Präsenzübungen

Aufgabe P 16. *Erweiterter euklidischer Algorithmus*

Es seien zwei ganze Zahlen x und y gegeben. Mit dem **erweiterten euklidischen Algorithmus** können wir

- den **größten gemeinsamen Teiler** $\mathrm{ggT}\,(x,y)$ von x und y bestimmen,
- die Zahl $\mathrm{ggT}\,(x,y)$ als sogenannte **Vielfachsumme** darstellen, d.h. ganze Zahlen a und b derart bestimmen, dass

$$\mathrm{ggT}\,(x,y) \;=\; a\cdot x \;+\; b\cdot y \qquad \text{gilt.}$$

Beispiel: Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst $\mathrm{ggT}\,(93,39)$:

$$\begin{aligned} 93 &= 2\cdot 39 + 15\\ 39 &= 2\cdot 15 + 9\\ 15 &= 1\cdot 9 + 6\\ 9 &= 1\cdot 6 + 3\\ 6 &= 2\cdot 3 + 0 \end{aligned}$$

Wir erkennen in der letzten Zeile die Abbruchbedingung „Division geht auf“:

$$6 = 2\cdot 3 + 0.$$

In den beiden letzten Zeilen sehen wir den größten gemeinsamen Teiler von 93 und 39.

$$\mathrm{ggT}\,(93,39) \;=\; 3.$$

Mit der **Erweiterung** des euklidischen Algorithmus' verschaffen wir uns nun eine Darstellung der Form

$$\mathrm{ggT}\,(93,39) = 3 \;=\; a\cdot 93 + b\cdot 39 :$$

Wir stellen hierzu zunächst die vorletzte Zeile $9 = 1\cdot 6 + 3$ unserer vorherigen Rechnung um:

$$3 = 9 - 1\cdot 6 \tag{1}$$

Dies ist bereits eine Vielfachsummendarstellung von 3, allerdings nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 9 und 6. Wir gehen nun schrittweise rückwärts vor.

Aus der **drittletzten** Zeile $15 = 1\cdot 9 + 6$ erhalten wir eine Darstellung für 6, nämlich $6 = 15 - 1\cdot 9$, die wir in Gleichung (1) einsetzen:

$$3 = 9 - 1\cdot \underbrace{(15 - 1\cdot 9)}_{6} = -1\cdot 15 + 2\cdot 9 \tag{2}$$

Aus der **viertletzten** Zeile $39 = 2\cdot 15 + 9$ erhalten wir eine Darstellung für 9, nämlich $9 = 39 - 2\cdot 15$, die wir in Gleichung (2) einsetzen:

$$3 = -1\cdot 15 + 2\cdot \underbrace{(39 - 2\cdot 15)}_{9} = -5\cdot 15 + 2\cdot 39 \tag{3}$$

Zwischenergebnis:

$$3 = -5\cdot 15 \;+\; 2\cdot 39 \tag{3}$$

Auch dies ist eine Vielfachsummendarstellung von 3, allerdings noch immer nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 15 und 39. Wir müssen also die Zahl 15 noch ersetzen. Aus der **fünftletzten** Zeile $93 = 2\cdot 39 + 15$

erhalten wir eine Darstellung für 15, nämlich $15 = 93 - 2 \cdot 39$, die wir in Gleichung (3) einsetzen:

$$3 = -5 \cdot 15 + 2 \cdot 39 = -5 \cdot \underbrace{(93 - 2 \cdot 39)}_{15} + 2 \cdot 39 = -5 \cdot 93 + 12 \cdot 39 \tag{4}$$

Auf der rechten Seite der Gleichung $3 = -5 \cdot 93 + 12 \cdot 39$ steht nun die gesuchte Vielfachsummendarstellung von $3 = \mathrm{ggT}\,(93, 39)$ in Abhängigkeit von 93 und 39.

Probe: $-5 \cdot 93 + 12 \cdot 39 = -465 + 468 = 3$ ✓

Anwendung: Wird beim RSA-Verfahren ein Verschlüsselungsexponenten d bei gegegeben Werten $\varphi(n)$ und e bestimmt, so ergibt sich speziell

- eine Vielfachsummendarstellung von $1 = \mathrm{ggT}\,(e, \varphi(n))$ in der Form
$$1 = a \cdot e + b \cdot \varphi(n);$$
- Hieraus ergibt sich $a \cdot e = -b \cdot \varphi(n) + 1 \underset{\varphi(n)}{\equiv} 1$, wir setzten dann $d = a$.

