RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae, Philipp Wagner, Vera Knüppels

Hausübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 4

Abgabe bis 30. April 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F2 (4 Punkte)**:**
Bestimmen Sie mit Hilfe der Kongruenzrechnung die letzten beiden Dezimalstellen der Zahl $9^{123456789}$.

Lösung: Zunächst bestimmt man die Ordnung von 9 mod 100:

$$\begin{aligned}
9 &\equiv 9 \bmod 100\\
9^2 &\equiv 81 \bmod 100\\
9^3 &\equiv 29 \bmod 100\\
9^4 &\equiv 61 \bmod 100\\
9^5 &\equiv 49 \bmod 100\\
9^6 &\equiv 41 \bmod 100\\
9^7 &\equiv 69 \bmod 100\\
9^8 &\equiv 21 \bmod 100\\
9^9 &\equiv 89 \bmod 100\\
9^{10} &\equiv 1 \bmod 100
\end{aligned}$$

Nun gilt

$$\begin{aligned}
9^{123456789} &\equiv 9^{123456789 \bmod 10} \bmod 100\\
&\equiv 9^9 \bmod 100\\
&\equiv 89 \bmod 100
\end{aligned}$$

Damit ergeben sich die letzten beiden Ziffern zu 89.

Eine weitere Lösungsmöglichkeit liefert die Euler'sche φ-Funktion. Es gilt

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2^1)(5^2 - 5^1) = 40$$

und damit

$$9^{123456789} \equiv 9^{123456789 \bmod 40} \equiv 9^{29} \bmod 100.$$

Aus

$$9^{29} \equiv 9^{29 \bmod 20} \equiv 9^9 \equiv 14 \bmod 25$$

und

$$9^{29} \equiv 9^{29 \bmod 3} \equiv 1^2 \equiv 1 \bmod 4$$

folgt mit CRT: $9^{29} \equiv 25 + 14 \cdot 4 \cdot 19 \equiv 89 \bmod 100$.

AUFGABE 2 F1 (6 Punkte)**:**
Finden Sie ein x, dass alle folgenden Kongruenzen erfüllt. Geben Sie alle Zwischenschritte an.

$$\begin{aligned} x &\equiv 2 \bmod 5 \\ x &\equiv 7 \bmod 14 \\ x &\equiv 5 \bmod 18 \end{aligned}$$

Lösung: Es gilt

$$x \equiv 7 \bmod 14 \Leftrightarrow x \equiv 7 \bmod 2 \wedge x \equiv 7 \bmod 7$$

und

$$x \equiv 5 \bmod 18 \Leftrightarrow x \equiv 5 \bmod 2 \wedge x \equiv 5 \bmod 9.$$

Da $5 \equiv 7 \bmod 2$ existiert eine Lösung, für die gelten muss:

$$\begin{aligned} x &\equiv 2 \bmod 5 \\ x &\equiv 0 \bmod 7 \\ x &\equiv 1 \bmod 2 \\ x &\equiv 5 \bmod 9 \end{aligned}$$

Der Chinesische Restsatz liefert

$$\begin{aligned} x &\equiv 2 \cdot 126_5^{-1} \cdot 126 + 0 \cdot 90_7^{-1} \cdot 90 + 2 \cdot 315_2^{-1} \cdot 315 + 5 \cdot 70_9^{-1} \cdot 70 \bmod 630 \\ &\equiv 2 \cdot 126 + 0 + 315 + 5 \cdot 4 \cdot 70 \bmod 630 \\ &\equiv 1967 \bmod 630 \\ &\equiv 77 \bmod 630 \end{aligned}$$

AUFGABE 3 F2 (5 Punkte)**:**
Ein Bienenvolk hat zwischen 200 und 250 Mitglieder. Stellt man sie in 7er Reihen auf, so bleibt eine Biene alleine. Stellt man sie dagegen in 5er Reihen auf, so bleiben drei übrig. Wie viele Bienen sind es genau?

Lösung: Sei x die Anzahl der Bienen. Laut Aufgabenstellung gilt $x \equiv 1 \bmod 7$ und $x \equiv 3 \bmod 5$. Mit CRT folgt:

$$x \equiv 1 \cdot 5 \cdot 3 + 3 \cdot 7 \cdot 3 \equiv 78 \equiv 8 \bmod 35$$

Damit gilt $x = 35k + 8$ für $k \in \mathbb{N}$. Das einzige k für das x zwischen 200 und 250 liegt, ist $k = 6$. Damit hat das Volk genau 218 Bienen.