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

SS 2017
19. Juli 2017

Einführung in die Zahlentheorie

Übungsblatt 12

Aufgabe 45

Sei $(N, e) = (8881, 17)$ der öffentliche Schlüssel eines Mini-RSA-Systems (d.h. eines unrealistisch kleinen RSA-Systems). Man berechne den Entschlüsselungs-Exponenten d.

Aufgabe 46

Sei (N, e) der öffentliche Schlüssel eines RSA-Systems,
wobei $N = pq$, $p \neq q$ prim, $\gcd(e, (p-1)(q-1)) = 1$, und

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

die Verschlüsselungs-Funktion.

a) Man zeige: Es gibt einen Exponenten $r > 0$, so dass $E^r(x) = x$ für alle $x \in \mathbb{Z}/N$, also $E^{-1} = E^{r-1}$.

b) Man berechne r in den Fällen $(N, e) = (8881, 17)$ und $(N, e) = (9017, 17)$.

Aufgabe 47

Alice und Bob benutzen zur Schlüssel-Vereinbarung ein Mini-Diffie-Hellman-System mit der multiplikativen Gruppe $(\mathbb{Z}/p)^*$ mit $p := 8039$ und der Primitivwurzel $g := 11$. Alice schickt an Bob das Element

$$A = g^\alpha = 5655 \in (\mathbb{Z}/p)^*$$

und Bob an Alice das Element

$$B = g^\beta = 5802 \in (\mathbb{Z}/p)^*.$$

Welcher gemeinsame Schlüssel $K = A^\beta = B^\alpha \in (\mathbb{Z}/p)^*$ ergibt sich daraus?

Aufgabe 48

a) Sei p eine ungerade Primzahl. Man zeige: Genau dann lässt sich p in der Form $p = x^2+2y^2$ mit ganzen Zahlen x, y darstellen, wenn $p \equiv 1 \bmod 8$ oder $p \equiv 3 \bmod 8$.

b) Welche natürlichen Zahlen n lassen sich in der Form $n = x^2 + 2y^2$ darstellen?

Hinweis. Man benutze, dass der Ring $\mathbb{Z}[\sqrt{-2}]$ euklidisch ist.