(a) **Bestimmen Sie** $\mathrm{ggT}\,(1134, 770)$, d.h., den größten gemeinsamen Teiler der Zahlen 1134 und 770, mit dem euklidischen Algorithmus.

(b) **Verwenden Sie** die Erweiterung des euklidischen Algorithmus, um $\mathrm{ggT}\,(1134, 770)$ als Vielfachsumme von 1134 und 770 darzustellen. Überprüfen Sie Ihr Ergebnis.

(c) **Stellen Sie** $1 = \mathrm{ggT}\,(7, 240)$ als Vielfachsumme von 7 und 240 dar und ermitteln Sie hieraus den RSA-Entschlüsselungsexponenten d für den Fall $n = 385 = 5 \cdot 7 \cdot 11$ und $e = 7$.

Aufgabe P 17. *Für Schnelle sogleich, für alle anderen zuhause.*

(a) Das folgende Beispiel zeigt, dass das RSA-Verfahren auch dann funktioniert, wenn für e eine Zahl gewählt wird, die zwar **teilerfremd** zu $\varphi(n)$ aber **keine Primzahl** ist. Berechnen Sie $\varphi(47 \cdot 53)$. Stellen Sie $1 = \mathrm{ggT}\left(15, \varphi(47 \cdot 53)\right)$ als Vielfachsumme von 15 und $\varphi(47 \cdot 53)$ dar und ermitteln Sie hieraus den RSA-Entschlüsselungsexponenten d für den Fall $n = 47 \cdot 53$ und $e = 15$.

(b) Bestimmen Sie den größten gemeinsamen Teiler der Zahlen 2100 und 4935 mit dem euklidischen Algorithmus.

(c) Stellen Sie $\mathrm{ggT}\,(2100, 4935)$ als Vielfachsumme von 2100 und 4935 dar.

(d) In der Praxis wird als Verschlüsselungsexponent oft die Fermat-Zahl

$$F_4 = 2^{2^4} + 1 = 65537$$

verwendet. Bestimmen Sie den Entschlüsselungsexponenten d für den Fall $n = 479 \cdot 199$ und $e = F_4$. Zu lösen ist die Kongruenz

$$65537 \cdot d \underset{94644}{\equiv} 1$$

Ziel-Zeitmarke: 45 Minuten

Aufgabe P 18. *Faktorisierung von Restklassenringen zur Rechenvereinfachung*

Man kann die Berechnung hoher Potenzen $\mod n$ vereinfachen, wenn man die Faktorisierung von n in Primzahlpotenzen kennt.

Beispiel: $15 = 3 \cdot 5$. Wir berechnen $7^3 \mod 15$ wie folgt:

$$7 \mapsto \left(\left[7 \mod 3\right]_{\underset{3}{\equiv}}, \left[7 \mod 5\right]_{\underset{5}{\equiv}} \right) = \left(\left[1\right]_{\underset{3}{\equiv}}, \left[2\right]_{\underset{5}{\equiv}} \right)$$

$$7^3 \mapsto \left(\left[1^3\right]_{\underset{3}{\equiv}}, \left[2^3\right]_{\underset{5}{\equiv}} \right) = \left(\left[1\right]_{\underset{3}{\equiv}}, \left[8\right]_{\underset{5}{\equiv}} \right) = \left(\left[1\right]_{\underset{3}{\equiv}}, \left[3\right]_{\underset{5}{\equiv}} \right) =: (\bar{1}, \bar{3}).$$

Wir suchen nun die kleinste nichtnegative Zahl x kleiner 15, welche die sogenannte **simultane Kongruenz**

$$\begin{aligned} x \mod 3 &= 1 \\ x \mod 5 &= 3 \end{aligned}$$

erfüllt. Die Lösung[1] ist $x = 13$. Wir führen eine Probe durch: $7^3 = 343 = = 330 + 13 = 16 \cdot 15 + 13$.

