Schlotter Ildikó
ildi@cs.bme.hu

12. gyakorlat
Euklideszi algoritmus, prímtesztelés, nyilvános kulcsú titkosírás

1. Az euklideszi algoritmus segítségével határozd meg 7038 és 2499 legnagyobb közös osztóját! Mely számok állíthatóak elő $k \cdot 7038 + \ell \cdot 2499$ alakban, ha k és ℓ tetszőleges egészek lehetnek?

2. Az angol ábécé 26 betűjét a $0, 1, \ldots, 25$ számokkal helyettesítem. ($A = 0, B = 1, \ldots, Z = 25$.) Nyilvános kódolófüggvényem:

   $$x \to x^{43} \pmod{85}.$$

   Ezzel a függvénnyel kódoltam titkos üzenetemet, a kód a következő lett:

   $$59 \quad 2 \quad 59 \quad 20 \quad 44 \quad 52.$$

   Törd fel a kódomat, vagyis készítsd el a fenti kódolófüggvényhez a dekódolófüggvényt, és fejtsd meg vele a titkos üzenetet is!

3. A nyilvános kulcsú titkosírás dekódoló kulcsának működése a következő állításon alapszik: ha x és N adottak, akkor $x^{k \cdot \varphi(N)+1} \equiv x \pmod{N}$ teljesül minden k pozitív egészre. Ez az állítás könnyen bizonyítható, ha az Euler-Fermat tételből nyert $x^{\varphi(N)} \equiv 1 \pmod{N}$ összefüggést a k-adik hatványra emeljük, majd x-szel szorozzuk. Azonban az Euler-Fermat tétel alkalmazásához szükség van arra is, hogy $(x, N) = 1$ teljesüljön.

   Bizonyítsd be, hogy ha N két különböző prím szorzata (ez a nyilvános kulcsú titkosításnál fennáll), akkor $x^{k \cdot \varphi(N)+1} \equiv x \pmod{N}$ teljesüléséhez nem kell, hogy $(x, N) = 1$ igaz legyen!

4. Gyűrűt, ferdetestet, vagy testet alkotnak-e az alábbi halmazok? Ha más nincs feltüntetve, akkor a két művelet a szokásos összeadás és szorzás.

   a) $\{a + bi : a, b \in \mathbb{Z}, ab = 0\}$

   b) $\{a + bi : a, b \in \mathbb{Z}, b \text{ páros}\}$

   c) $\{a + bi : a, b \in \mathbb{Z}, a \text{ páros}\}$

   d) $\{0, 1\}$ a modulo 2 összeadással és szorzással

   e) a modulo m maradékosztályok a modulo m összeadással és szorzással

   e) a modulo m maradékosztályok a modulo m összeadással és szorzással, ha m prím

   f) a pozitív valós számok halmaza, a két művelet $a \oplus b = a \cdot b$ és $a \odot b = a^{\lg b}$

---

5. Bizonyítsd be, hogy az 561 $(= 3 \cdot 11 \cdot 17)$ Carmicheal-szám!

6. Sikerült elfognunk Recski tanár úr emailjét, amit Szeszlér tanár úrnak küldött, és leírja benne, hogy mi lesz a kérdés a vizsgán. Sajnálatos módon a levél az RSA algoritmussal titkosítva van, de az ismeretes, hogy Szeszlér tanár úr nyilvános kulcsa $(85, 43)$. Az eredeti üzenetben a számok jelentése:

A=2	D=6	G=11	J=21	M=26	P=31	S=36	V=41	Y=46
B=3	E=7	H=12	K=22	N=27	Q=32	T=37	W=42	Z=47
C=4	F=8	I=13	L=23	O=28	R=33	U=38	X=43	=48

   A titkosított üzenet a következő:

   $$8 \quad 27 \quad 58 \quad 48 \quad 22 \quad 81 \quad 48 \quad 76 \quad 27 \quad 8 \quad 3 \quad 6 \quad 8 \quad 46.$$

   Próbáljuk meg dekódolni a levelet!