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

Einführung in Algebra und Zahlentheorie – Übungsblatt 11

Aufgabe 1 (4 Punkte)
Sei R ein kommutativer Ring, $d, g \in R$ mit $d|g-1$. Weiterhin sei $x \in R$ g-adisch dargestellt durch

$$x = \sum_{i=0}^{n} a_i g^i \text{ mit } n \in \mathbb{N}_0, a_i \in R.$$

Zeige, dass d genau dann ein Teiler von x ist, wenn es die Summe $\sum_{i=0}^{n} a_i$ der Koeffizienten teilt.[1]

Lösung Aufgabe 1
d ist genau dann ein Teiler eines Elements y, wenn $y \in (d) = dR$, wenn also $\overline{y} = 0$ in $R/(d)$. Alle nachfolgenden Restklassen seien modulo d:
Wegen $d|g-1$ gilt $\overline{g-1} = 0 \Rightarrow \overline{g} = \overline{1}$. Damit aber ist $\overline{x} = \overline{\sum\ a_i g^i} = \overline{\sum\ a_i}$.
Insbesondere ist also $\overline{x} = 0 \Leftrightarrow \overline{\sum\ a_i} = 0$, was zu zeigen war.

Aufgabe 2 (4 Punkte)

a) Ist $2^n - 1$ für $n \in \mathbb{N}$ eine Primzahl, so ist bereits n prim.

b) Ist $2^n + 1$ für $n \in \mathbb{N}$ eine Primzahl, so ist n eine Zweierpotenz $n = 2^k$ für ein $k \in \mathbb{N}_0$.

c) Zeige, dass für $F_k = 2^{(2^k)} + 1$, $k \in \mathbb{N}_0$ die folgende Rekursion gilt: $F_k = \prod_{i=0}^{k-1} F_i + 2$.

d) Folgere aus c), dass es unendlich viele Primzahlen gibt.

Bemerkung: Die Umkehrungen von a) und b) wurden lange Zeit vermutet, sind aber jeweils falsch. Die kleinsten Gegenbeispiele sind $2^{11} - 1 = 23 \cdot 89$ und $2^{(2^5)} + 1 = 641 \cdot 6700417$.
Eine (Prim-)Zahl der Form $2^n - 1$ heißt *Mersenne-(Prim-)Zahl*. Diese spielen heute bei der Suche nach großen Primzahlen eine wichtige Rolle. Eine (Prim-)Zahl der Form $2^{(2^k)} + 1$ heißt *Fermat-(Prim-)Zahl*.

Lösung Aufgabe 2

a) Es ist $n \neq 1$, also reicht es zu zeigen, dass aus $n = k \cdot l$ mit $k, l \in \mathbb{N}$ folgt, dass $k = 1$ oder $l = 1$ ist. Es ist $2^n - 1 = 2^{kl} - 1 = (2^k)^l - 1$ und dies können wir - dabei könnte es helfen, gedanklich 2^k mit X zu substituieren - wie folgt zerlegen:

$$(2^k)^l - 1 = (2^k - 1) \sum_{i=0}^{l-1} 2^i.$$

(*Hinweis:* Es ist dabei gar nicht zwingend nötig, den zweiten Faktor zu finden. Nach der gedanklichen Substitution sieht man doch in jedem Fall, dass man $X - 1 = 2^k - 1$ als Faktor abspalten kann, denn 1 ist doch eine Nullstelle von $X^l - 1$. Das genügt.)
Da $2^n - 1$ prim ist, ist der Faktor $2^k - 1$ also 1 oder $2^n - 1$. Ersteres impliziert $k = 1$, zweiteres dann $k = n$, also $l = 1$.

b) Wir zerlegen $n = u \cdot g$ mit ungeradem u und einer Zweierpotenz g. Zu zeigen ist $u \overset{(!)}{=} 1$.
Wir betrachten $2^n + 1 = 2^{ug} + 1 = (2^g)^u + 1$ modulo $2^g + 1$: Dann ist $\overline{2^g} = \overline{-1}$ und da u ungerade

