Mathematisches Institut
Georg-August-Universität Göttingen
Prof. Dr. E. Viada, Dr. V. Cantoral

Lösungen zu Übungsblatt 11.

Aufgabe 1 (10 Punkte)**.** Berechnen Sie jeweils die kleinste natürliche Zahl n mit

(i) $\bar{4}^7 = \bar{n}$ in $\mathbb{Z}/13\mathbb{Z}$. (*Hinweis:* Schreiben Sie $7 = 2^2 + 2 + 1$ und berechnen Sie 4^2, $(4^2)^2$ modulo 13.)

(ii) $\bar{6}^{21} = \bar{n}$ in $\mathbb{Z}/39\mathbb{Z}$

Lösung zu Aufgabe 1. Lösung zu (i). (5 Punkte) Es gilt

$$\bar{4}^7 = \bar{4}^{2^2+2+1} = \bar{4}^{2^2} \cdot \bar{4}^2 \cdot \bar{4}$$

wobei in $\mathbb{Z}/13\mathbb{Z}$ gilt, dass

$$\bar{4}^2 = \bar{16} = \bar{3}$$
$$\bar{4}^{2^2} = (\bar{4}^2)^2 = \bar{3}^2 = \bar{9}.$$

Somit ist

$$\bar{4}^7 = \bar{9} \cdot \bar{3} \cdot \bar{4} = \overline{27} \cdot \bar{4} = \bar{1} \cdot \bar{4} = \bar{4}$$

und die gesuchte Lösung ist demnach $n = 4$.

Lösung zu (ii). (5 Punkte) Hier ist $21 = 16 + 4 + 1 = 2^4 + 2^2 + 1$. In $\mathbb{Z}/39\mathbb{Z}$ gilt

$$\bar{6}^2 = \overline{36} = \overline{-3}$$
$$\bar{6}^4 = (\bar{6}^2)^2 = \overline{-3}^2 = \bar{9}$$
$$\bar{6}^8 = (\bar{6}^4)^2 = \bar{9}^2 = \overline{81} = \bar{3}$$
$$\bar{6}^{16} = (\bar{6}^8)^2 = \bar{3}^2 = \bar{9}.$$

Wir berechnen daher:

$$\begin{aligned}\bar{6}^{21} &= \bar{6}^{16+4+1} = \bar{6}^{16} \cdot \bar{6}^4 \cdot \bar{6} \\ &= \bar{9} \cdot \bar{9} \cdot \bar{6} = \overline{81} \cdot \bar{6} = \bar{3} \cdot \bar{6} = \overline{18}\end{aligned}$$

und die gesuchte Lösung ist daher $n = 18$.

Aufgabe 2 (10 Punkte)**.** Berechnen Sie jeweils das multiplikative Inverse des gegebenen Elements $\bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$. Geben Sie hierbei das Inverse als Element aus $\{\bar{0}, \ldots, \overline{p-1}\}$ an.

(i) Von $\bar{2}$ in $\mathbb{Z}/43\mathbb{Z}$,

(ii) Von $\bar{5}$ in $\mathbb{Z}/23\mathbb{Z}$,

(iii) Von $\overline{12}$ in $\mathbb{Z}/17\mathbb{Z}$.

Lösung zu Aufgabe 2. Lösung zu (i). (2 Punkte) Wir suchen $\bar{b} \in \mathbb{Z}/43\mathbb{Z}$ mit $\bar{2} \cdot \bar{b} = \bar{1}$. Man sieht schnell, dass $\bar{2} \cdot \overline{22} = \overline{44} = \bar{1}$, und damit $\overline{22}$ das inverse Element zu $\bar{2}$ in $\mathbb{Z}/43\mathbb{Z}$.

