Név: _____
Neptun-kód: _____
Pontszám: _____

Diszkrét modellek alkalmazásai ZH 2
Javító

2024. december 10.

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

$$10x \equiv 16 \pmod 9$$
$$6x \equiv 3 \pmod{21}$$
$$3x \equiv 2 \pmod 5$$

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

   (a) **Generátor-e** 10 **modulo** 23**? Bizonyítsd be, vagy cáfold meg! Mennyi lesz** $\log_{10} 5$**,** $\log_{10} 9$**,** $\log_{10} 20$ **modulo** 23**?**

   (b) **Generátor-e** 9 **modulo** 17**? Bizonyítsd be, vagy cáfold meg! Mennyi lesz** $\log_9 16$**,** $\log_9 7$**,** $\log_9 12$ **modulo** 17**?**

3. **Egy RSA titkosításnál legyen a két titkos prím** $p = 3$**,** $q = 17$ **és a titkosító exponens** $e = 9$**. Fejtsd vissza az kódolt üzenetet** $c = 8$**!** **(12 pont)**

4. **Számítsd ki az Euklideszi algoritmussal az alábbi polinomok legnagyobb közös osztóját** $\mathbb{Z}_7$ **felett!** **(16 pont)**

$f(x) = 9x^6 - 18x^5 + 7x^4 + 11x^3 - 19x^2 + 80x - 10$
$g(x) = 14x^6 + 4x^5 - 3x^4 + 35x^3 - x^2 + 5$