[1] Erinnere dich daran, dass du das für $R = \mathbb{Z}$, $g = 10$, $d = 3$ (oder auch $d = 9$) bereits aus der Schule kennst.

ist, ist $(-1)^u = -1$. Also gilt

$$\overline{2^n + 1} = \overline{(2^g)^u + 1} = \overline{(-1)^u + 1} = \overline{0}.$$

Es folgt, dass $2^g + 1$ ein Teiler von $2^n + 1$ ist. Da $2^n + 1$ prim ist, ist $2^g + 1 \in \{1, 2^n + 1\}$, aber wegen $2^n + 1 \geq 2$ muss $2^g + 1 = 2^n + 1$ sein, woraus $u = 1$ folgt.

c) Genießer beginnen den Induktionsanfang mit $k = 0$. Es ist $F_0 = 2^{(2^0)} + 1 = 3$, ebenso wie $\prod_{i=0}^{-1} F_i + 2$, denn das leere Produkt ist 1.
Wer es etwas handfester mag, beweist die Rekursion ab $k = 1$ und sicher ist $\prod_{i=0}^{0} F_i + 2 = 3 + 2 = 5 = F_1$.

Gelte $F_n - 2 = \prod_{i=0}^{n-1} F_i$ für ein $n \in \mathbb{N}_0$. Dann ist
$\prod_{i=0}^{n} F_i = F_n \cdot \prod_{i=0}^{n-1} F_i = F_n \cdot (F_n - 2) = F_n^2 - 2 \cdot F_n = (2^{(2^n)} + 1)^2 - 2 \cdot (2^{(2^n)} + 1) = 2^{(2^{n+1})} + 2 \cdot 2^{(2^n)} + 1 - 2 \cdot 2^{(2^n)} - 2 = 2^{(2^{n+1})} - 1 = F_{n+1} - 2$.

d) Es reicht zu zeigen, dass verschiedene F_k keinen gemeinsamen Teiler haben. Dann ist die Menge der Primteiler aller F_k unendlich, denn jedes F_k gibt mindestens einen neuen Primteiler und es gibt ja unendlich viele F_k.
Die Behauptung folgt aber aus der Rekursionsformel: Sei l ein gemeinsamer Teiler von F_r, F_s ohne Einschränkung $r > s$, dann ist F_s (und damit l) ein Teiler von $F_r - 2$ wegen der Rekursion. l ist also Teiler von $F_r, F_r - 2$, also auch von 2. Aber da alle F_k ungerade sind, ist $l \neq 2$, also $l = 1$.

Aufgabe 3 (4 Punkte)
Seien $n \in \mathbb{N}$ quadratfrei, $a \in \mathbb{Z}$ beliebig. φ sei die eulersche φ-Funktion. Zeige folgende Aussagen:

a) Für alle $k \in \mathbb{N}_0$ ist $a^{k \cdot \varphi(n)+1} \equiv a$ (modulo n).

b) Für $e \in \mathbb{N}$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$ ist die Abbildung $a \mapsto a^e$ eine Bijektion auf $\mathbb{Z}/n\mathbb{Z}$.

Bemerkung: Das RSA-Verfahren basiert auf einem Spezialfall dieser Aussage.

Lösung Aufgabe 3

a) Es ist $n = \prod_{i=1}^{r} p_i$ für paarweise verschiedene Primzahlen $p_1, ..., p_r$ und $\varphi(n) = \prod_{i=1}^{r} (p_i - 1)$.
Wir zeigen, dass für alle j die Kongruenz $a^{k \cdot \varphi(n)+1} \equiv a$ (modulo p_j) gilt. Dies ist offensichtlich richtig für $a \equiv 0$(modulo p_j). Ist a hingegen $\not\equiv 0$, so gilt $a^{p_j - 1} \equiv 1$ modulo p_j, denn wegen $\#\mathbb{Z}/p_j\mathbb{Z}^\times = p_j - 1$ folgt die Gleichheit aus dem Satz von Lagrange.
Mit $c := k \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r} (p_i - 1)$ gilt $a^{k \cdot \varphi(n)+1} = a^{(p_j - 1) \cdot c} \cdot a^1 = (a^{p_j - 1})^c \cdot a \equiv a$ (modulo p_j).
Die Aussage ist also richtig für $r = 1$, für $r \geq 1$ folgt die Aussage mit dem chinesischen Restsatz, denn es gibt genau einen Rest modulo n, der bei Division durch die p_i die gegebenen Reste lässt. Dies ist offensichtlich a (modulo n).