Lösung zu (ii). (4 Punkte) Hier sehen wir die Lösung nicht direkt. Wir können sie aber mithilfe des euklidischen Algorithmus und Rückeinsetzen finden. Wir berechnen hierfür $\mathrm{ggT}(23, 5)$:

$$\begin{aligned}23 &= 4 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0\end{aligned}$$

Beginnend in der vorletzten Zeile lesen wir daher ab:

$$\begin{aligned}1 &= 3 - 1 \cdot 2 \\ &= 3 = (5 - 1 \cdot 3) = 3 - 5 + 1 \cdot 3 = 2 \cdot 3 - 5 \\ &= 2 \cdot (23 - 4 \cdot 5) - 5 = 2 \cdot 23 - 8 \cdot 5 - 5 = 2 \cdot 23 - 9 \cdot 5.\end{aligned}$$

Damit ist also $1 = 2 \cdot 23 - 9 \cdot 5$ und daher dann auch $-9 \cdot 5 \equiv 1 \mod 23$ bzw. in $\mathbb{Z}/23\mathbb{Z}$ ist $\overline{-9} \cdot \bar{5} = \bar{1}$ und daher $\overline{-9} = \overline{14}$ das Inverse zu $\bar{5}$ in $\mathbb{Z}/23\mathbb{Z}$.

Lösung zu (iii). (4 Punkte) Wir gehen wie in (ii) und finden dass 10 das Inverse zu 12 in $\mathbb{Z}/17\mathbb{Z}$ ist.

Aufgabe 3 (10 Punkte)**.** Zeigen Sie:

(i) $2^{1149} - 6$ ist durch 11 teilbar

(ii) $5^{6350} \equiv 4 \mod 7$

Lösung zu Aufgabe 3. Lösung zu (i). (5 Punkte) Es gilt nach dem kleinen fermatschen Satz, dass $a^{p-1} \equiv 1 \mod p$ für alle Primzahlen p. Da 11 eine Primzahl ist, ist also $2^{10} \equiv 1 \mod 11$. Damit folgt:

$$2^{1149} = 2^{1140+9} = 2^{10 \cdot 114} \cdot 2^9 = (2^{10})^{114} \cdot 2^9 = (1)^{114} \cdot 2^9 = 2^9 \mod 11$$

Wir können nun $2^9 \mod 11$ per Hand berechnen oder sehen, dass $2 \cdot 2^9 = 1 \mod 11$, also das multiplikative Inverse zu $\bar{2}$ in $\mathbb{Z}/11\mathbb{Z}$ ist. Da $2 \cdot 6 = 12 \equiv 1 \mod 11$, ist dies gegeben durch $\bar{6}$, sodass $2^{1149} \equiv 2^9 \equiv 6 \mod 11$ gelten muss. Insbesondere ist also

$$2^{1149} - 6 \equiv 0 \mod 11,$$

sprich $2^{1149} - 6$ ist durch 11 teilbar.
Lösung zu (ii). (5 Punkte) Wir gehen wie in (i) vor, da auch hier der Modulus 7 prim ist:

$$\begin{aligned} 5^{6350} &= 5^{6000+300+50} = 5^{6 \cdot 1000 + 6 \cdot 50 + 6 \cdot 8 + 2} = 5^{6 \cdot (1000+50+8)} \cdot 5^2 \\ &= (5^6)^{1000+50+8} \cdot 5^2 \equiv (1)^{1000+50+8} \cdot 5^2 = 5^2 = 25 \equiv 4 \mod 7. \end{aligned}$$

Aufgabe 4. Was lässt sich jeweils mithilfe der gegebenen Kongruenz und des kleinen Fermatschen Satzes über die Primalität des Modulus sagen?

(i) $6^{851} \equiv 31 \mod 851$ und $184^{850} \equiv 1 \mod 851$

Finden Sie alle Erzeugenden von $(\mathbb{Z}/11\mathbb{Z})^*$ und bestimmen Sie die Ordnung von 3 in $(\mathbb{Z}/11\mathbb{Z})^*$. Wie viele Erzeuger hat $(\mathbb{Z}/23\mathbb{Z})^*$?

Lösung zu Aufgabe 4. Hierfür brauchen wir nur zu wissen:

- Gilt $a^n \equiv a \mod n$ bzw. $a^{n1} \equiv 1 \mod n$, so ist n Pseodoprim bzgl. a.
- Gibt es eine Zahl a, sodass n nicht Pseodoprim bzgl. a ist, so ist n nicht prim.

