KRY: Wahlfach Kryptologie
Serie 3: Chinesischer Restsatz, Attacken auf RSA

Aufgabe 1
Es sollen mit Hilfe von PARI/GP **Common Modulus Attacken** gerechnet werden. Bekannt sind dabei jeweils: Der (gemeinsame) Modulus m, Alice's öffentlicher Schlüssel e_2, sowie das eigene Schlüsselpaar d_1/e_1.

Rechnen Sie je mit den folgenden Angaben:

- $m = 91$, $e_1 = 5$, $d_1 = 29$, $e_2 = 7$. **Zugehöriges Ergebnis:** $d_2 = 103$.
- $m = 221$, $e_1 = 5$, $d_1 = 269$, $e_2 = 35$. **Zugehöriges Ergebnis:** $d_2 = 11$.

Aufgabe 2
Es soll mit Hilfe von PARI/GP eine **Low Exponent Attacke** für $e = 3$ durchgeführt werden. Bekannt sind dazu:

- die drei RSA-Module
$$m_1 = 15, m_2 = 22, m_3 = 391,$$
- die drei entsprechenden Chiffrate
$$c_1 = 2, c_2 = 6, c_3 = 121.$$

Wie lautet die gesendete Klartextnachricht?

Aufgabe 3
Von einer Klasse mit n Personen weiss man, dass bei der Aufteilung in Zweiergruppen, Dreiergruppen, Vierergruppen jeweils eine Person übrigbleibt. Teilt man sie in Fünfergruppen, so bleiben sogar 2 übrig.

Bestimmen Sie n mit Hilfe des chinesischen Restsatzes, wenn man weiss, dass die Klasse weniger als 60 Leute hat.