Übung zu Modul: Innermathematische Beziehungen
Zahlentheorie

Fabian Grünig
gruenig@ph-heidelberg.de

Sommersemester 2017
Mittwoch, 12:00 Uhr, A233

Aufgabe 38 *(Die Eulersche φ-Funktion)*
Wir bezeichnen mit φ die Eulersche Phi-Funktion, die einer natürlichen Zahl die Anzahl der zu dieser Zahl kleineren, teilerfremden natürlichen Zahlen zuordnet.

(i) Berechne $\varphi(1), \varphi(2), \varphi(3), \varphi(5)$ und $\varphi(7)$.

(ii) Berechne $\varphi(6), \varphi(10), \varphi(15)$ und $\varphi(21)$.

(iii) Es seien p, q verschiedene Primzahlen. Bestimme $\varphi(p^2), \varphi(p^3), \varphi(p \cdot q)$ und $\varphi(p^2 \cdot q^2)$.

(iv) Es seien $p_1, p_2, \ldots, p_k$ paarweise verschieden Primzahlen. Bestimme $\varphi(p_1 \cdot p_2 \cdot \cdots \cdot p_k)$.

(v) Es seien $p_1, p_2, \ldots, p_k$ paarweise verschieden Primzahlen und $n_1, n_2, \ldots, n_k$ natürliche Zahlen. Bestimme $\varphi(p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_k^{n_k})$.

Aufgabe 39 *(Satz von Euler, Kleiner Satz von Fermat)*

(i) Berechne $(6^{25} \mod 11)$, $(3^{82} \mod 17)$ und $(6^{100003} \mod 101)$ mit Hilfe des kleinen Satzes von Fermat.

(ii) Bestimme die letzte Dezimalstelle (Einer-Stelle) von 7^{222} mit Hilfe des Satzes von Euler.

(iii) Zeige, dass 17 ein Teiler von $11^{104} + 1$ ist.

(iv) Bestimme die letzten beiden Ziffern der Dezimaldarstellung von 3^{256}.

(v) Drücke das multiplikative Inverse von $[15]_{103}$ in $\mathbb{Z}_{103}$ als eine Potenz von $[15]_{103}$ aus.
(Tipp: 103 ist eine Primzahl.)

Aufgabe 40 *(Systeme von Kongruenzgleichungen, Chinesischer Restsatz)*
Eine Bande von 17 Räubern stahl einen Sack mit Goldstücken. Als sie ihre Beute in gleiche Teile teilen wollten, blieben 3 Stücke übrig. Beim Streit darüber, wer ein Goldstück mehr erhalten sollte, wurde ein Räuber erschlagen. Jetzt blieben bei der erneuten Verteilung auf 16 Räuber 10 Goldstücke übrig. Der aufkommende Streit kostete wieder einem Rüuber das Leben. Jetzt ließ sich die Beute gleichmäßig auf die übrigen 15 Räuber verteilen. Wie viele Goldstücke waren mindestens im Sack? Wie viele Goldstücke können es allgemein gewesen sein?

Betrachte das folgende System von Kongruenzgleichungen.

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ x &\equiv a_3 \mod m_3 \end{aligned}$$

Wie musst du die Koeffizienten wählen, dass dieses System zu der obigen Geschichte passt, wenn man in x die mögliche Anzahl der Goldstücke bestimmen möchte?

Zur Lösung obigen Systems folgen wir Kapitel 6, Seite 34 im Skript.

(i) Prüfe zunächst, dass m_1, m_2, m_3 paarweise teilerfremd sind.

(ii) Berechne (der Notation aus dem Skript folgend) $m := m_1 \cdot m_2 \cdot m_3$ sowie $k_1 := \frac{m}{m_1}$, $k_2 := \frac{m}{m_2}$ und $k_3 := \frac{m}{m_3}$.

(iii) Verifiziere, dass nun tatsächlich $\mathrm{ggT}(k_i, m_i) = 1$ für $i = 1,2,3$ gilt. Warum muss dies unter den Bedingungen des Chinesischen Restsatzes immer gelten?

(iv) Obige Aussage liefert, dass $[k_i]_{m_i}$ als Element in $\mathbb{Z}_{m_i}$ invertierbar ist. Finde für $i = 1,2,3$ jeweils $[x_i]_{m_i}$ in $\mathbb{Z}_{m_i}$, sodass $[k_i]_{m_i} \cdot [x_i]_{m_i} = [1]_{m_i}$.

(v) Berechne $x := a_1 x_1 k_1 + a_2 x_2 k_2 + a_3 x_3 k_3$.

(vi) Verifiziere, dass $(k_j \equiv 0 \mod m_i)$ für $i \neq j$ sowie $(x \equiv a_i \mod m_i)$. Wir finden in x also eine spezielle Lösung des Gleichungssystems.

(vii) Vollziehe die folgenden Schlüsse nach: Sei y eine weitere Lösung des Gleichungssystems, dann gilt wegen $(y \equiv a_i \mod m_i)$ auch $(y \equiv x \mod m_i)$. Demnach also $m_i \mid (x - y)$.

(viii) Zeige: $x \equiv y \mod m$.

(ix) Zeige: Für beliebiges $k \in \mathbb{Z}$ ist $x + k \cdot m$ auch eine Lösung des obigen Systems.

Damit erhalten wir die allgemeinen Lösungen des Systems $\{x + k \cdot m \mid k \in \mathbb{Z}\}$. Der Algorithmus zur Lösung dieser Kongruenzgleichungen, besteht aus den Schritten (i), (ii), (iv) und (v), sowie der Angabe der allgemeinen Lösungen.