan x egészet, mely egyszerre elégíti ki a következő kongruenciákat:

$$\left.\begin{aligned} 2x &\equiv 1 \mod 3 \\ 4x &\equiv 3 \mod 5 \end{aligned}\right\}$$

A konkurenciákat külön megoldva

$$\left.\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 5 \end{aligned}\right\}$$

Látszik, hogy $x = 2$ megoldás lesz.

22. Kínai maradék-tétel

Legyenek $1 <, m_1, m_2, ..., m_n$ relatív prím számok, $c_1, c_2, ..., c_n$ egészek. Ekkor

$$\left.\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \\ &\vdots \\ x &\equiv c_n \mod m_n \end{aligned}\right\}$$

23. Maradékosztályok

Algebrai alapok, polinomokkal kapcsolatos alapfogalmak

Polinomok maradékos osztásának tétele és következményei

Polinomok algebrai deriváltja, véges testek, racionális gyökteszt, Lagrange-interpoláció

Polinomok felbonthatósága

Entrópia, forráskódolás

Hibakorlátozó és lineáris kódolás

Bebizonyítással Kért Tételek

Számelméleti alapok

Algebrai alapok, polinomokkal kapcsolatos alapfogalmak

Polinomok maradékos osztásának tétele és következményei

Polinomok algebrai deriváltja, véges testek, racionális gyökteszt, Lagrange-interpoláció

Polinomok felbonthatósága

Entrópia, forráskódolás

Hibakorlátozó és lineáris kódolás