Ohne Verwendung des Chinesischen Restsatzes könnte man eine Liste der Korrespondenzen betrachten:

$$\begin{aligned}
0 &\mapsto \left(\left[0\right]_{\underset{3}{\equiv}}, \left[0\right]_{\underset{5}{\equiv}} \right) \\
1 &\mapsto \left(\left[1\right]_{\underset{3}{\equiv}}, \left[1\right]_{\underset{5}{\equiv}} \right) \\
2 &\mapsto \left(\left[1+1\right]_{\underset{3}{\equiv}}, \left[1+1\right]_{\underset{5}{\equiv}} \right) = \left(\left[2\right]_{\underset{3}{\equiv}}, \left[2\right]_{\underset{5}{\equiv}} \right) \\
3 &\mapsto \left(\left[2+1\right]_{\underset{3}{\equiv}}, \left[2+1\right]_{\underset{5}{\equiv}} \right) = \left(\left[0\right]_{\underset{3}{\equiv}}, \left[3\right]_{\underset{5}{\equiv}} \right) \\
4 &\mapsto \left(\left[1\right]_{\underset{3}{\equiv}}, \left[4\right]_{\underset{5}{\equiv}} \right) \\
5 &\mapsto \left(\left[2\right]_{\underset{3}{\equiv}}, \left[0\right]_{\underset{5}{\equiv}} \right) \\
6 &\mapsto \left(\left[0\right]_{\underset{3}{\equiv}}, \left[1\right]_{\underset{5}{\equiv}} \right)
\end{aligned}$$

$$\begin{aligned}
7 &\mapsto \left(\left[1\right]_{\underset{3}{\equiv}}, \left[2\right]_{\underset{5}{\equiv}} \right) \\
8 &\mapsto \left(\left[2\right]_{\underset{3}{\equiv}}, \left[3\right]_{\underset{5}{\equiv}} \right) \\
9 &\mapsto \left(\left[0\right]_{\underset{3}{\equiv}}, \left[4\right]_{\underset{5}{\equiv}} \right) \\
10 &\mapsto \left(\left[1\right]_{\underset{3}{\equiv}}, \left[0\right]_{\underset{5}{\equiv}} \right) \\
11 &\mapsto \left(\left[2\right]_{\underset{3}{\equiv}}, \left[1\right]_{\underset{5}{\equiv}} \right) \\
12 &\mapsto \left(\left[0\right]_{\underset{3}{\equiv}}, \left[2\right]_{\underset{5}{\equiv}} \right) \\
13 &\mapsto \left(\left[1\right]_{\underset{3}{\equiv}}, \left[3\right]_{\underset{5}{\equiv}} \right) \\
14 &\mapsto \left(\left[2\right]_{\underset{3}{\equiv}}, \left[4\right]_{\underset{5}{\equiv}} \right)
\end{aligned}$$

[1] Mit der Formel aus dem Chinesischen Restsatz ergibt sich hier $x \underset{3\cdot 5}{\equiv} 3 - 2 \cdot 5 \cdot (3-1) = -17 \underset{15}{\equiv} 13$.

Versuchen Sie, auf analoge Weise die folgenden Potenzen zu berechnen:

(a) $14^7 \mod 187$ **(b)** $10^5 \mod 221$ **(c)** $108^{77} \mod 221$

Hinweise:

- $221 = 13 \cdot 17$, $77 = 64 + 8 + 4 + 1$, *d.h.* $108^{77} = 108^{64} \cdot 108^8 \cdot 108^4 \cdot 108^1$.
- *Der sogenannte* ***Chinesische Restsatz*** *liefert eine Formel zur Lösung simultaner Kongruenzen: Falls natürliche Zahlen m und n teilerfremd sind, so ergeben sich mit dem erweiterten euklidischen Algorithmus Zahlen y und z mit $1 = y\,m + z\,n$. Die Lösung des Systems*

$$x \underset{m}{\equiv} a, \quad x \underset{n}{\equiv} b$$

ist dann gegeben durch

$$x \underset{m \cdot n}{\equiv} b - z \cdot n \cdot (b - a).$$

Hausübungen

Aufgabe H 38. *Erweiterter euklidischer Algorithmus*

(a) Bestimmen Sie $\operatorname{ggT}(23205, 3773)$, d.h. den größten gemeinsamen Teiler der Zahlen 23205 und 3773 mit dem euklidischen Algorithmus.

