Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 1

Aufgabe 1 (4 Punkte)
Seien $a, b \in \mathbb{N}$, $a, b \geq 2$. Zeigen Sie die folgenden Aussagen:

a) Ist $a^b + 1$ eine Primzahl, so ist a gerade und b eine Zweierpotenz.

b) Ist $a^b - 1$ eine Primzahl, so ist $a = 2$ und b eine Primzahl.

Lösung:

a) Ist $a^b + 1$ eine Primzahl, so ist es ungerade, da $a^b \geq 4$. Daher muss a gerade sein. Wäre b ungerade, so wäre $a^b \equiv -1 \pmod{a+1}$, da $a \equiv -1 \pmod{a+1}$. Schlichter gesagt wäre $a + 1$ ein Teiler von $a^b + 1$, was man an

$$(a+1) \cdot (a^{b-1} - a^{b-2} + a^{b-3} \pm \cdots - a + 1) = a^b + 1$$

sieht. Wegen $a, b \geq 2$ kann dann $a^b + 1$ keine Primzahl sein.
Daher ist auch b gerade.
Wäre b keine Zweierpotenz, so wäre $b = 2^e \cdot c$ mit $e \in \mathbb{N}$ und ungeradem $c > 1$. Dann aber wäre

$$a^b + 1 = (a^{2^e})^c + 1$$

immer noch eine Primzahl, und das widerspricht unserer Einsicht, dass der Exponent – in diesem Fall c – gerade ist.

b) Immer ist $a - 1$ ein Teiler von $a^b - 1$:

$$\frac{a^b - 1}{a - 1} = 1 + a + a^2 + \ldots + a^{b-1}.$$

Ist $a^b - 1$ eine Primzahl, so ist demnach $a - 1 = 1$, also $a = 2$.
Weiter ist für $b = cd$

$$2^{cd} - 1 = (2^c - 1)(1 + 2^c + 2^{2c} + \ldots + 2^{(d-1)c})$$

eine Zerlegung von $a^b - 1$ in zwei Faktoren, also muss einer von beiden gleich 1 sein, da $a^b - 1$ Primzahl ist. Es folgt $c = 1$ oder $c = b$, was zeigt, dass b eine Primzahl ist, da es voraussetzungsgemäß größer als 1 ist.

Aufgabe 2 (4 Punkte)
Sei $N \in \mathbb{N}$ eine natürliche Zahl, die $2^N - 1$ teilt. Zeigen Sie die folgenden Aussagen:

a) N ist ungerade.

b) Für einen Primteiler p von N und $a := \text{ggT}(p-1, N)$ ist p ein Teiler von $2^a - 1$.

c) $N = 1$.

Lösung: Aufgabenteil b) haben wir damals grundlegender durchgerechnet. Da ich die Lösung am Ende des Semesters nachreiche, setze ich ein paar Dinge voraus. Wer sich für die grundlegende Lösung interessiert, schaue in den Aufschrieb der damaligen Übung.

a) 2^N ist gerade, also $2^N - 1$ ungerade. Dann muss auch der Teiler N ungerade sein.

b) Wir können den ggT als Linearkombination schreiben: $a = k \cdot (p-1) + l \cdot N$ mit $k, l \in \mathbb{Z}$.
Modulo p gilt: $2^{p-1} \equiv 1(p)$ nach Lagrange und $2^N \equiv 1(p)$, denn $p|2^N - 1$.
Damit folgt $2^a - 1 = 2^{k(p-1)+lN} - 1 = (2^{p-1})^k \cdot (2^N)^l - 1 \equiv 1^k 1^l - 1 \equiv 0(p)$, also $p|2^a - 1$ wie gefordert.

c) Wäre $N \neq 1$, so gäbe es einen kleinsten Primteiler p_0 von N. Wegen $p_0 - 1 < p_0$ sind $p_0 - 1$ und N teilerfremd, also $\text{ggT}(p_0 - 1, N) = 1$.
Nach b) gilt dann $p_0|2^1 - 1 = 1$, was offensichtlich ein Widerspruch ist.

