TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Prof. Dr. Mathias Schulze
Dipl.-Math. Cornelia Rottner
Fachbereich Mathematik

Elementare Zahlentheorie

Sommersemester 2016 - 3.Übungsblatt

Abgabetermin: **25.5.2016, 16:00h**

Aufgabe 1. Zeigen Sie: Lässt sich eine natürliche Zahl n auf zwei verschiedene Arten als Summe zweier Quadratzahlen schreiben, das heißt, gilt $n = x^2 + y^2 = z^2 + w^2$ mit $x, y, z, w \in \mathbb{Z}$ und $\{x^2, y^2\} \neq \{z^2, w^2\}$, so ist n keine Primzahl.

Hinweis: Es ist hilfreich zunächst folgende Behauptungen zu zeigen:

(a) *O.B.d.A. kann man* $x \equiv z \pmod 2$ *und* $y \equiv w \pmod 2$ *voraussetzen.*

(b) *Die Gleichungen*

$$\frac{x+z}{2} = ac, \frac{z-x}{2} = bd, \frac{y+w}{2} = cb, \frac{y-w}{2} = ad$$

haben ganzzahlige Lösungen $a, b, c, d \in \mathbb{Z}$.

(c) *Es gilt* $n = (a^2 + b^2)(c^2 + d^2)$.

Aufgabe 2.

(a) Sie wollen die Nachricht $m = 2016$ mit mithilfe des RSA-Verfahrens verschlüsseln. Hierzu wählen Sie die Primzahlen $p = 53$ und $q = 71$. Bestimmen Sie einen geeigneten geheimen Schlüssel, sowie den dazugehörigen öffentlichen Schlüssel und verschlüsseln Sie ihre Nachricht. Wie viele Möglichkeiten gibt es den geheimen Schlüssel zu wählen?

(b) Sie hören die mit dem RSA-Verfahren verschlüsselte Nachricht 17 mit. Von dem „öffentlichen“ Schlüssel (d, n) ist Ihnen nur $n = 21$ bekannt. Entschlüsseln Sie die Nachricht unter der Annahme, dass $f_{(d,n)} \neq \mathrm{id}$ gilt.

Aufgabe 3. Zeigen Sie, dass für eine Zahl $n \in \mathbb{Z}_{\geq 2}$ folgende Aussagen äquivalent sind:

(a) n ist das Produkt paarweise verschiedener Primzahlen.

(b) Für alle $a \in \mathbb{Z}$ gilt $a^{\varphi(n)+1} \equiv a \pmod n$.

(c) Für alle $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$ mit $b \equiv 1 \pmod{\varphi(n)}$ gilt $a^b \equiv a \pmod n$.

Aufgabe 4. Betrachten Sie für $a, b, m, n \in \mathbb{Z}_{>0}$ das Element $(\bar{a}_m, \bar{b}_n) \in (\mathbb{Z}_m \times \mathbb{Z}_n, +)$.

(a) Zeigen Sie: Für die Ordnung von $(\bar{a}_m, \bar{b}_n)$ gilt

$$o((\bar{a}_m, \bar{b}_n)) = \mathrm{kgv}(o(\bar{a}_m), o(\bar{b}_n)) = \mathrm{kgv}\left(\frac{\mathrm{kgv}(a,m)}{a}, \frac{\mathrm{kgv}(b,n)}{b}\right).$$

(b) Folgern Sie aus Teil (a): $\mathbb{Z}_m \times \mathbb{Z}_n$ ist nicht zyklisch, wenn m und n nicht teilerfremd sind.

(c) Geben Sie einen Alternativbeweis für die Aussage in Aufgabenteil (b) unter Verwendung eines Resultates aus der Vorlesung.