(b) Verwenden Sie Erweiterung des euklidischen Algorithmus, um $\operatorname{ggT}(23205, 3773)$ als Vielfachsumme von 23205 und 3773 darzustellen. Überprüfen Sie Ihr Ergebnis.

Aufgabe H 39. *Systeme von Kongruenzen (simultane Kongruenzen)*

(a) Bestimmen Sie die kleinste Zahl $x \in \mathbb{N}$, für die Folgendes gilt:

$$x \underset{3}{\equiv} 2 \qquad \text{bzw.} \qquad x \mod 3 = 2,$$
$$x \underset{5}{\equiv} 3 \qquad \text{bzw.} \qquad x \mod 5 = 3.$$

Hinweis: Im Folgenden verwenden wir nur noch die Notation der Form $x \underset{n}{\equiv} a$. Sie können stattdessen jeweils $x \mod n = a$ denken oder schreiben.

(b) Bestimmen Sie die kleinste Zahl $x \in \mathbb{N}$, für die Folgendes gilt:

$$x \underset{3}{\equiv} 2, \qquad x \underset{5}{\equiv} 3, \qquad x \underset{7}{\equiv} 2.$$

(c) Ist das folgende System simultaner Kongruenzen lösbar?

$$x \underset{8}{\equiv} 5, \qquad x \underset{12}{\equiv} 3$$

(d) Ist das folgende System simultaner Kongruenzen lösbar?

$$x \underset{8}{\equiv} 5, \qquad x \underset{12}{\equiv} 9$$

(e) Bestimmen Sie die kleinste Zahl $x \in \mathbb{N}$, für die Folgendes gilt:

$$x \underset{2}{\equiv} 1, \qquad x \underset{3}{\equiv} 2, \qquad x \underset{4}{\equiv} 3,$$
$$x \underset{5}{\equiv} 4, \qquad x \underset{6}{\equiv} 5, \qquad x \underset{7}{\equiv} 6,$$
$$x \underset{8}{\equiv} 7, \qquad x \underset{9}{\equiv} 8, \qquad x \underset{10}{\equiv} 9.$$

Hinweis: Sie können dieses System zunächst vereinfachen. Zum Beispiel ist $x \underset{2}{\equiv} 1$ „automatisch“ erfüllt, wenn $x \underset{10}{\equiv} 9$ gilt.

*Hinweis: Der sogenannte **Chinesische Restsatz** liefert eine Formel zur Lösung simultaner Kongruenzen: Falls die natürliche Zahlen m und n den größten gemeinsamen Teiler $d := \operatorname{ggT}(m, n)$ besitzen, so ergeben sich mit dem erweiterten euklidischen Algorithmus Zahlen y und z mit $d = y\,m + z\,n$. Das System*

$$x \underset{m}{\equiv} a, \quad x \underset{n}{\equiv} b$$

ist genau dann lösbar, wenn $a \underset{d}{\equiv} b$ *gilt. In diesem Fall ist die Lösung gegeben durch*

$$x \underset{\frac{m\cdot n}{d}}{\equiv} b - z \cdot n \cdot \tfrac{b-a}{d}.$$

Aufgabe H 40. *Faktorisierung von Restklassenringen zur Rechenvereinfachung*

Berechnen Sie die folgenden Potenzen mit der Faktorisierung des Restklassenrings $\mathbb{Z}/221\mathbb{Z}$.

(a) $108^2 \mod 221$ **(b)** $108^2 \mod 221$ **(c)** $108^4 \mod 221$ **(d)** $108^8 \mod 221$
(e) $108^{16} \mod 221$ **(f)** $108^{32} \mod 221$ **(g)** $108^{64} \mod 221$ **(h)** $108^{77} \mod 221$.

