Präsenzübungen

Aufgabe P 1. *Modulare Arithmetik*

Wir betrachten ganzzahlige Division durch 13.

(a) Bestimmen Sie $42 \mod 13$ sowie $18 \mod 13$. Wählen Sie hierzu jeweils die Darstellung

$$x = a \cdot 13 + r \quad \text{mit} \quad 0 \leq r < 13.$$

(b) Listen Sie einige negative und positive Elemente der Restklassen $[42]_{\underset{13}{\equiv}}$ und $[18]_{\underset{13}{\equiv}}$ auf, darunter jeweils das Element, das im Bereich von 0 bis 12 liegt.

Zur Notation: Wenn zwei ganz Zahlen x und y **in der gleichen Restklasse** bgzl. ganzzahliger Division durch 13 sind wie die Zahl 7 so lässt sich dies wie folgt notieren:

$$x \underset{13}{\equiv} y \quad \text{bzw.} \quad [x]_{\underset{13}{\equiv}} = [y]_{\underset{13}{\equiv}} \quad \text{bzw.}$$

$$x \mod 13 = y \mod 13,$$

denn es gilt nach Voraussetzung ja $x \mod 13 = 7$ und $y \mod 13 = 7$. Eine weitere Variante, die wir nicht verwenden, die Sie jedoch in der Literatur finden, liest sich wie folgt:

$$x \equiv y \mod 13.$$

Dies ist eine alternative Schreibweise für die Aussage $x \underset{13}{\equiv} y$, gelesen: „$x$ kongruent y modulo 13."

In der Vorlesung haben wir für festen Modulus n die Verknüpfung von Restklassen definiert:

$$[x]_{\underset{n}{\equiv}} \cdot [y]_{\underset{n}{\equiv}} := [x \cdot y]_{\underset{n}{\equiv}} \qquad \text{und} \qquad [x]_{\underset{n}{\equiv}} + [y]_{\underset{n}{\equiv}} := [x + y]_{\underset{n}{\equiv}}$$

Wenn Sie diesen Definitionen folgend z.B. $[42]_{\underset{13}{\equiv}} + [18]_{\underset{13}{\equiv}}$ und $[42]_{\underset{13}{\equiv}} \cdot [18]_{\underset{13}{\equiv}}$ ausrechnen wollen, so müssen Sie $[42 + 18]_{\underset{13}{\equiv}} = [60]_{\underset{13}{\equiv}}$ bzw. $[42 \cdot 18]_{\underset{13}{\equiv}}$ bestimmen.

Bei der Summe macht dies keinerlei Schwierigkeiten: $60 = 4 \cdot 13 + 8$, also können wir schreiben

$$[42]_{\underset{13}{\equiv}} + [18]_{\underset{13}{\equiv}} = [60]_{\underset{13}{\equiv}} = [8]_{\underset{13}{\equiv}} \quad \text{oder auch} \quad (42 + 18) \mod 13 = 8 \quad \text{oder auch} \quad 42 + 18 \underset{13}{\equiv} 8.$$

Auch das Produkt $42 \cdot 18$ lässt sich natürlich ausrechnen und dann „modulo 13 ausreduzieren".[1]

Einfacher ist es jedoch, wenn man sich klarmacht, dass

$$18 \mod 13 = 5 \quad \text{bzw.} \quad 18 \underset{13}{\equiv} 5 \quad \text{bzw.} \quad [18]_{\underset{13}{\equiv}} = [5]_{\underset{13}{\equiv}} \quad \text{und}$$

$$42 \mod 13 = 3 \quad \text{bzw.} \quad 42 \underset{13}{\equiv} 3 \quad \text{bzw.} \quad [42]_{\underset{13}{\equiv}} = [3]_{\underset{13}{\equiv}}$$

gilt und wie folgt rechnet: $[42]_{\underset{13}{\equiv}} \cdot [18]_{\underset{13}{\equiv}} = [3]_{\underset{13}{\equiv}} \cdot [5]_{\underset{13}{\equiv}} = [3 \cdot 5]_{\underset{13}{\equiv}}$ bzw. $42 \cdot 18 \underset{13}{\equiv} 3 \cdot 5 \underset{13}{\equiv} 2$.

[1] Diese Sprechweise bedeutet nichts anderes als dass man den (nichtnegativen) Rest bestimmt, der sich bei ganzzahliger Division von $42 \cdot 18$ durch 13 ergibt.

(c) Die Zahl 16 liegt in der Restklasse $[3]_{\underset{13}{\equiv}}$, die Zahl 18 liegt in der Restklasse $[5]_{\underset{13}{\equiv}}$. Berechnen Sie $16 \cdot 18$ und überzeugen Sie sich davon, dass $(16 \cdot 18) \mod 13 = 2$ gilt.

(d) Verfizieren Sie, dass $225 \underset{13}{\equiv} 4$ sowie $225 \underset{13}{\equiv} 264$ gilt.

(e) Bestimmen Sie $(42 \cdot 18)^2 \mod 13$.

Aufgabe P 2. *Eulersche φ-Funktion*

(a) Ermitteln Sie die Menge $E(30)$ derjenigen ganzen Zahlen x im Bereich $\{1, 2, 3, \ldots, 29, 30\}$, die zu 30 teilerfremd sind (für die also $\text{ggT}(x, 30) = 1$ gilt), sowie deren Elementeanzahl $|E(30)|$ „von Hand".