Aufgabe 3 (4 Punkte)

a) Zeigen Sie, dass eine natürliche Zahl durch 9 teilbar ist, wenn ihre Quersumme durch 9 teilbar ist.

b) Finden Sie eine Regel für die Teilbarkeit durch 11 und beweisen Sie diese.

Lösung: Hinweis: Wir haben das Ganze damals grundlegender durchgerechnet, wer sich dafür interessiert, schaut in den Mitschrieb der Übung. Da ich diese schriftliche Lösung am Ende des Semesters nachreiche, verwende ich den eleganteren Weg.

Stelle $x \in \mathbb{N}$ dar als $x = \sum_{i=0}^{<\infty} a_i 10^i$ mit Ziffern $a_i \in \{0, ..., 9\}$.

a) Die Quersumme von $x \in \mathbb{N}$ ist $\text{QS}(x) = \sum_{i=0}^{<\infty} a_i$.
Wegen $10 \equiv 1$ modulo 9 ist $x \equiv \text{QS}(x)$ modulo 9.
Stärker gilt also sogar, dass x und $\text{QS}(x)$ den gleichen Rest bei Division durch 9 lassen, also insbesondere
$9|x \Leftrightarrow x \equiv 0(9) \Leftrightarrow \text{QS}(x) \equiv 0(9) \Leftrightarrow 9|\text{QS}(x)$.

b) Hier gibt es zwei naheliegende Ansätze, die wegen $-1 \equiv 10\ (11)$ aber gleichwertig sind.
Ansatz 1: Stelle x 100-adisch dar, das heißt $x = \sum_{i=0}^{<\infty} b_i 100^i$ mit $b_i \in \{0, ..., 99\}$.
Die Summe der b_i nennen wir $\text{gQS}(x)$ und es gilt – analog zu a) – $x \equiv \text{gQS}(x)\ (11)$, also ist x durch 11 teilbar, wenn die *gewichtete Quersumme* durch 11 teilbar ist.

Der Name „gewichtet“ rührt daher, dass wir gQS aus der 10-adischen Darstellung durch $\mathrm{gQS}(x) = a_0 + 10a_1 + a_2 + 10a_3 + ...$ ausrechnen.
Ansatz 2: Anstelle der Gewichtung 10 nehmen wir die Gewichtung -1. Modulo 11 ist das egal. Anders gedacht, es ist $10 \equiv -1\ (11)$, also
$x = \sum_{i=0}^{<\infty} a_i 10^i \equiv \sum_{i=0}^{<\infty} a_i(-1)^i = a_0 - a_1 + a_2 - a_3 + ... =: \mathrm{aQS}(x)$.
Also ist x durch 11 teilbar, wenn die *alternierende Quersumme* von x durch 11 teilbar ist. Der Name „alternierend“ ist selbsterklärend, nicht wahr?

Aufgabe (4 Punkte)
Berechnen Sie den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache der Zahlen 4928 und 2233. Stellen Sie anschließend den ggT als ganzzahlige Linearkombination der beiden Zahlen dar.

Lösung:
Wir wenden den Euklidischen Algorithmus an:
$4928 = 2 \cdot 2233 + 462$
$2233 = 4 \cdot 462 + 385$
$462 = 385 + 77$
$385 = 5 \cdot 77 + 0$. Der ggT ist 77. Rückwärtsrechnen gibt
$77 = 462 - 385 = 462 - (2233 - 4 \cdot 462) = 5 \cdot 462 - 2233 = 5 \cdot (4928 - 2 \cdot 2233) - 2233 = 5 \cdot 4928 - 11 \cdot 2233$.

Für natürliche Zahlen a, b gilt $a \cdot b = \mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b)$, also können wir den gesuchten kgV ausrechnen als
$\frac{4928 \cdot 2233}{77} = 142912$.