Hinweise:

- *Wegen* $221 = 13 \cdot 15$ *müssen Sie wie folgt vorgehen:* $108 \mapsto \big(108 \mod 13,\ 108 \mod 17\big)$, $108^2 \mapsto \big((108 \mod 13)^2,\ (1088 \mod 17)^2\big)$, *etc. Nutzen Sie am Ende aus, dass* $77 = 64 + 8 + 4 + 1$, *und somit* $108^{77} = 108^{64} \cdot 108^8 \cdot 108^4 \cdot 108^1$ *gilt.*
- *Falls natürliche Zahlen* m *und* n *teilerfremd sind, so ergeben sich mit dem erweiterten euklidischen Algorithmus Zahlen* y *und* z *mit* $1 = y\,m + z\,n$. *Die Lösung des Systems* $x \underset{m}{\equiv} a, \quad x \underset{n}{\equiv} b$ *ist dann nach dem Chinesische Restsatzdann gegeben durch* $x \underset{m\cdot n}{\equiv} b - z \cdot n \cdot (b - a)$.

Aufgabe H 41. *RSA-Verfahren – Klausuraufgabe vom SoSe 2015*

(a) Bestimmen Sie $\varphi(12)$, also die Anzahl derjenigen natürlichen Zahlen a mit $1 \leq a \leq 12$, für die $\mathrm{ggT}\,(a, 12) = 1$ gilt.

Im Folgenden gelte stets $n = 11 \cdot 17$ und $\varphi(n) = 10 \cdot 16 = 160$ sowie $e = 7$.

(b) Verifizieren Sie, dass die Zahl $d = 23$ die Eigenschaft $7 \cdot d \underset{160}{\equiv} 1$ besitzt.

(c) Es sei gegeben die Klartextnachricht $m = 3$. Bestimmen Sie das Chiffrat $c = 3^7 \mod 187$. *Hinweise:* $3^7 = 3^{4+2+1} = 81 \cdot 9 \cdot 3$ *und* $81 \cdot 3 = 243 = 1 \cdot 187 + 56$.

(d) Welche Rechnung müsste der Empfänger des in der vorigen Teilaufgabe ermittelten Chiffrats c durchführen, um die Klartextnachricht m zu bestimmen.

Aufgabe H 42. *RSA-Verfahren – Klausuraufgabe vom SoSe 2016*

(a) Es ist $5 \cdot 7 = 35$ und $5 \cdot 7 \cdot 11 = 385$. Bestimmen Sie die folgenden Werte der eulerschen Phi-Funktion: $\varphi(5)$, $\varphi(35)$ und $\varphi(385)$.

(b) Verwenden Sie den erweiterten euklidischen Algorithmus (EEA), um eine Vielfachsummendarstellung von 1 in der Form $1 = a \cdot 240 + b \cdot 7$ zu finden. Anders ausgedrückt: Bestimmen Sie mit dem EEA **ganze** Zahlen a und b so, dass die Gleichung

$$1 \;=\; a \cdot 240 \;+\; b \cdot 7 \qquad \text{erfüllt ist.}$$

(c) Wir betrachten Schlüsselerzeugung beim RSA-Verfahren. Nehmen Sie an, dass für den öffentlichen Schüssel $(n, e) = (385, 7)$ gewählt wurde. Bestimmen Sie aus der Gleichung

$$103 \cdot 7 = 3 \cdot 240 + 1$$

den Entschlüsselungsexponenten d (als Teil des privaten Schlüssels (n, d)).

(d) Verschlüsseln Sie die Nachricht $m = 10$ mit dem RSA-Verfahren unter Verwendung des öffentlichen Schüssels $(n, e) = (385, 7)$. Berechnen Sie hierzu (ggf. mit dem Verfahren sukzessiven Quadrierens) den Wert des Ausdrucks $10^7 \mod 385$.

Aufgabe H 43. *RSA-Verfahren mit kleinem RSA-Modul*

Bob möchte Alice eine Nachricht verschlüsselt schicken. Dazu schlägt er Alices öffentlicher Schlüssel nach: $P = (n, e) = (221, 5)$.

(a) Berechnen Sie das Chiffrat $c = m^e \mod n$ für die Nachricht $m = 10$.

(b) Bestimmen Sie den geheimen Schlüssel d von Alice.

(c) Alice benutzt ihren geheimen Schlüssel d, um das Chiffrat c zu entschlüsseln: $m = c^d \mod n$.

Aufgabe H 44. *RSA-Algorithmus mit größerem RSA-Modul*

Sie benutzen die Primzahlen $p = 113$ und $q = 71$, um das RSA-Verfahren durchzuführen. Dazu wählen Sie den öffentlichen Schlüssel $e = 79$.

