Schulmathematik vom höheren Standpunkt **M. Hofacker / W. Kimmerle**
WS 2015/16

Übungsblatt 5

Aufgabe 21:

Sei n das Produkt von drei Primzahlen p, q, r. Ist für dieses n die Aussage von Lemma 3.11, dass für jedes $x \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$x^{k\cdot\varphi(n)+1} = x$$

ebenfalls richtig?
Diskutieren Sie die Antwort im Zusammenhang mit dem RSA - Verfahren.

Aufgabe 22:

a) Welche der folgenden Zahlen sind Pseudoprimzahlen zur Basis 2, welche sind Carmichaelzahlen.

$$127, 6601, 15709, 294409, \quad 21 \cdot p \quad \text{mit} \quad p \quad \text{Primzahl}$$

b) Welche Zahl ist die kleinste Carmichaelzahl ?
c) Zeigen Sie (Methode von Chernick): Sind $6m+1, 12m+1, 18m+1$ Primzahlen, dann ist ihr Produkt eine Carmichaelzahl.

Aufgabe 23:

a) Zeigen Sie: Ist n eine ungerade Pseudoprimzahl zur Basis 2, dann ist auch $2^n - 1$ eine Pseudoprimzahl zur Basis 2.
b) Müssen Pseudoprimzahlen p zu einer Basis a quadratfrei sein ?

Aufgabe 24:

Die Bezeichnungen seien wie beim RSA - Verfahren. B gibt als öffentlichen Schlüssel $(n, e) = (1633, 13)$ bekannt. K sendet daraufhin an B die Ziffernfolge $87, 1478, 120$. Wie lautet die Ziffernfolge der eigentlichen Mitteilung von K an B?
Welche Berechnungen musste B zur Erstellung des öffentlichen Schlüssels durchführen und welche zum Dechiffrieren ?

Aufgabe 25:

(eine Formel von Legendre). Sei $n \in \mathbb{N}, p \in \mathbb{N}$ eine Primzahl und

$$n = \sum_{i=1}^{r} a_i p^i$$

mit $r = \left\lceil \frac{log\ n}{log\ p} \right\rceil$ die p - adische Zifferdarstellung von n. Setze $s_p(n) := \sum_{i=1}^{r} a_i$. Dann gilt

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1} \ .$$