DMA - Serie 9

Pascale Welsch
13-204-821

1. Eine Zahl z kann durch $z = (z_n \cdots z_1 z_0)_{10}$ im Dezimalsystem dargestellt werden.

$\forall z \in \mathbb{N}$ gilt: $11 | z \iff \sum_{j=0}^{k} 10^j \cdot z_j \equiv 0 \pmod{11}$

Bei der Division einer Zehnerpotenz durch 11 können zwei Fälle unterschieden werden:

$10^0 \equiv 1 \pmod{11}$
$10^1 \equiv 10 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$
$10^3 \equiv 10 \pmod{11}$
$\vdots$

Das heisst

$$11 | z \iff \begin{cases} \sum_{j=0}^{(k-1)/2} 1 \cdot z_{2j} + 10 \cdot z_{2j+1} \equiv 0 \pmod{11} & \text{für } k \text{ ungerade} \\ \left(\sum_{j=0}^{(k/2)-1} 1 \cdot z_{2j} + 10 \cdot z_{2j+1} \right) + z_k \equiv 0 \pmod{11} & \text{für } k \text{ gerade} \end{cases}$$

Dies könnte auch anders formuliert werden:

$10^0 \equiv 1 \pmod{11}$
$10^1 + 1 \equiv 0 \pmod{11} \iff 10^1 \equiv -1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$
$10^3 + 1 \equiv 0 \pmod{11} \iff 10^3 \equiv -1 \pmod{11}$

Daraus folgt, dass

$$11 | z \iff \sum_{j=0}^{k} (-1)^j \cdot z_j \equiv 0 \pmod{11}$$

Ausformuliert heisst dies: 11 teilt z genau dann wenn 11 auch die alternierende Quersumme von z teilt.

(2) Da p eine Primzahl ist, sind alle Zahlen $1, 2, \dots (p-1)$, sowie auch die Zahl a, da diese einen Wert zwischen 1 und $(p-1)$ annimmt, teilerfremd zu p. Dies bedeutet, dass für kein Element $k \in \{a \bmod p, 2a \bmod p, \dots, (p-1) \cdot a \bmod p\}$ gilt, dass $k \equiv 0 \pmod p$. Zudem muss jedes Element k kleiner als p sein. Die Menge

$X = \{a \bmod p, 2a \bmod p, \dots (p-1) \cdot a \bmod p\}$ muss also mindestens eine Teilmenge von

$Y = \{1, 2, \dots (p-1)\}$ sein.

Da wir wissen, dass die Mengen X, Y gleich viele Elemente haben, reicht es zu zeigen, dass alle Elemente von X verschieden (eindeutig) sind, um die Äquivalenz von X und Y zu zeigen.

In diesem Beispiel gilt, dass

$$b \cdot a \equiv c \cdot a \pmod p \overset{(1)}{\Longleftrightarrow} b \equiv c \pmod p$$ und da $b < p$, gilt $b = c$. Die Elemente aus X sind also alle verschieden und somit gilt $X = Y$.

(1) gilt, weil per Definition gilt:

$$a \equiv b \pmod{m} \Longleftrightarrow m \mid (a-b), \text{ also}$$

$$x \cdot a \equiv xb \pmod m \Longleftrightarrow m \mid (xa - xb) \Longleftrightarrow m \mid x \cdot (a-b).$$

Damit $m / x \cdot (a-b)$, muss m entweder x oder $(a-b)$ teilen. Auf die obenstehende Aufgabe bezogen bedeutet dies, dass

$$b \cdot a \equiv c \cdot a \pmod p \Longleftrightarrow p \mid (ba - c \cdot a) \Longleftrightarrow p \mid a \cdot (b-c)$$
$$\Longleftrightarrow p \mid a \quad \vee \quad p \mid (b-c). \quad \text{Da } p > a \Rightarrow \neg (p \mid a).$$
also muss gelten, dass $p \mid (b-c) \Longleftrightarrow b \equiv c \pmod p$.

Bemerkung: Es wäre sinnvoller, zuerst Aufgabe 9.3 zu lösen, da diese für Aufgabe 9.2 benötigt wird.

③ Zu zeigen: $ac \equiv bc \pmod p \Rightarrow a \equiv b \pmod p$

Per definition $ac \equiv bc \pmod p \Leftrightarrow p \mid (ac - bc) \Leftrightarrow p \mid c \cdot (a-b)$

$p \mid c \cdot (a-b) \overset{*}{\Leftrightarrow} p \mid c \lor p \mid (a-b)$.

Aus der Aufgabenstellung wissen wir, dass $\neg(p \mid c)$, also gilt $p \mid (a-b) \Leftrightarrow a \equiv b \pmod p$.

* Folgt aus Lemma 2,3 S. 271 (Rosen, 7th edition).

④ a) $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1) \cdot a \mod p$

$= a^{p-1} \cdot (p-1)! \mod p$

b) In Aufgabe 9.2 wurde gezeigt, dass

$\{a \bmod p, 2a \bmod p, \ldots, (p-1) \bmod p\} = \{1, 2, \ldots (p-1)\}$

Bei einer Multiplikation mod p gilt, dass

$a \cdot b \mod p = ((a \bmod p) \cdot (b \bmod p)) \mod p$.

Bei Aufgabe a) gilt deshalb, dass

$a \cdot 2a \cdot \ldots \cdot (p-1) \cdot a \pmod p = (a \pmod p \cdot 2a \bmod p \cdot \ldots \cdot (p-1) \cdot a \pmod p)$
$\pmod p$

Sind gerade die Elemente der Menge X aus Aufgabe 9.2. Es wurde gezeigt, dass jedes Element der Menge X genau einem Element aus der Menge Y zugeordnet werden kann. Somit ist das Produkt über alle Elemente der Menge X gleich dem Produkt über alle Elemente der Menge Y, also gilt

$a \cdot 2a \cdot \ldots \cdot (p-1) \cdot a \pmod p = 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p$

Also gilt: $a^{p-1} \cdot (p-1)! \equiv (p-1)! \cdot 1 \pmod p$

c) 9.3 besagt, dass falls $ac \equiv bc \pmod p$ und $p \nmid c$, dann $a \equiv b \pmod p$.

Hier: $p \nmid (p-1)!$* also gilt: $p \mid (a^{p-1} - 1)$

$\Rightarrow a^{p-1} \equiv 1 \pmod p$ $\square$

*Folgt aus Wilson's Theorem