(a) Berechnen Sie Ihren geheimen Schlüssel d sowie den RSA-Modul n.

(b) Jemand schickt Ihnen die verschlüsselte Nachricht $c = 2973$. Entschlüsseln Sie die Nachricht.

Aufgabe H 45. *Zur Sicherheit des RSA-Verfahrens*

Seien $n_1 = 187$, $n_2 = 493$, $n_3 = 1189$. Drei Empfänger mit den öffentlichen Schlüsseln $(n_j, 3)$ erhalten die gleiche Nachricht m (eine Zahl) verschlüsselt als $c_1 = 168$, $c_2 = 236$, $c_3 = 729$. Versuchen Sie ohne sture Primzahlzerlegung (d.h. ohne dass Sie die kleinen Zahlen n_j von vornherein in Primzahlen zerlegen) herauszubekommen, was die Zahl m ist.

Hinweis: Testen Sie ob $\mathrm{ggT}(n_i, n_j) = 1$ *für alle* $i, j = 1, 2, 3$, $i \neq j$. *Ist dies nicht der Fall, so bekommen Sie für zwei der* n_j *die Primfaktorzerlegung, und damit können Sie den geheimen Schlüssel bestimmen.*

Aufgabe H 46. *Für Ambitionierte*

Versuchen Sie, die folgende Aussage zu beweisen: Wenn p, q und r drei (paarweise) voneinander verschiedene Primzahlen sind, so gilt $\varphi(p \cdot q \cdot r) = (p-1) \cdot (q-1) \cdot (r-1)$. Verfahren Sie hierbei analog zu dem in der Vorlesung geführten Beweis der Formel $\varphi(p \cdot q) = (p-1) \cdot (q-1)$.

Aufgabe H 47. *Modulare Arithmetik – Wochentagsproblem*

Welcher Wochentag war der 15.5.1955?

Hinweis: Der 1.1.1900 war ein Montag. Schaltjahre sind die Jahre, deren Jahreszahl durch 4 teilbar sind, mit Ausnahme der Jahre, deren Jahreszahlen durch 100, aber nicht durch 400 teilbar sind.

Tutoriumsübungen

Aufgabe T 28. *Erweiterter euklidischer Algorithmus*

(a) Bestimmen Sie den größten gemeinsamen Teiler der Zahlen 72 und 108 mit dem euklidischen Algorithmus.

(b) Stellen Sie $\mathrm{ggT}\,(72, 108)$ als Vielfachsumme von 72 und 108 dar.

(c) Stellen Sie $1 = \mathrm{ggT}\,(17, 72)$ als Vielfachsumme von 17 und 72 dar und ermitteln Sie hieraus den RSA-Entschlüsselungsexponenten d für den Fall $n = 7 \cdot 13$ und $e = 17$.

Erinnerung: Sie müssen d so bestimmen, dass $d \cdot 17 \underset{72}{\equiv} 1$ gilt.

Aufgabe T 29. *Faktorisierung von Restklassenringen zur Rechenvereinfachung*

Berechnen Sie die folgenden Potenzen mit der Faktorisierung des Restklassenrings $\mathbb{Z}/15\mathbb{Z}$.

(a) $8^2 \mod 15$

(b) $8^4 \mod 15$

(c) $8^7 \mod 15$

Hinweis:

- *Betrachten Sie das der Zahl 8 zugeordnete Paar $\left(\left[8 \mod 3\right]_{\underset{3}{\equiv}}, \left[8 \mod 5\right]_{\underset{5}{\equiv}} \right)$ im Ring $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.*
- *Bestimmen Sie $8^2 \mapsto \left(\left[(5 \mod 3)^2\right]_{\underset{3}{\equiv}}, \left[(8 \mod 5)^2\right]_{\underset{5}{\equiv}} \right)$, etc. Nutzen Sie für die dritte Teilaufgabe aus, dass $8^7 = 8^1 \cdot 8^2 \cdot 8^4$ gilt.*
- *Wenn Sie ein Paar $(a, b) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ berechnet haben, müssen Sie hieraus das zugehörige Element $x \in \mathbb{Z}/15\mathbb{Z}$ bestimmmen. Hierzu müssen sie sogenannte **simultane Kongruenz***

$$x \underset{3}{\equiv} a, \quad x \underset{5}{\equiv} b$$

lösen, was im vorliegenden Beispiel sehr einfach ist.

