Diszkrét matematika II. feladatok

6.

Gyakorló feladatok

1. Az RSA titkosításnál legyen $p = 11$, $q = 13$ és $e = 7$. a) Mi lesz d? b) Az $m = 4$ üzenetet szeretnénk titkosítani, mi lesz a titkosított üzenet?

2. Az RSA titkosításnál legyen $p = 7$, $q = 13$ és $e = 5$. A $c = 2$ titkosított üzenetet kaptuk. Mi az eredeti üzenet?

Érdekes feladatok

3. Az RSA titkosításnál legyen $n = 221$ és $e = 5$. A $c = 2$ titkosított üzenetet hallgattuk le. Mi lehet az eredeti üzenet?

Vegyes gyakorló feladatok

4. Számolja ki a $(3^{13} - 1, 3^8 - 1)$ ill. $(3^{15} - 1, 3^9 - 1)$ legnagyobb közös osztókat!

5. Oldja meg az $ax + by = c$ $(x, y \in \mathbb{Z})$ egyenletet adott a, b, c számok esetében

   a) $a = 27, b = 14, c = 5$; b) $a = 105, b = 40, c = 15$; c) $a = 115, b = -50, c = 10$;
   d) $a = -135, b = 70, c = 12$; e) $a = 117, b = -90, c = -6$; f) $a = 78, b = 93, c = -10$

6. Pajkos százlábúak futkároznak a ládában. Az egyik fajtának 12 lába van, a másiknak 23. Összesen 152 lábat számoltunk meg. Hány százlábú van a ládában?

7. A boltban a vásárlás során 150 forint a visszajáró. Hányféleképpen kaphatjuk meg a visszajárót, ha a pénztárgépben csak 20 és 50 forintosok vannak?

8. Oldja meg a következő egyenleteket egész számok körében!

   a) $27^a \cdot 81^b = 1/9$; b) $32^a \cdot 128^b = 16$ c) $i^a \cdot \left(\frac{1+i}{\sqrt{2}}\right)^b = -i$.

9. Legyen $a = 2^{13} - 1$ és $b = 2^8 - 1$. Határozza meg (számológép használata nélkül) azokat x, y egészeket, melyre $ax + by = (a, b)$.

10. Oldja meg az alábbi kongruenciákat:

    a) $13x \equiv 1 \mod 17$; b) $12x \equiv 18 \mod 15$; c) $7x \equiv 21 \mod 42$; d) $51x \equiv 69 \mod 152$
    a) $5x \equiv 1 \mod 25$; b) $31x \equiv 18 \mod 17$; c) $11x \equiv 21 \mod 120$; d) $65x \equiv 91 \mod 117$

11. Határozza meg azt a *két* legkisebb pozitív egész számot, mely

    a) 7-szeresét felírva 8-es számrendszerben az utolsó előtti jegy 4, az utolsó jegy pedig 3;

    b) 13-szorosát felírva 4-es számrendszerben az utolsó előtti jegy 2, az utolsó jegy pedig 1;

    c) 19-szorosát felírva 16-os számrendszerben az utolsó előtti jegy 1, az utolsó jegy pedig 2!

12. Határozza meg (a tízes számrendszerben felírt) 143^{143} utolsó három jegyét hármas alapú számrendszerben.

13. Milyen maradékot ad 103-mal osztva a következő szám: $205^{206^{207}}$?

14. Számolja ki az következő értékeket

    a) $6^{13^{20}} \mod 11$; b) $5^{15^{17}} \mod 12$; c) $13^{7^{120}} \mod 8$; d) $13^{9^{45}} \mod 17$

15. Felhasználva, hogy $g = 5$ generátor modulo 23, számolja ki a következő értékeket a diszkrét logaritmus tulajdonságai segítségével. Az eredményt ellenőrizze!

    a) $\log_5(5)$; b) $\log_5(2)$; c) $\log_5(10)$; d) $\log_5(20)$ e) $\log_5(4)$; f) $\log_5(9)$

Szorgalmi feladatok

16. Legyen F_n az n-edik Fibonacci szám. Ekkor $(F_n, F_{n-1}) = 1$. Oldja meg a $F_n \cdot x + F_{n-1} \cdot y = 1$ lineáris diofantikus egyenletet!

17. Írjon programot egészek faktorizációjára! Tekintsük a következő k bites egészeket:

k	n
40	684793814603
60	603141140725829899
80	605165905583175532445917
100	6344446223211257885360873458 51
120	665263035897162070681897421870027857
140	69757885218991000827076872397853566959968 3
160	731464442511808404319136684547345616528481453723
180	766996059271257858790344715690184347937909872494372031
200	804253659846418472879149405411605577932569166668425013521027
220	843321085627118096604442632091346426470017620515795831183527030727

Mekkora k értékre tudja n-et faktorizálni?