A számítástudomány alapjai 2014. I. félév

11. gyakorlat. Összeállította: Fleiner Tamás (`fleiner@cs.bme.hu`)

Tudnivalók

Def: $a, b, m \in \mathbb{Z}$ esetén $a \equiv b (\mathrm{mod}\ m)$ (*a kongruens b modulo m*, röviden $a \equiv b(m)$), ha $m \mid a - b$.

Megfigyelés: A $\mathbb{Z}$ halmaz előáll m db halmaz diszjunkt uniójaként azzal a tulajdonsággal, hogy két egész pontosan akkor kongruens modulo m, ha ugyanabba a részhalmazba esnek. (Az i-dik ilyen részhalmazba a $\{i+km : k \in \mathbb{Z}\}$ számok tartoznak.) E részhalmazok az *m szerinti maradékosztályok.*

Állítás: Ha $a \equiv b(m)$ (a és b egyazon mod m maradékosztályból valók) akkor $(a, m) = (b, m)$.

Köv.: Ha $(a, m) = 1$, akkor az a maradékosztályának bármely eleme relatív prím a modulushoz.

Kongruenciák tulajdonságai: $\forall a, b, c, d, m \in \mathbb{Z}$-re (1) $a \equiv a(m)$, (2) $a \equiv b(m) \Rightarrow b \equiv a(m)$
(3) $a \equiv b(m), b \equiv c(m) \Rightarrow a \equiv c(m)$ (4) $a \equiv b(m)$, $c \equiv d(m) \Rightarrow a + c \equiv b + d(m)$, $ac \equiv bd(m)$
(5) $a \equiv b(m) \iff ac \equiv bc(mc)$ (6) $ad \equiv bd(m) \Rightarrow a \equiv b \left(\frac{m}{(m,d)}\right)$

Def: Az $\{a_1, a_2, \ldots, a_m\} \subset \mathbb{Z}$ halmaz *teljes maradékrendszer modulo m* (*tmr mod m*), ha minden mod m maradékosztályból pontosan egy elemet tartalmaz. (Pl. $\{1, 2, \ldots, m\}$ tmr mod m.)

Def: Az $\{a_1, a_2, \ldots, a_n\} \subset \mathbb{Z}$ halmaz *redukált maradékrendszer modulo m* (*rmr mod m*), ha minden m-hez rel. prím mod m maradékosztályból pontosan egy elemet tartalmaz. (Pl. az m-nél kisebb, m-hez rel. prím természetes számok.) A mod m rmr mérete $\varphi(m)$. (*Euler-féle φ függvény.*)

Tétel: Ha $\{a_1, a_2, \ldots, a_m\}$ rmr mod m, és $(b, m) = 1$, akkor $\{ba_1, ba_2, \ldots, ba_m\}$ is rmr mod m.

Euler-Fermat tétel: $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1(m)$. **Kis Fermat:** p prím, $a \in \mathbb{Z} \Rightarrow a^p \equiv a(p)$.

Tétel: Ha p prím, akkor (1) $\varphi(p) = p - 1$, (2) $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.
(3) $(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$. (4) Ha $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, akkor $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

Tétel (lineáris kongruenciák megoldása): Az $ax \equiv b(m)$ kongruencia megoldható $\iff$ $(a, m) \mid b$. Ekkor (a, m) db maradékosztály modulo m a megoldás. Ha $(a, m) = 1$, akkor a fenti kongruencia megoldása $x \equiv a^{\varphi(m)-1} b(m)$.

Konkrét lineáris kongruencia megoldása: A megoldandó $ax \equiv b(m)$ lineáris kongruenciát kiegészítjük az $mx \equiv 0(m)$ kongruenciával, és az így kapott rendszert oldjuk meg, úgy, hogy mindig a nagyobb együtthatósból vonjuk ki a kisebb együtthatós kongruenci többszörösét, épp ahogy az Euklideszi algoritmusnál. Amint az egyik kongruencia $0x \equiv z(m)$ lesz, akkor $z \not\equiv 0(m)$ esetén nincs megoldás, $z = 0$ esetén pedig a másik kongruenciát le tudjuk osztani, és az adja a megoldást.

Gyakorlatok

1. Oldogassunk lineáris kongruenciákat. Pl: (a) $202x \equiv 157(203)$, (b) $309x \equiv 451(617)$
   (c)$5x \equiv 13(137)$, (d) $113x \equiv 77(120)$, (e) $11x \equiv 12(18)$,
   (f) $14x - 4 \equiv 80(21)$ (g) $49^{49}x \equiv 3(15)$ (h) $3^{80}x \equiv 23(100)$
2. Számítsuk ki a $\varphi(533)$, $\varphi(2007)$ és $\varphi(540)$ értékeket.
3. Bizonyítsuk be, hogy $11 \mid n^{11} + 10n$ és $42 \mid n^7 - n$ teljesül tetszőleges $n \in N$ esetén.
4. Bizonyítsuk be, hogy tetszőleges $h_1, h_2, \ldots, h_k$ pozitív egészekre és p prímszámra fennáll, hogy $(h_1 + h_2 + \ldots + h_k)^p \equiv h_1^p + h_2^p + \ldots + h_k^p (\mathrm{mod}\ p)$. (ZH '02)
5. Milyen maradékot ad a 31-gyel osztva, ha $a^{100} \equiv 5(\mathrm{mod}\ 31)$ és $a^{101} \equiv 19(\mathrm{mod}\ 31)$? (V '00)
6. Mi a 403^{402} utolsó három, a $29^{39^{49}}$ utolsó két és a $7^{6^{5^{4^{3^2}}}}$ szám utolsó jegye tízes számrendszerben?
7. Milyen maradékot ad 59^{99} 101-gyel osztva? (ZH '03)
8. Hogyan számíthatjuk ki gyorsan a 7^{73} 19-es maradékát? Ugyanez a kérdés, de a φ függvény értékét nem használhatjuk. Mi a helyzet az n^k kiszámításával modulo m?
9. Mi az utolsó három jegye a $999^{777^{8888}}$ számnak? Mi az utolsó két jegye az $1997^{2001^{2005}}$ számnak?
10. Bb: ha $p > 5$ prím, akkor az $1, 11, 111, \ldots$ számok között végtelen sok többszöröse van!(ZH '01)
11. Bb: $17 | 2002^{2002} + 1$ (ZH '02)
12. Legyenek m és n pozitív egészek, továbbá $m \mid n$. Bizonyítsuk be, hogy $\varphi(m) \mid \varphi(n)$.(ZH '00)
13. Mely n számokra lesz $\varphi(n)$ prímszám? Hát aztán mikor lesz $\varphi(n)$ páratlan? (ZH '99)
14. Mely n természetes számokra igaz, hogy $\varphi(5n) + \varphi(3n) = 7\varphi(n)$? (ZH '03)
15. Bb: ha $d \mid n$, akkor $d - \varphi(d) \leq n - \varphi(n)$. (V '00)
16. Bb: $\sum_{0<i<n,\ (i,n)=1} i = \frac{n \cdot \varphi(n)}{2}$, ha $n > 1$, egész. (V '99)
17. Ha $r_1, r_2, \ldots, r_{\varphi(n)}$ redukált maradékrendszer modulo n, akkor $\sum_{i=1}^{\varphi(n)} r_i \equiv 0(\mathrm{mod}\ n)$. (V '00)