Számítástudomány alapjai
12. gyakorlat megoldások

1. (a) $3x \equiv 5 (\mathrm{mod}\, 7)$. Itt $(3,7) = 1$, így egy megoldás van. Ezt most kétféleképpen is meghatározzuk. Egyrészt $x \equiv 5 \cdot 3^{\varphi(7)-1} \equiv 5 \cdot 3^5 \pmod 7$, ahonnan $3^3 \equiv 27 \equiv -1 \pmod 7$ és $3^2 \equiv 2 \pmod 7$ miatt $x \equiv 5 \cdot (-1) \cdot 2 \equiv -10 \equiv 4 \pmod 7$. Másrészt az x együtthatója egy kicsi egész szám, így gyorsan végzünk, ha megkeressük az $5, 5+7, 5+2\cdot 7$ számok közül a 3-mal oszthatót. Ez itt az $5+7=12$, így $3x \equiv 12 \pmod 7$ és $x \equiv 4 \pmod 7$.

   (b) $14x \equiv 8 (\mathrm{mod}\, 21)$. Itt $(14,21) = 7 \nmid 8$, így nincs megoldás.

   (c) $11x \equiv 12 \pmod{18}$. Itt $(11,18) = 1$, így egy megoldás van. $x \equiv 12 \cdot 11^{\varphi(18)-1} \pmod{18}$. $\varphi(18) = 18(1-\frac{1}{2})(1-\frac{1}{3}) = 6$; $11^2 \equiv 121 \equiv 13 \pmod{18}$ és $11^3 \equiv 11^2 \cdot 11 \equiv 11 \cdot 13 \equiv 143 \equiv -1 \pmod{18}$. Végül $x \equiv 12 \cdot 13 \cdot (-1) \equiv -156 \equiv 6 \pmod{18}$.

   (d) $9x \equiv 24 (\mathrm{mod}\, 96)$. Itt $(9,96) = 3 | 24$, így 3 megoldás van. Ekkor az egészet egyszerűsítjük 3-mal, és először megoldjuk a $3\widetilde{x} \equiv 8 \pmod{32}$ kongruenciát (aminek egy megoldása van). $\widetilde{x}$ együtthatója kicsi, így érdemes a $8, 8+32, 8+2\cdot 32$ számok között megkeresni a 3-mal oszthatót, ez a $8+2\cdot 32 = 72$, ahonnan $3\widetilde{x} \equiv 72 \pmod{32}$ és $\widetilde{x} \equiv 24 \pmod{32}$. Az eredeti kongruencia megoldásai: $x \equiv 24, 24+32, 24+2\cdot 32 \pmod{96}$.

   (e) $ax \equiv 5 (\mathrm{mod}\, 35)$, ha $a = 5$, 6 vagy 7.

   Ha $a = 5$, akkor $5x \equiv 5 \pmod{35}$. Itt $(5,35) = 5 | 5$, így 5 megoldás van. Egyszerűsítünk 5-tel: $\widetilde{x} \equiv 1 \pmod 7$, ez a kongruencia eleve „meg van oldva", így nem kell tovább dolgoznunk vele. Az eredeti kongruencia megoldásai pedig $x \equiv 1, 1+7, 1+14, 1+21, 1+28 \pmod{35}$.

   Ha $a = 6$, akkor $6x \equiv 5 \pmod{35}$. Itt $(6,35) = 1$, így egy megoldás van, méghozzá $x \equiv 5 \cdot 6^{\varphi(35)-1} \equiv 5 \cdot 6^{23} \pmod{35}$. De $6^2 \equiv 36 \equiv 1 \pmod{35}$, így $x \equiv 5 \cdot (6^2)^{11} \cdot 6 \equiv 5 \cdot 6 \equiv 30 \pmod{35}$.

   Ha $a = 7$, akkor $7x \equiv 5 \pmod{35}$. Itt $(7,35) = 7 \nmid 5$, így ekkor nincs megoldás.

