Név: _____
Neptun-kód: _____
Pontszám: _____

Diszkrét modellek alkalmazásai ZH 2

2024. december 3.

1. **Oldd meg a következő szimultán kongruencia-rendszert!** **(12 pont)**

$$\begin{aligned} 5x &\equiv 1 \pmod 7 \\ 4x &\equiv 1 \pmod 9 \\ 8x &\equiv 1 \pmod{13} \end{aligned}$$

2. **Oldd meg a következő generátorokkal és diszkrét logaritmussal kapcsolatos feladatokat!** **(10 pont)**

   (a) **Generátor-e** 3 **modulo** 19**? Bizonyítsd be, vagy cáfold meg! Mennyi lesz** $\log_3 5$**,** $\log_3 8$**,** $\log_3 14$ **modulo** 19**?**

   (b) **Generátor-e** 2 **modulo** 23**? Bizonyítsd be, vagy cáfold meg! Mennyi lesz** $\log_2 3$**,** $\log_2 4$**,** $\log_2 12$ **modulo** 23**?**

3. **Egy RSA titkosításnál legyen a két titkos prím** $p = 7$**,** $q = 13$ **és a titkosító exponens** $e = 23$**. Titkosítsd az üzenetet** $m = 12$**!** **(12 pont)**

4. **Számítsd ki az Euklideszi algoritmussal az alábbi polinomok legnagyobb közös osztóját** $\mathbb{Z}_5$ **felett!** **(16 pont)**

$f(x) = x^5 - 20x^4 + 19x^3 - 3x^2 - 5x + 38$
$g(x) = 10x^5 + 12x^4 + 3x^3 - 7x^2 - 9x + 304$