b) Wir berechnen $d \in \mathbb{N}$ mit $\overline{d} \cdot \overline{e} = \overline{1} \in \mathbb{Z}/\varphi(n)\mathbb{Z}$. Dies geht wegen der Teilerfremdheit von e und $\varphi(n)$. Es gibt also $k \in \mathbb{N}$, so dass $de = k \cdot \varphi(n) + 1$, und nach a) ist $(a^d)^e = (a^e)^d = a^{(de)} = a^{k \cdot \varphi(n)+1} = a$ für jede Restklasse $a \in \mathbb{Z}/n\mathbb{Z}$. Dies zeigt, dass $\cdot^e$ und $\cdot^d$ Umkehrfunktionen voneinander sind.

Aufgabe 4 (4 Punkte) (**Aufgabenteil c) umformuliert**)

Seien $a, b \in \mathbb{N}$ und $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Desweiteren seien $g = \text{ggt}(a, b)$, $k = \text{kgV}(a, b)$.

a) Finde einen Isomorphismus zwischen $\mathbb{Z}^2/A\mathbb{Z}^2$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

b) Finde $S, T \in \text{SL}_2(\mathbb{Z})$ mit S von der Form $\begin{pmatrix} 1 & 1 \\ * & * \end{pmatrix}$, so dass $SAT = \begin{pmatrix} g & 0 \\ 0 & k \end{pmatrix}$.

c) Zeige $\mathbb{Z}^2/A\mathbb{Z}^2 \cong \mathbb{Z}^2/SAT\mathbb{Z}^2$ oder $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ und folgere anschließend die jeweils andere Aussage daraus.

Lösung Aufgabe 4

a) Wir untersuchen die natürliche Projektion $\psi : \mathbb{Z}^2 \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto (x + a\mathbb{Z}, y + b\mathbb{Z})$. Dies ist ein Ringhomomorphismus, offensichtlich surjektiv.
Es reicht zu zeigen, dass $\text{Kern}(\psi) = A\mathbb{Z}^2$, dann folgt die Aussage aus dem Homomorphiesatz. (Insbesondere sehen wir damit auch ein, dass $A\mathbb{Z}^2$ überhaupt ein Ideal von $\mathbb{Z}^2$ ist, was nicht für jede Matrix aus $\mathbb{Z}^{2\times 2}$ gegeben ist. Man kann das natürlich auch direkt nachweisen.)
Aber $\text{Kern}(\psi) = \{\begin{pmatrix} x \\ y \end{pmatrix} : x \in a\mathbb{Z}, y \in b\mathbb{Z}\} = \{\begin{pmatrix} x \\ y \end{pmatrix} : x = ax', y = by' \text{ für } x', y' \in \mathbb{Z}\}$ und $A\mathbb{Z}^2 = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix} : x' \in \mathbb{Z}, y' \in \mathbb{Z}\} = \{\begin{pmatrix} ax' \\ by' \end{pmatrix} : x' \in \mathbb{Z}, y' \in \mathbb{Z}\}$, was die Gleichheit zeigt.

