Übungsblatt #1 – Lösung

Vorüberlegung (*):

Es ist $(x-1)\cdot\sum_{i=0}^{n-1} x^i = x^n - 1$, also $x-1 \mid x^n-1$

für $n \in \mathbb{N}$, sogar $n \in \mathbb{N}_0$ (für $n=0$ ist $x^n-1 = 0$, $x-1 \neq 0$ ✓)

A1

a) $a,b \geq 2 \Rightarrow a^b+1 \geq 5 \Rightarrow a^b+1 \neq 2$.

Annahme: a ungerade $\Rightarrow a^b$ ungerade $\Rightarrow 2 \mid a^b+1$ } $\lightning$ zu a^b+1 prim.

$\Rightarrow$ a ist gerade.

$b = 2^\ell \cdot u$ mit $\ell \in \mathbb{N}_0$ und $2 \nmid u$. zz. ist $u = 1$.

Variante 1: reduce modulo $a^{2^\ell}+1$: $a^{2^\ell}+1$

$$a^b+1 = a^{2^\ell \cdot u}+1 = (a^{2^\ell})^u + 1 \equiv (-1)^u + 1 = -1+1 = 0 \mod a^{2^\ell}+1.$$

(u ungerade)

$\Rightarrow a^{2^\ell}+1 \mid a^b+1$.

Da a^b+1 prim $\longrightarrow a^{2^\ell}+1 \in \{1, a^b+1\}$.

$a^{2^\ell}+1 > 1 \Rightarrow a^{2^\ell}+1 = a^b+1 \Rightarrow 2^\ell = b \Rightarrow u = 1$.

Variante 2: Wir schreiben die Zerlegung hin:

$$(a^{2^\ell})^u + 1 = (a^{2^\ell}+1)\cdot\left((a^{2^\ell})^{u-1} - (a^{2^\ell})^{u-2} + \ldots + a^{2^\ell} + 1\right)$$

$$\left(x^u + 1 = (x+1)\cdot\left(x^{u-1} - x^{u-2} + \ldots - x + 1\right)\right)$$

Rest wie oben.

b) Nach (*) gilt $a-1 \mid a^5-1$.

a^5-1 prim $\Rightarrow a-1 \in [1, a^5-1]$ mod wegen $b \geq 2$

ist $a-1 \neq a^5-1 \Rightarrow a-1=1 \Leftrightarrow a=2$.

Sei nun 2^b-1 prim, $b=m \cdot n$. Da $b \geq 2$ reicht es,

$m=1$ oder $n=1$ zu zeigen.

$2^{m \cdot n}-1 = (2^m)^n-1$ und wieder mit * gilt

$2^m-1 \mid (2^m)^n-1$.

$\underset{(2^m)^n-1 \text{ prim}}{\Longrightarrow} 2^m-1 \in \{1, (2^m)^n-1\}$.

Fall 1: $2^m-1=1 \Rightarrow m=1$.

Fall 2: $2^n-1=(2^m)^n-1 \Rightarrow n=1$.

A2 a) $N \in \mathbb{N} \Rightarrow 2 \mid 2^N \Rightarrow 2 \nmid 2^N-1$.

Annahme: $2 \mid N \Rightarrow 2 \mid N$ und $N \mid 2^N-1 \Rightarrow 2 \nmid 2^N-1$ ↯.

b) Es gibt $k, \ell \in \mathbb{Z}$: $a = k \cdot (p-1) + \ell \cdot N$.

Weiters gilt: $p \mid N \mid 2^N-1 \Rightarrow p \mid 2^N-1 \Rightarrow 2^N \equiv 1 \bmod p$

Fermat: $p \mid 2^p-2 = 2(2^{p-1}-1) \underset{a) p \neq 2}{\overset{p \text{ prim}}{\Longrightarrow}} p \mid 2^{p-1}-1 \Rightarrow 2^{p-1} \equiv 1 \bmod p$.

Variante 1: $2^a-1 = 2^{k \cdot (p-1) + \ell \cdot N} - 1 = (2^{p-1})^k \cdot (2^N)^\ell - 1$

$\equiv 1 \cdot 1 - 1 = 0$ modulo p.

$\Rightarrow p \mid 2^a-1$.

Variante 2:

$2^N \equiv 1 \pmod p \Longrightarrow \exists r \in \mathbb{N}_0 : 2^N = 1 + r \cdot p$.

$2^{p-1} \equiv 1 \pmod p \Longrightarrow \exists s \in \mathbb{N}_0 : 2^{p-1} = 1 + s \cdot p$.

$a = k \cdot (p-1) + \ell \cdot N$ ($\hat{=}\ k \in \mathbb{N}_0,\ \ell \in -\mathbb{N}_0$, denn

wegen $a \leq p-1$, $a \leq N$ sind k, ℓ nicht beide gleichzeitig > 0 oder < 0.

Nutze weiter: $(1+tp)^m = \sum_{i=0}^{m} \binom{m}{i} \cdot (tp)^i \cdot 1^{m-i}$

$= 1 + \underbrace{\sum_{i=1}^{m} \binom{m}{i} \cdot t^i p^i}_{\text{Vielfaches von } p} = 1 + t' \cdot p$

für ein $t' \in \mathbb{N}$, für alle $t \in \mathbb{Z}$, $m \in \mathbb{N}_0$.

