Nicola Oswald, Prof. Dr. Jörn Steuding
Institut für Mathematik, Universität Würzburg
Virtuelle Hochschule Bayern

Grundlagen der elementaren Zahlentheorie — Übungsaufgaben zum dritten Modul

Aufgabe 1.
Erstelle zu den Zahlen $3300, 315000,$ *und* 3402000 *eine Tabelle, die deren Primzahlzerlegung darstellt. Eine Spalte soll hierbei jeweils einer Primzahl gewidmet sein. Füge zwei weitere Zeilen ein, die*

- *den größten gemeinsamen Teiler und*
- *das kleinste gemeinsame Vielfache*

der Zahlen in ihrer Primfaktorzerlegung auflisten.
Wäre dieses Verfahren für die Zahlen $3300, 315001,$ *und* 3402001 *wesentlich schwieriger? Berechne* $ggT(3300, 315001, 3402001)$.

Aufgabe 2.
Bestimme mit Hilfe des aus der Vorlesung bekannten Verfahrens den größten gemeinsamen Teiler von

- 1287 *und* 871.
- 71894 *und* 45327.

Lösungsskizze

- Es gilt
$$\begin{aligned} 1287 &= 1 \cdot 871 + 416 \\ 871 &= 2 \cdot 416 + 39 \\ 416 &= 10 \cdot 39 + 26 \\ 39 &= 1 \cdot 26 + 13 \\ 26 &= 2 \cdot 13, \end{aligned}$$
woraus folgt, dass der größte gemeinse Teiler von 1287 und 871 die 13 ist.
- Es gilt
$$\begin{aligned} 71894 &= 1 \cdot 45327 + 26567 \\ 45327 &= 1 \cdot 26567 + 18760 \\ 26567 &= 1 \cdot 18760 + 7807 \\ 18760 &= 2 \cdot 7807 + 3146 \\ 7807 &= 2 \cdot 3146 + 1515 \\ 3146 &= 2 \cdot 1515 + 116 \\ 1515 &= 13 \cdot 116 + 7 \\ 116 &= 16 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1, \end{aligned}$$
also ist der größte gemeinsame Teiler von 71894 und 45327 die 1, sprich 71894 und 45327 sind teilerfremd.

Aufgabe 3.

- *Finde mit Hilfe des euklidischen Algorithmus eine ganzzahlige Lösung für die Gleichung*
$$29x - 13y = 17.$$
- *Gib die Lösungsgesamtheit der Gleichung*
$$106X - 333Y = 1$$
an.
- *Untersuche, für welche Werte die diophantische Gleichung*
$$5x + 8y = c$$
lösbar ist. Gebe gegebenenfalls die Lösungsmenge an.

Aufgabe 4.

(i) *Berechne die Kettenbrüche der rationalen Zahlen:* $\frac{97}{23}$, $\frac{99}{70}$, $-\frac{351}{17}$, $\frac{13\,254}{53\,412}$.

(ii) *welche rationalen Zahlen besitzen die folgenden Kettenbruchentwicklungen:*
$$[1,1,1],\ [1,1,1,1],\ [1,2,3,4]\ ?$$

Aufgabe 5.
Ein Jahr hat $J := 365,2425$ *Tage und ein synodischer Mondumlauf zählt* $M := 29,53059$ *Tage. Die Griechen haben so gerechnet, dass* 235 *Monate gerade* 19 *Jahre ergeben. Offensichtlich ist* $\frac{19}{235}$ *eine sehr gute Näherung für* $w := \frac{M}{J}$ *. Begründe dies mit Hilfe des Kettenbruchs von* $\frac{M}{J}$ *. Um welche Konvergente handelt es sich? Gebe den nächsten Koeffizienten an und schätze den Fehler ab.*
Zusatzfrage: Warum fällt Ostern alle 19 Jahre auf 'fast' dasselbe Datum?

Aufgabe 6.

- *Bestimme die Lösung des Systems*
$$\begin{aligned} 5x &\equiv 2 \bmod 3 \\ 4x &\equiv 7 \bmod 9 \\ 2x &\equiv 4 \bmod 10. \end{aligned}$$
- *Aus einem indischen Rechenbuch (Mahaviracarya, um* 850 *n. Chr.):*
Aus Früchten werden 63 *gleich große Haufen gelegt,* 7 *Stück bleiben übrig. Es kommen* 23 *Reisende, unter denen die Früchte gleichmäßig verteilt werden, so dass keine übrigbleibt. Wie viele waren es?*

Aufgabe 7.

(i) *Berechne* $\varphi(72)$.
(ii) *Was ist die Definition einer 'multiplikativen zahlentheoretischen Funktion'. Gib Deine Quelle an - Internet ist nicht erlaubt!*
(iii) *Beweise, dass die Eulersche* φ*-Funktione eine multiplikative Funktion ist.*

Aufgabe 8.
Als öffentlicher Schlüssel eines RSA-Systems hat Bob Alice $N = 247$ *und* $e = 7$ *zukommen lassen.*

(i) *Du bist Alice und möchtest die Nachricht* $M = 10$ *verschlüsseln.*
(ii) *Verschlüssel als nchstes die Nachricht* $M = 100 = 10^2$.
(iii) *Jetzt bist Du Bob und willst Dir Deinen geheimen Schlüssel* d *berechnen.*
(iv) *Du empfängst die verschlüsselte Nachricht* $C = 2$ *von Alice. Wie lautet der entsprechende Klartext?*

Aufgabe 9.
Ein Planet wird von zwei Monden umrundet. Der erste braucht für die Umrundung 31 *Tage, der zweite* 65 *Tage, immer relativ zur Sonnenposition gerechnet. Zurzeit sind vom Vollmond des ersten Mondes* 7 *Tage vergangen und der zweite steht bei Tag* 25 *seit seinem letzten Vollmond. Unsere Zeitrechnung beginnt, wenn beide Monde im Vollmond stehen. Nach wie vielen Tagen ist die beschriebene Konstellation erreicht?*

Aufgabe 10.
Angenommen, man kennt einen öffentlichen RSA-Schlüssel mit dem Modul $N = 143$ *und dem Exponenten* $e = 11$.

(i) *Ist die Wahl des Exponenten zulässig (von der eher unrealistischen Größe mal abgesehen)? Begründe Deine Antwort!*
(ii) *Bestimme den zur Nachricht* $M = 60$ *gehörenden Geheimtext.*
(iii) *Breche die Verschlüsselung, indem Du den geheimen Schlüssel* d *bestimmst.*