Elementare Zahlentheorie

Blatt 6 — 21.05.2015

Aufgabe 21. (3 Punkte)

Bestimmen Sie (ohne Rechner!) die letzten zwei Ziffern in der Dezimaldarstellung von $7^{\left(7^{\left(7^7\right)}\right)}$.

Aufgabe 22. (Fermat-Pseudoprimzahlen, 4 Punkte)

Zeigen Sie:

(a) 341 ist eine Fermat-Pseudoprimzahl zur Basis 2.

(b) Es gibt unendlich viele Fermat-Pseudoprimzahlen zur Basis 2.
Hinweis: Zeigen Sie dazu, dass mit n auch $2^n - 1$ eine Fermat-Pseudoprimzahl zur Basis 2 ist.

Aufgabe 23. (Primitivwurzeln, 3+2+2* Punkte)

(a) Bestimmen Sie *alle* Primitivwurzeln modulo 11, 13 und 17.

(b) Zeigen Sie: Es gibt keine Primzahl p, so dass 4 eine Primitivwurzel modulo p ist.

(c*) Nutzen Sie ein Computeralgebrasystem, um die kleinste Primzahl zu berechnen, für die die kleinste Primitivwurzel größer als 100 ist.

— bitte wenden —

Aufgabe 24. (RSA-Verfahren, 4 Punkte)

Alice will sich mit Bob zu einem geheimen Treffen verabreden. Dazu hat Bob einen öffentlichen RSA-Schlüssel $(4141, 127)$ rausgegeben, und Alice hat ihre Nachricht durch das RSA-Verfahren verschlüsselt und an Bob gesendet. Inzwischen haben Sie doch einen Zugriff auf diese Nachricht, die folgendermaßen lautet:

$$2993 \quad 3130 \quad 1627$$

Können Sie diese hacken? Sie dürfen für die Bearbeitung dieser Aufgabe einen Computer benutzen.

Erläuterung: Zur Verschlüsselung werden die Buchstaben gemäß folgender Tabelle in Zahlen umgewandelt. Anschließend wurde die Ziffernfolge in 4-stellige Blöcke unterteilt. Bei Bedarf wird der letzte Block mit Leerzeichen " " = 36 aufgefüllt.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Abgabe: Am kommenden Donnerstag, den 28.05.2015, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/54089776/Elementare_Zahlentheorie`
