Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2017
12. Juli 2017

Einführung in die Zahlentheorie

Übungsblatt 11

Aufgabe 41

Sei $N = pq$ ein RSA-Modul und e ein zugehöriger Verschlüsselungs-Exponent, d.h. $\gcd(e, \varphi(N)) = 1$. Sei $\lambda(N) := \operatorname{lcm}(p-1, q-1)$ und d' definiert durch

$$ed' \equiv 1 \bmod \lambda(N).$$

Man zeige, dass man d' als Entschlüsselungs-Exponent verwenden kann, d.h.

$$x^{ed'} \equiv x \bmod N \quad \text{für alle } x \in \mathbb{Z}/N.$$

In welcher Beziehung steht d' zum üblichen Entschlüsselungs-Exponenten d, der durch $ed \equiv 1 \bmod \varphi(N)$ definiert ist?

Aufgabe 42

Seien N, p, q, e, d wie in Aufgabe 41 und

$$E : \mathbb{Z}/N \to \mathbb{Z}/N, \quad x \mapsto E(x) := x^e,$$

die Verschlüsselungs-Funktion. Ein Fixpunkt von E ist ein Element $x \in \mathbb{Z}/N$ mit $E(x) = x$.

a) Man zeige, dass die Abbildung E mindestens 9 Fixpunkte besitzt (darunter die trivialen $x = 0, \pm 1$). Genauer beweise man für die Anzahl r der Fixpunkte die Formel

$$r = (1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1)).$$

b) Man überlege sich, wie man im Fall $r = 9$ aus der Kenntnis eines nicht-trivialen Fixpunkts die Faktorzerlegung von N ableiten kann.

c) Man berechne alle Fixpunkte im Fall $(N, e) := (47299541, 65)$.

Aufgabe 43

Seien $p, q \geqslant 3$ teilerfremde ungerade Zahlen, die entweder prim oder Carmichael-Zahlen sind. Sei $N := pq$ und seien e und d natürliche Zahlen mit $ed \equiv 1 \bmod (p-1)(q-1)$. Man zeige

$$x^{ed} \equiv x \bmod N \quad \text{für alle} \quad x \in \mathbb{Z}.$$

Warum ist es beim RSA-Kryptosystem trotzdem vorzuziehen, für p und q Primzahlen und nicht Carmichael-Zahlen zu verwenden?

---

b.w.

Aufgabe 44

Der *Fermatsche Algorithmus* zur Faktorisierung einer zusammengesetzten ungeraden Zahl $N \geqslant 9$ arbeitet wie folgt: Mit $x_0 := \lceil \sqrt{N} \rceil$ berechne man für $x := x_0 + k$, $k = 0, 1, 2, 3, \ldots$, der Reihe nach die Differenzen $x^2 - N$, bis sich eine Quadratzahl ergibt:

$$x^2 - N = y^2.$$

Dann ist $N = (x - y)(x + y)$ eine nicht-triviale Faktorzerlegung von N.

a) Man beweise, dass der Algorithmus stets nach einer endlichen (aber möglicherweise großen) Anzahl von Schritten erfolgreich ist.

Man faktorisiere mit diesem Verfahren die Zahlen

$$N_1 := 3763, \qquad N_2 := 23843, \qquad N_3 := 39889.$$

b) Sei $N = uv$ mit positiven ganzen Zahlen u, v, die der Abschätzung

$$|u - v| \leqslant \alpha \sqrt[4]{N}$$

mit einer (nicht zu großen) reellen Konstanten α genügen. Man schätze (in Abhängigkeit von α) die Anzahl der Schritte ab, die der Fermatsche Algorithmus zur Faktorisierung von N braucht.

c) Um ein RSA-System mit Modul $N = pq$, wobei $2^{2m-1} < N < 2^{2m}$, (z.B. $m = 512$) aufzustellen, wird empfohlen, die Primzahlen p, q so zu wählen, dass

$$|p - q| \geqslant 2^{m-7}.$$

Warum ist das Fermatsche Faktorisierungs-Verfahren zur Faktorisierung von N dann ungeeignet?