(b) Lesen Sie den folgenden, in der Vorlesung behandelten **Satz:**

Wenn p, q und r drei (paarweise) voneinander verschiedene Primzahlen sind, so gilt

$$\varphi(p \cdot q) = (p-1) \cdot (q-1)$$
$$\varphi(p \cdot q \cdot r) = (p-1) \cdot (q-1) \cdot (r-1).$$

(c) Verwenden Sie die jeweils einschlägige Formel zur Berechnung der folgende Werte:

$$\text{(i) } \varphi(30) \qquad \text{(ii) } \varphi(91) \qquad \text{(iii) } \varphi(1001)$$

Aufgabe P 3. *Schnelles Berechnen hoher Potenzen – Sukzessives Quadrieren*

Bei der Durchführung des sogenannten RSA-Algorithmus müssen für große Zahlen, die als Potenzen vorliegen, die Reste bei ganzzahliger Division durch eine feste Zahl n berechnet werden. Hierfür erweist sich die folgende Methode („Sukzessives Quadrieren") als zweckmäßig:

Zunächst wird der Exponent als Summe von Zweierpotenzen geschrieben, wie im folgenden Demonstrationsbeispiel (mit kleinen Exponenten): $100^7 = 100^{1+2+4} = 100 \cdot 100^2 \cdot 100^4$.

Möchte man etwa $100^7 \mod 13$ bestimmen, so wird zunächst der Wert $100 \mod 13$ ermittelt, danach wird sukzessive quadriert und jeweils „modulo 13 ausreduziert".

$$100 \underset{13}{\equiv} 9, \quad \text{denn } 100 = 7 \cdot 13 + 9.$$
$$100^2 \underset{13}{\equiv} 9^2 = 81 \underset{13}{\equiv} 3, \quad \text{denn } 81 = 6 \cdot 13 + 3.$$
$$100^4 \underset{13}{\equiv} 3^2 \underset{13}{\equiv} 9.$$

Kombination dieser Zwischenergebnisse liefert $100^7 \underset{13}{\equiv} 9 \cdot 3 \cdot 9 = 27 \cdot 9 \underset{13}{\equiv} 1 \cdot 9 \underset{13}{\equiv} 9$.

(a) **Berechnen Sie** $87^{27} \mod 103$.
Hinweis: Sie können z.B. ausnutzen, dass $87 \underset{103}{\equiv} -16$ *ist.*

Für Schnelle sogleich, für alle anderen zuhause:

(b) Berechnen Sie $87^{43} \mod 103$.

(c) Vollenden bzw. wiederholen Sie die Rechnung, die in der Vorlesung zur Demonstration der RSA-Entschlüsselung diente: $m' = 108^{77} \mod 221$.

Hausübungen

Aufgabe H 1. *RSA-Algorithmus*

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 2. *RSA-Algorithmus*

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 3. *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 $ggT(n_i, n_j) = 1$ 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 4. *Beweisführung 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 5. *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 1. *Modulare Arithmetik*

Bestimmen Sie für die folgenden negativen Zahlen jeweils die kleinste positive Zahl, die in derselben Restklasse steckt.

(a) $-7 \underset{2}{\equiv}$

(b) $-3 \underset{12}{\equiv}$

(c) $-5 \underset{23}{\equiv}$

(d) $-25 \underset{23}{\equiv}$

(e) $-75 \underset{23}{\equiv}$

Aufgabe T 2. *Modulare Arithmetik*

Bestimmen Sie die Reste $\mod n$. Beachten Sie hierbei, dass wir im Gegensatz zu mancher Programmiersprache als Ergebnis der Operation $\mod$ stets die **kleinsten nichtnegativen Vertreter** einer Restklasse auswählen.

(a) $3 \mod 5$

(b) $-3 \mod 5$?

(c) $40 \mod 11$?

(d) $-40 \mod 11$?

Aufgabe T 3. *Modulare Arithmetik*

(a) Bestimmen Sie die Prüfziffer der folgenden ISBN: $3-528-57259-?$ Multiplizieren Sie hierzu die vorderste Ziffer mit 1, die nächste Ziffer mit 2 die dritte mit 3 usw. Bilden Sie die Summe der zehn Terme und dividieren Sie diese mit Rest durch 11. Die Prüfziffer ist gleich diesem Rest, hat dieser den Wert 10, so verwendet man das Symbol X.

(b) Ist die Zahlenfolge $3-528-47259-6$ eine gültige ISBN-Nummer? Um welches Buch handelt es sich?

Aufgabe T 4. *RSA-Verfahren*

Sie benutzen die Primzahlen $p = 13$ und $q = 7$, um das RSA-Verfahren durchzuführen. Dazu wählen Sie den öffentlichen Schlüssel $e = 7$.

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

(b) Jemand schickt Ihnen die verschlüsselte Nachricht $c = 37$. Entschlüsseln Sie die Nachricht.

Aufgabe T 5. *RSA-Sicherheit*

Sind p und q voneinander verschiedene Primzahlen und ist $n = p \cdot q$, so kann man aus der Kenntnis von n und $\varphi(n) = (p-1)(q-1)$ die beiden Primzahlen p und q berechnen.

Bestimmen Sie p, q für $n = 1207$ und $\varphi(n) = 1120$.