Aufgabe 6.1 (2 Pkt.)

Berechnen Sie das Inverse von 51 modulo 293 mit dem erweiterten Euklidischen Algorithmus. Geben Sie die Tabelle mit allen Zwischenergebnissen an!

Aufgabe 6.2 (1+1 Pkt.)

Zeigen Sie:

a) Für jedes $m \in \mathbb{N}$ gibt es nur endlich viele $n \in \mathbb{N}$ mit $\varphi(n) = m$.
Hinweis: Zeigen Sie zunächst, dass der größte Primteiler einer Zahl n mit $\varphi(n) = m$ kleiner gleich $m + 1$ ist.

b) Für jedes $m \in \mathbb{N}$ gibt es unendlich viele n mit $m \mid \varphi(n)$.

Aufgabe 6.3 (2+1 Pkt.)

Eine Variante des Euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier Zahlen $a, b \in \mathbb{N} \cup \{0\}$ ist der sogenannte binäre Euklidische Algorithmus. Wir betrachten folgende rekursive Formulierung dieses Algorithmus:

$$\mathrm{ggT}(a,b) = \begin{cases} a & \text{falls } b = 0 \\ b & \text{sonst, falls } a = 0 \\ 2\,\mathrm{ggT}\left(\frac{a}{2}, \frac{b}{2}\right) & \text{sonst, falls } a \text{ und } b \text{ gerade} \\ \mathrm{ggT}\left(a, \frac{b}{2}\right) & \text{sonst, falls } a \text{ ungerade und } b \text{ gerade} \\ \mathrm{ggT}\left(\frac{a}{2}, b\right) & \text{sonst, falls } a \text{ gerade und } b \text{ ungerade} \\ \mathrm{ggT}\left(a, \frac{b-a}{2}\right) & \text{sonst, falls } a \leq b \\ \mathrm{ggT}\left(b, \frac{a-b}{2}\right) & \text{sonst} \end{cases}$$

a) Zeigen Sie, dass der Algorithmus den größten gemeinsamen Teiler von a und b berechnet (bzw. 0 als Ergebnis liefert, falls $a = b = 0$).

b) Zeigen Sie, dass $\mathrm{ggT}(a, b)$ mit Bitkomplexität $\mathcal{O}(n^2)$ berechnet werden kann, wenn a und b n-Bit-Zahlen sind.

Hinweis: Beweisen Sie zuerst, dass obiger Algorithmus $\mathcal{O}(\log(ab))$ rekursive Aufrufe benötigt.

Aufgabe 6.4 (1+1 Pkt.)

Beweisen Sie folgende Eigenschaften der Eulerschen φ-Funktion:

a) Für jede Primzahl p gilt

$$\sum_{d \in \mathbb{N},\ d \mid p^k} \varphi(d) = p^k\,.$$

b) Für alle $n \in \mathbb{N}$ gilt

$$\sum_{d \in \mathbb{N},\ d \mid n} \varphi(d) = n\,.$$

Aufgabe 6.5 (3 Pkt.)

Wir betrachten die rekursive Formulierung des Euklidschen Algorithmus aus der Vorlesung mit Eingaben (a, b), wobei wir $a > b \geq 0$ voraussetzen. Sei H_k die Menge der Eingaben, die k rekursive Aufrufe verursacht – anders formuliert:

$$H_k \coloneqq \big\{(a, b) \;\big|\; \text{Euklid}(a, b) \text{ benötigt } k \text{ Modulo-Rechnungen}\big\} \; .$$

Es seien $F_0 \coloneqq 0$, $F_1 \coloneqq 1$, $F_{k+2} \coloneqq F_k + F_{k+1}$ die Fibonacci-Zahlen. Beweisen Sie: Für $k \geq 1$ ist (F_{k+2}, F_{k+1}) die kleinste Eingabe aus H_k, genauer:

- $(F_{k+2}, F_{k+1}) \in H_k$,
- $F_{k+2} = \min\{a \in \mathbb{N} \mid \exists\, b < a \colon (a, b) \in H_k\}$ und
- $F_{k+1} = \min\{b \in \mathbb{N} \mid \exists\, a > b \colon (a, b) \in H_k\}$.

Aufgabe 6.6 (4 Pkt.)

Lösen Sie die SPOX-Aufgabe „Fibonacci-Zahlen über Restklassenringen“.