Übungen zur Vorlesung **Blatt 2**
Elliptische Kurven und Kryptographie 27.04.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 4. Mai 2015, bis 12:15 Uhr in die Briefkästen

---

Aufgabe 1:

Entfernt man aus einem Korb jedesmal gleichzeitig $2, 3, 4, 5$ oder 6 Eier, bleiben jeweils $1, 2, 3, 4$ bzw. 5 Eier zurück. Nimmt man jedesmal 7 Eier zugleich fort, bleibt keines übrig. Bestimmen Sie die kleinste Anzahl von Eiern, die der Korb enthalten haben kann.

Aufgabe 2:

Berechnen Sie durch schnelles Potenzieren bzw. mithilfe des Satzes von Euler-Fermat folgende Werte:

(a) $3^{201} \bmod 11$,

(b) $2^{917} \bmod 111$.

Aufgabe 3:

(a) Finden Sie vier Zahlen $n \in \mathbb{N}$ mit $\varphi(n) = 16$.

(b) Zeigen Sie, dass $2\varphi(n) = n$ genau dann gilt, wenn $n = 2^\ell$ mit $\ell \in \mathbb{N}$.

(c) Zeigen Sie, dass $3\varphi(n) = n$ genau dann gilt, wenn $n = 2^\ell 3^m$ mit $\ell, m \in \mathbb{N}$.

Aufgabe 4:

(a) Zeigen Sie, dass eine endliche Gruppe von Primzahlordnung zyklisch ist.

(b) Zeigen Sie $a^p \equiv a \bmod p$ für beliebiges $a \in \mathbb{Z}, p \in \mathbb{P}$. Gilt auch $a^{\varphi(n)+1} \equiv a \bmod n$ für beliebiges $a \in \mathbb{Z}, n \in \mathbb{N}$? (Hinweis: Betrachte $n = p^2, a = ?$.)

(c) Bestimmen Sie mithilfe des Satzes von Euler-Fermat die letzten beiden Ziffern von 7^{111111}.