Damit gilt

$a\ 2^a = 2^{k(p-1)+\ell \cdot N} = (2^{p-1})^k \cdot (2^N)^\ell$

$= (1+sp)^k \cdot (1+rp)^\ell = \cancel{1 + s'p} \quad \cancel{\exists s' \in \mathbb{N}} \quad \cancel{1 + t'p}$

$= \frac{(1+sp)^k}{(1+rp)^{-\ell}} \overset{\exists s', r' \in \mathbb{N}}{=} \frac{1+s'p}{1+r'p} = \frac{1 + r'p - r'p + s'p}{1+r'p}$

Für $k \leq 0, \ell \geq 0$ analog...

$= 1 + p \frac{s' - r'}{1+r'p} \in \mathbb{N}$.

$\Longrightarrow p \cdot \frac{s'-r'}{1+r'p} \in \mathbb{N}$, also $1 + r'p \mid p \cdot (s' - r')$

Wegen $p \nmid 1 + r'p \Longrightarrow ggT(p, 1+r'p) = 1$

$\Rightarrow 1 + r'p \mid s' - r'$.

$\Rightarrow 2^a \in 1 + p \cdot \mathbb{N} \Rightarrow p \mid 2^a - 1$.

A3 allgemein gilt: Sei $n \in \mathbb{N}$ fest $\vee$ ~~$x \equiv y \bmod n$~~ $n \mid x-y$,

d.h. $x - y = k \cdot n$ für ein $k \in \mathbb{Z}$. Dann gilt

$n \mid x \overset{(!)}{\Leftrightarrow} n \mid y$, denn:

"$\Rightarrow$" $n \mid x$, d.h. $x = n \cdot l$ für ein $l \in \mathbb{Z}$.

$\Rightarrow y = x - kn = nl - kn = n(l-k)$

$\Rightarrow n \mid y$.

"$\Leftarrow$" analog.

a) Für $x \in \mathbb{N}$ berechnet sich die Quersumme $QS(x)$ wie folgt:

Stelle x dar als $x = \sum_{i=0}^{m} a_i 10^i$, $a_i \in \{0, \dots, 9\}$, $m \in \mathbb{N}$.

$\Rightarrow QS(x) = \sum_{i=0}^{m} a_i$.

Für alle $i \in \mathbb{N}$ gilt mit (*): $9 = 10 - 1 \mid 10^i - 1$,

also gilt

$$9 \mid \sum_{i=0}^{m} a_i (10^i - 1) = \underbrace{\sum_{i=0}^{m} a_i 10^i}_{x} - \underbrace{\sum_{i=0}^{m} a_i}_{QS(x)}.$$

Die Behauptung folgt dann mit der Voraussetzung.

b) Wir beweisen $11 \mid 99 = 100 - 1$.

Stelle $x \in \mathbb{N}$ dar als $x = \sum_{i=0}^{m} a_i 100^i$ mit $a_i \in \{0, \dots, 99\}$.

(Das ist die normale Darstellung, wobei wir je 2 Ziffern zusammenfassen.)

$gQS(x) := \sum_{i=0}^{m} a_i$ sei die gewichtete Quersumme.

Dann gilt $11 \mid 99 = 100 - 1 \mid \sum_{i=0}^{m} a_i (100^i - 1)$

$$= \underbrace{\sum_{i=0}^{m} a_i 100^i}_{x} - \underbrace{\sum_{i=0}^{m} a_i}_{gQS(x)}.$$

Also gilt $11 | x \Leftrightarrow 11 | gQS(x)$, die sich in der normalen Darstellung $x = \sum_{i=0}^{m'} b_i \cdot 10^i$ als

$gQS(x) = b_0 + 10 b_1 + b_2 + 10 b_3 + \ldots$ berechnet. □

Alternative:

Es gilt auch $11 | x \Leftrightarrow 11 | aQS(x)$, wobei:

für $x = \sum_{i=0}^{m'} b_i \cdot 10^i$ die alternierende Quersumme

$aQS(x) = b_0 - b_1 + b_2 - b_3 + \ldots$ ist.

Wir sehen das direkt, weil $11 | gQS - aQS$.

Ein anderer Weg, das zu zeigen, wäre Rechnen modulo 11:

$$\sum_{i=0}^{m'} b_i \cdot 10^i \equiv \sum_{i=0}^{m'} b_i (-1)^i \quad \text{modulo } 11,$$

was sofort die Behauptung zeigt.

Wegen $10 \equiv 1 \pmod 9$ folgt a) genauso und die Lösung der Aufgabe wäre ein nicht einmal eine halbe Seite lang.

A4 $4928 = 2 \cdot 2233 + 462$

$2233 = 4 \cdot 462 + 385$ (NR: $2233 - 4 \cdot 462 = 2233 - 1848 = 385$)

$462 = 385 + 77$

$385 = 5 \cdot 77 + 0$

$\Rightarrow ggT(4928, 2233) = 77.$

$$kgV(4928, 2233) = \frac{4928 \cdot 2233}{77} = 4928 \cdot 29 = 142912.$$

NR:

```
 2233 : 77 = 29
-154
 693
-693
   0
```

NR:

```
  4928 · 29
 ---------
  9856
 44352
 ---------
142912
```

Es ist $77 = 462 - 385 = 462 - (2233 - 4 \cdot 462)$

$= 5 \cdot 462 - 2233 = 5 \cdot (4928 - 2 \cdot 2233) - 2233$

$= 5 \cdot 4928 - 11 \cdot 2233.$