1. Ha egy egész szám 3 maradékot ad 4-gyel osztva, 1 maradékot 6-tal osztva, és 13 maradékot 15-tel osztva, akkor mennyi maradékot ad 20-szal osztva?

2. Oldjuk meg a következő szimultán kongruenciákat (ha megoldhatóak)!

a) $\begin{aligned} 5x &\equiv 16 \pmod{12} \\ x &\equiv 11 \pmod{63} \\ 4x &\equiv 12 \pmod{66} \end{aligned}$ b) $\begin{aligned} x &\equiv 15 \pmod{104} \\ x &\equiv -2 \pmod{39} \\ x &\equiv 5 \pmod{20} \end{aligned}$ c) $\begin{aligned} 3x &\equiv 15 \pmod{24} \\ 10x &\equiv 8 \pmod{14} \end{aligned}$

3. Oldjuk meg!

a) $5x^3 - 93 \equiv 0 \pmod{231}$
b) $x^{20} - 20x^2 - 5x + 3 \equiv 0 \pmod{836}$
c) $8x^{12} - 3x + 11 \equiv 0 \pmod{1001}$

4. a) Mennyi 2 rendje modulo: i) 7; ii) 15; iii) 257?
b) Lássuk be, hogy bármely k temészetes számra csak véges sok olyan p prím létezik, amelyre $o_p(2) = k$.

5. Ha $o_p(a) = 2000$ valamely p prímre, mennyi lehet: a) $o_p(a^2)$; b) $o_p(a^3)$; c) $o_p(-a)$?

6. Legyen $o_m(a) = k$ és $o_m(b) = \ell$. Bizonyítsuk be, hogy $o_m(ab)$ osztója $[k, \ell]$-nek, de többszöröse $\frac{[k,\ell]}{(k,\ell)}$-nek.

7. a) Tegyük fel, hogy $a^{33} \equiv -1 \pmod{71}$. Mennyi a^{22} maradéka modulo 71?
: −) b) Bizonyítsuk be, hogy ha b olyan természetes szám, amelyre $b^{12} \equiv -1 \pmod{71}$, akkor $2^b - 1$ prímszám.

8. Adjuk meg az összes primitív gyököt modulo: a) 13; b) 10; c) 18.

9. Keressünk egy primitív gyököt modulo 625.

10. Bizonyítsuk be, hogy ha m páratlan, és g primitív gyök modulo m, akkor g és $g + m$ közül a páratlan primitív gyök modulo $2m$.

11. Bizonyítsuk be, hogy ha $m > 1$ páratlan szám, és van primitív gyök modulo m, akkor $\mathbb{Z}_m^*$-ban egyetlen másodrendű elem van.

12. A 11. feladat eredményét felhasználva lássuk be, hogy nincs primitív gyök modulo m, ha m nem p^α, $2p^\alpha$ (valamely p páratlan prímre), vagy 4.

13. Hány megoldása van az $x^2 \equiv 1 \pmod{m}$ kongruenciának, ha $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$?

14. Lássuk be, hogy ha $a_1, a_2, \ldots, a_{\varphi(m)}$ redukált maradékrendszer modulo m, és $(k, \varphi(m)) = 1$ egy k természetes számra, akkor $a_1^k, a_2^k, \ldots, a_r^k$ is redukált maradékrendszer modulo m.