(d) Berechnen Sie $10^5 \mod 221$ mit der Faktorisierung des Restklassenrings $\mathbb{Z}/221\mathbb{Z}$.
Hinweis: $221 = 13 \cdot 17$, $5 = 4 + 1$, *d.h.* $10^5 = 10^4 \cdot 10^1$.

Wenn Sie ein Paar $(a, b) \in \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$ berechnet haben, müssen Sie hieraus das zugehörige Element $x \in \mathbb{Z}/221\mathbb{Z}$ bestimmmen. Hierbei hilft Ihnen der **Chinesische Restsatz**, den wir hier in der folgenden Formulierung verwenden:

Falls natürliche Zahlen m und n teilerfremd sind, so ergeben sich mit dem erweiterten euklidischen Algorithmus Zahlen y und z mit $1 = y\,m + z\,n$. Die Lösung eines Systems

$$x \underset{m}{\equiv} a, \quad x \underset{n}{\equiv} b$$

ist dann gegeben durch

$$x \underset{m\cdot n}{\equiv} b - z \cdot n \cdot (b - a).$$

Aufgabe T 30. *Modulare Arithmetik und RSA-Verfahren – in Anlehnung an eine Klausuraufgabe*

(a) Zur Bestimmung von $\varphi(20)$ schreiben Sie alle Zahlen x auf, welche die beiden Bedingungen $1 \leq x \leq 20$ und ggT$(x, 20) = 1$ erfüllen.

(b) Es ist $11 \cdot 17 = 187$ und $5 \cdot 7 \cdot 11 = 385$. **Bestimmen Sie** die folgenden Werte der eulerschen Phi-Funktion: $\varphi(11)$, $\varphi(187)$ und $\varphi(385)$.

(c) **Bestimmen Sie** $19 \cdot 19 \mod 20$ sowie $15 \cdot 15 \mod 20$. Gibt es eine ganze Zahl x mit der Eigenschaft, dass $x \cdot 15 \mod 20 = 1$ gilt?

(d) **Verwenden Sie** den erweiterten euklidischen Algorithmus (EEA), um eine Vielfachsummendarstellung von 1 in der Form $1 = a \cdot 160 + b \cdot 7$ zu finden. Anders ausgedrückt: **Bestimmen Sie** mit dem EEA **ganze** Zahlen a und b so, dass die Gleichung

$$1 = a \cdot 160 + b \cdot 7 \qquad \text{erfüllt ist.}$$

(e) Wir betrachten Schlüsselerzeugung beim RSA-Verfahren. Nehmen Sie an, dass für den öffentlichen Schüssel $(n, e) = (187, 7)$ gewählt wurde. Bestimmen Sie aus der Gleichung

$$183 \cdot 7 = 8 \cdot 160 + 1$$

den Entschlüsselungsexponenten d (als Teil des privaten Schlüssels (n, d)).

(f) Betrachten Sie das der Zahl 15 zugeordnete Paar $\left([15 \mod 11]_{\underset{11}{\equiv}}, [15 \mod 17]_{\underset{17}{\equiv}} \right)$ im Ring $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. Berechnen Sie

$$\left([15 \mod 11]_{\underset{11}{\equiv}}, [15 \mod 17]_{\underset{17}{\equiv}} \right)^2,$$

und

$$\left([15 \mod 11]_{\underset{11}{\equiv}}, [15 \mod 17]_{\underset{17}{\equiv}} \right)^4,$$

sowie

$$(15 \mod 11,\ 15 \mod 17) \cdot (15 \mod 11,\ 15 \mod 17)^2 \cdot (15 \mod 11,\ 15 \mod 17)^4$$

in diesem Ring.

(g) Verschlüsseln Sie die Nachricht $m = 15$ mit dem RSA-Verfahren unter Verwendung des öffentlichen Schüssels $(n, e) = (187, 7)$. Berechnen Sie hierzu (ggf. mit dem Verfahren sukzessiven Quadrierens) den Wert des Ausdrucks $15^7 \mod 187$. Am Ende mag Ihnen der Chinesische Restsatz von Nutzen sein.