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.

1) $x \cdot e_2 \bmod v = 1 \rightarrow \varphi(n) \mid v$

↳ $x \cdot e_2 \bmod \varphi(n) = 1$

① $v = e_1 \cdot d_1 - 1 = 5 \cdot 29 - 1 = 144$

② $ggT(v, e_2) = 1 = ggT(7, 144)$

↳ $x \cdot e_2 \bmod v = 1$

$= x \cdot 7 \bmod 144 = 1$

$x = 103$

```
gp > Mod(7,144)^-1
%2 = Mod(103, 144)
```

euklid

$144 = 20 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

---

2) $m_1 = 15$; $m_2 = 22$; $m_3 = 391$

$c_1 = 2$; $c_2 = 6$; $c_3 = 121$

$e = 3$

pari/gp

$M_1 = 22 \cdot 391 = 8602$

$M_2 = 15 \cdot 391 = 5865$

$M_3 = 15 \cdot 22 = 330$

$u_1 = Mod(8602, 15)^{-1} = 13$

$u_2 = Mod(5865, 22)^{-1} = 17$

$u_3 = Mod(330, 391)^{-1} = 141$

$X = 2 \cdot 13 \cdot 8602 + 6 \cdot 17 \cdot 5865 + 121 \cdot 141 \cdot 330 \bmod (15 \cdot 22 \cdot 391)$

$= 6'452'012 \bmod 129'030 = \underline{512}$

$x^{\frac{1}{3}} = 512^{\frac{1}{3}} = \underline{\underline{8}}$

3)

$x \bmod 2 = 1$
$x \bmod 3 = 1$
$x \bmod 4 = 1$
$x \bmod 5 = 2$

nicht teilerfremd, also mod 2 nicht nötig

↳ $m_1 = 3$; $m_2 = 4$; $m_3 = 5$ $\quad y_1 = 1$; $y_2 = 1$; $y_3 = 2$

$M_1 = 4 \cdot 5 = 20$
$M_2 = 3 \cdot 5 = 15$
$M_3 = 3 \cdot 4 = 12$

$u_1 = \text{Mod}(20, 3)^{-1} = 2$
$u_2 = \text{Mod}(15, 4)^{-1} = 3$
$u_3 = \text{Mod}(12, 5)^{-1} = 3$

{ pari/gp

$x = 1 \cdot 2 \cdot 20 + 1 \cdot 3 \cdot 15 + 2 \cdot 3 \cdot 12 \bmod 60$
$= 157 \bmod 60 = \underline{37}$