   (f) $ax \equiv 3 (\mathrm{mod}\, 21)$, ha $a = 6$, 7 vagy 8.

   Ha $a = 6$, akkor $6x \equiv 3 \pmod{21}$. Itt $(6,21) = 3 | 3$, így 3 megoldás van. $2\widetilde{x} \equiv 1 \pmod 7$. Itt $\widetilde{x}$ együtthatója kicsi, így megkeressük az $1, 1+7$ számok közül a párosat, ami $1+7=8$, innen $\widetilde{x} \equiv 4 \pmod 7$ és $x \equiv 4, 4+7, 4+2\cdot 7$.

   Ha $a = 7$, akkor $7x \equiv 3 \pmod{21}$. Itt $(7,21) = 7 \nmid 3$, így ekkor nincs megoldás.

   Ha $a = 8$, akkor $8x \equiv 3 \pmod{21}$. Itt $(8,21) = 1$, így egy megoldás van, méghozzá $x \equiv 3 \cdot 8^{\varphi(21)-1} \equiv 3 \cdot 8^{12} \pmod{21}$. Itt $8^2 \equiv 64 \equiv 1 \pmod{21}$, így $x \equiv 3 \cdot (8^2)^6 \equiv 1 \pmod{21}$.

   (g) $ax \equiv b (\mathrm{mod}\, 12)$, ha $a = 4$ vagy 5, $b = 2$ vagy 3.

   Ha $a = 4, b = 2$, akkor $4x \equiv 2 (\mathrm{mod}\, 12)$. Itt $(4,12) = 4 \nmid 2$, így ekkor nincs megoldás.

   Ha $a = 4, b = 3$, akkor $4x \equiv 3 (\mathrm{mod}\, 12)$. Itt $(4,12) = 4 \nmid 3$, így ekkor sincs megoldás.

   Ha $a = 5, b = 2$, akkor $5x \equiv 2 \pmod{12}$. Itt $(5,12) = 1$, így egy megoldás van: $x \equiv 2 \cdot 5^{\varphi(12)-1} \equiv 2 \cdot 5^3 \pmod{12}$. Mivel $5^2 \equiv 1 \pmod{12}$, így $x \equiv 2 \cdot 5^2 \cdot 5 \equiv 10 \pmod{12}$.

   Ha $a = 5, b = 3$, akkor $5x \equiv 3 \pmod{12}$. Itt $(5,12) = 1$, így egy megoldás van: $x \equiv 3 \cdot 5^{\varphi(12)-1} \equiv 3 \cdot 5^3 \equiv 3 \cdot 5 \equiv 3 \pmod{12}$.

2. Ha n prímtényezős felbontása $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, akkor $d(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$. Mivel 9 csak kétféle lényegesen különböző módon áll elő szorzat alakban: maga 9 vagy $3 \cdot 3$, így az n szám prímtényezős alakjára csak két lehetőség van: $n = p_1^8$ vagy $n = p_1^2 p_2^2$. Az első esetben $p_1 = 2$ jó, $p_1 = 3$ viszont már nem, mert $3^9 > 1000$. A második esethez előre annyit, hogy $31^2 < 1000 < 32^2$. Így a szóba jövő p_1, p_2 párokra $p_1 p_2 < 32$ kell teljesüljön, hogy $p_1^2 p_2^2 < 1000$ legyen. Így a párok: $(2,3), (2,5), (2,7), (2,11), (2,13), (3,5), (3,7)$. Végül n lehetséges értékei: $2^8, 2^2 \cdot 3^2, 2^2 \cdot 5^2, 2^2 \cdot 7^2, 2^2 \cdot 11^2, 2^2 \cdot 13^2, 3^2 \cdot 5^2, 3^2 \cdot 7^2$.

   Végül egy megjegyzés: az, hogy $d(n)$ páratlan, ekvivalens azzal, hogy n négyzetszám, hiszen a $d(n) = (\alpha_1+1)\dots(\alpha_k+1)$ szorzat pontosan akkor páratlan, ha minden tényezője páratlan, azaz minden α_i páros, ekkor viszont n minden prímtényezője páros hatványon szerepel, és így n négyzetszám.