Damit können wir die Aussagen direkt aus den Gleichungen ablesen:

(i) (4 Punkte) 851 ist nicht Pseodoprim bzgl. 6, insbesondere ist 851 nicht prim. Jedoch ist 851 Pseodoprim bzgl. 184.

(4 Punkte) Die multiplikative Gruppe $(\mathbb{Z}/11\mathbb{Z})^*$ ist zyklisch, weil sie die multiplikative Gruppe des endlichen Körpers $\mathbb{Z}/11\mathbb{Z}$ ist. Insbesonderes gibt es $\varphi(11-1) = 4$ erzeugende Elemente in $(\mathbb{Z}/11\mathbb{Z})^*$. Welche sind es? Wir testen modulo 11:

- $\bar{2}$, $\bar{2}^2 = 4$, $\bar{2}^3 = 8$, $\bar{2}^4 = 5$, $\bar{2}^5 = 10$. Da alle diese Elemente verschieden von $\bar{1}$ sind, muss gelten $ord(\bar{2}) > 5$. Aber wie wir wissen gilt auch $ord(\bar{2}) | 10 = \varphi(11)$. Damit ist $ord(\bar{2}) = 10$, und $\bar{2}$ ist ein erzeugendes Element von $(\mathbb{Z}/11\mathbb{Z})^*$.
- Es ist $\bar{2} \cdot \bar{6} = \bar{1}$. Damit gilt für $k \in \mathbb{N}$

  $$\bar{6}^k = \bar{1} \Leftrightarrow \bar{2}^k \cdot \bar{7}^k = \bar{2}^k \Leftrightarrow \bar{1} = \bar{2}^k.$$

  Es folgt sofort, $ord(\bar{6}) = ord(\bar{2}) = 10$. Damit ist auch $\bar{6}$ ein erzeugendes Element.
- $\bar{3}$, $\bar{3}^2 = 9$, $\bar{3}^3 = 5$, $\bar{3}^4 = 4$, $\bar{3}^5 = 1$. Damit ist die Ordnung von 3 in $(\mathbb{Z}/11\mathbb{Z})^*$ gleich 5.
- $\bar{4}$, $\bar{4}^2 = 5$, $\bar{4}^3 = 9$, $\bar{4}^4 = 3$, $\bar{4}^5 = 1$.
- $\bar{5}$, $\bar{5}^2 = 3$, $\bar{5}^3 = 4$, $\bar{5}^4 = 9$, $\bar{5}^5 = 1$.
- $\bar{7}$, $\bar{7}^2 = 5$, $\bar{7}^3 = 2$, $\bar{7}^4 = 3$, $\bar{7}^5 = 10$. Da alle diese Elemente verschieden von $\bar{1}$ sind, muss gelten $ord(\bar{7}) > 5$. Aber wie wir wissen gilt auch $ord(\bar{7}) | 10 = \varphi(11)$. Damit ist $ord(\bar{7}) = 10$, und $\bar{7}$ ist ein erzeugendes Element von $(\mathbb{Z}/11\mathbb{Z})^*$.

- Es ist $\bar{7} \cdot \bar{8} = \bar{1}$. Damit gilt für $k \in \mathbb{N}$

$$\bar{8}^k = \bar{1} \Leftrightarrow \bar{7}^k \cdot \bar{8}^k = \bar{7}^k \Leftrightarrow \bar{1} = \bar{7}^k.$$

  Es folgt sofort, $ord(\bar{8}) = ord(\bar{7}) = 10$. Damit ist auch $\bar{8}$ ein erzeugendes Element.

Da wir wissen, dass es genau 4 dieser Elemente gibt, haben wir mit $\bar{2}$, $\bar{6}$, $\bar{7}$, und $\bar{8}$ alle erzeugende Elemente von $(\mathbb{Z}/11\mathbb{Z})^*$ gefunden.

(2 Punkte) Die multiplikative Gruppe $(\mathbb{Z}/23\mathbb{Z})^*$ ist zyklisch. Insbesonderes gibt es $\varphi(23-1) = 10$ erzeugende Elemente in $(\mathbb{Z}/23\mathbb{Z})^*$.