1.
a) Číslo $0 \leq x < 10000$ je v tzv. modulání reprezentaci vzhledem k prvočíslům 17, 23, 29 dáno svými zbytky (5, 13, 9) po dělení těmito prvočísly:
$x \equiv 5 \pmod{17}$, $x \equiv 13 \pmod{23}$, $x \equiv 9 \pmod{29}$.
Převeďte jej do modulární reprezentace vzhledem k prvočíslům 19, 31, 37.
(Nápověda: Určete prvně x.)
b) Jak se odpověď změní, nebudeme-li nadále požadovat $0 \leq x < 10000$?
(Nápověda: pro jaké reprezentace (a, b, c) vzhledem k 17, 23, 29 a (d, e, f) vzhledem k 19, 31, 37 bude nějaké x existovat?)

2.
a) Ukažte, že 55 je primitivní kořen modulo 106.
b) Kolik existuje primitivních kořenů modulo 106?

3.
V šifrovacím systému RSA s veřejným klíčem daným modulem 1763 a exponentem 97 došlo k prozrazení faktorizace modulu:
1763 = 41.43
Dešifrujte zprávu 11. (Nic nešifrujte, chce se po vás pouze dešifrování.)

4.
Zbytková třída a (mod m) splňuje $a^{48} \equiv 1 \pmod{m}$, $a^{38} \equiv 1 \pmod{m}$. Jaký může být řád této zbytkové třídy? Pro obě možnosti uveďte příklad takové zbytkové třídy, tj. čísla a. (Nápověda: Využijte Eukleidova algoritmu k postupnému dělení mocnin a^{48}/a^{38} atd.)

5.
Najděte všechna přirozená čísla m, pro něž $\varphi(m) = 46$, kde φ značí Eulerovu funkci.