3. Diofantoszi egyenletek nem szerepeltek előadáson, így ezeket nem is kell tudni zh-ra.

4.
- 303^{404} utolsó két számjegye éppen az a $0 \leq x < 100$ szám, melyre $x \equiv 303^{404} (\mathrm{mod}\, 100)$.
- $303 \equiv 3 (\mathrm{mod}\, 100) \Longrightarrow 303^{404} \equiv 3^{404} (\mathrm{mod}\, 100)$
- Az Euler–Fermat-tétel szerint ha $(3, 100) = 1$ (ami itt teljesül), akkor $3^{\varphi(100)} \equiv 1 (\mathrm{mod}\, 100)$ és mivel $\varphi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$, így $3^{40} \equiv 1 (\mathrm{mod}\, 100)$.
- Ekkor $3^{404} \equiv (3^{40})^{10} \cdot 3^4 \equiv 3^4 (\mathrm{mod}\, 100)$. Végül $3^4 \equiv 81 (\mathrm{mod}\, 100)$, így 303^{404} utolsó két számjegye 81.

5. (a) $5x \equiv 61 \pmod{444}$. $(5, 444) = 1$, így egy megoldás van. Az x együtthatója egy kicsi egész szám, ilyenkor érdemes a megoldást úgy keresni, hogy nézzük a 61, $61 + 444$, $61 + 2 \cdot 444$, $\ldots$, $61 + 4 \cdot 444$ számokat, és ezek között megkeresni az 5-tel oszthatót. Lehet pl. sorban venni őket, és már a második osztható is lesz 5-tel, $61 + 444 = 505$, így az $\frac{505}{5} = 101$ nyilván kielégíti a kongruenciát, és mivel a megoldás mod 444 egyértelmű, így a megoldás $x \equiv 101 \pmod{444}$.

   (b) $202x \equiv 157 \pmod{203}$. Itt pedig az segít, ha észrevesszük, hogy $202 \equiv -1 \pmod{203}$, azaz $-x \equiv 157 \pmod{203}$ és így $x \equiv -157 \equiv 46 \pmod{203}$.

6. Az Euler–Fermat-tétel szerint ha $(n, 35) = 1$ teljesül, akkor $n^{\varphi(35)} \equiv 1 \pmod{35}$. $\varphi(35) = 35(1 - \frac{1}{5})(1 - \frac{1}{7}) = 24$, és $(3, 35) = 1$, így $3^{24} \equiv 1 \pmod{35}$. Hasonlóan $(4, 35) = 1$ miatt $4^{24} \equiv 1 \pmod{35}$) is igaz, így $4^{24} \equiv 3^{24} \pmod{35}$), ami viszont épp azt jelenti, hogy $35 | 4^{24} - 3^{24}$.

7. 11 prím, így a kis-Fermat-tétel szerint $11 | n^{11} - n$ minden n pozitív egészre. Továbbá nyilván $11 | 11n$ minden n egészre, és így $11 | (n^{11} - n) + 11n = n^{11} + 10n$ minden n egészre.

8. Kínai maradéktétel sem szerepelt előadáson, így ezt sem kell tudni.

9. $(a + b)^p = \binom{p}{0} a^0 b^p + \binom{p}{1} a^1 b^{p-1} + \binom{p}{2} a^2 b^{p-2} + \cdots + \binom{p}{p} a^p b^0$. Itt a két szélső tag éppen a^p és b^p. Megvizsgáljuk a középső tagokat. Mindegyikben szerepel egy $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ binomiális együttható, ami osztható p-vel, mert a számlálóban van egy p prímtényező, míg a nevezőben minden tényező p-nél kisebb, így a nevezőben nincsen p-s prímtényező. Így a középső tagok mindegyike osztható p-vel, ami épp azt jelenti, hogy $(a + b)^p \equiv a^p + b^p \pmod{p}$.