*Ein **alternativer Lösungsweg**, ohne den Homomorphiesatz direkt anzuwenden, ist der folgende. Man macht im Endeffekt aber gar nichts anderes als oben.*
Man zeigt, dass $\begin{pmatrix} x \\ y \end{pmatrix} \sim \begin{pmatrix} x' \\ y' \end{pmatrix}$ modulo $A\mathbb{Z}^2$ genau dann gilt, wenn $x \sim x'$ modulo a und $y \sim y'$ modulo b.
Die Abbildung $\mathbb{Z}^2/A\mathbb{Z}^2 \mapsto \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $\begin{pmatrix} x \\ y \end{pmatrix} + A\mathbb{Z}^2 \mapsto (x + a\mathbb{Z}, y + b\mathbb{Z})$ ist dann wegen „$\Rightarrow$“ wohldefiniert, wegen „$\Leftarrow$“ injektiv und offensichtlich surjektiv.
Da auf beiden Seiten alle verknüpfungen komponentenweise funktionieren, liegt ein Ringisomorphismus vor.

b) Wir konstruieren S, T stückweise. Wir erinnern uns, dass es $s, t \in \mathbb{Z}$ gibt mit $as + bt = g$ $(*)$, weiterhin erinnern wir uns, dass $a \cdot b = g \cdot k$ $(**)$ ist.
Es ist $SA = \begin{pmatrix} 1 & 1 \\ * & * \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & b \\ * & * \end{pmatrix}$ und wir sehen mit $(*)$, dass $\begin{pmatrix} s & * \\ t & * \end{pmatrix}$ ein guter Ansatz ist, um den Eintrag g in der ersten Komponente von SAT zu erhalten.
Weiterhin soll $\det(T) = 1$ sein, wieder nutzen wir $(*)$ und $g|a, g|b$, um den Ansatz $T = \begin{pmatrix} s & -\frac{b}{g} \\ t & \frac{a}{g} \end{pmatrix}$ zu erhalten.

Mit diesem T erhalten wir SAT wie folgt, wobei wir die beiden unbekannten Einträge in S mit c, d bezeichnen:
$SAT = \begin{pmatrix} 1 & 1 \\ c & d \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} s & -\frac{b}{g} \\ t & \frac{a}{g} \end{pmatrix} = \begin{pmatrix} g & 0 \\ sac + bdt & \frac{ab(d-c)}{g} \end{pmatrix}$.
Die Forderung $det(S) = 1$, Komponentenvergleich von SAT mit $\begin{pmatrix} g & 0 \\ 0 & k \end{pmatrix}$ gibt folgende Bedingungen an c, d:
Determinante: $d - c = 1$.
$\frac{ab(d-c)}{g} = k \overset{(**)}{\Rightarrow} d - c = 1$, passend zur ersten Bedingung.
$sac + bdt = 0$. Durch Einsetzen von $d = 1 + c$ erhalten wir $0 = sac + bct + bt = (sa + bt)c + bt \overset{(*)}{=} gc + bt$ und umstellen ergibt $c = \frac{-bt}{g} \in \mathbb{Z}$.
Schließlich errechnen wir $d = 1 + c \overset{(*)}{=} \frac{as+bt}{g} + \frac{-bt}{g} = \frac{as}{g} \in \mathbb{Z}$.

Damit sind alle Bedingungen erfüllt. Die gefundenen Matrizen sind

$$S = \begin{pmatrix} 1 & 1 \\ \frac{-bt}{g} & \frac{as}{g} \end{pmatrix}, T = \begin{pmatrix} s & \frac{-b}{g} \\ t & \frac{a}{g} \end{pmatrix}.$$

c) Mit a) folgt offensichtlich auch $\mathbb{Z}^2/SAT\mathbb{Z}^2 \simeq \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/h\mathbb{Z}$. Offensichtlich folgt also jede der Äquivalenzen im Aufgabenteil c) direkt aus der anderen.
(Der Übungsleiter wollte die Isormophie zunächst in der „Matrizenwelt“ zeigen, darum die ursprüngliche Aufgabenstellung. Er hat sich umentschieden, dass dies in der anderen Welt doch leichter ist, freut sich aber über Rückmeldung, wer die erste Isomorphie direkt gezeigt hat.)

Wir zeigen $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \overset{(!)}{\cong} \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$. Dafür erinnern wir uns an folgende Aussagen:
Es ist $\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ für teilerfremde m, n (Chinesischer Restsatz), was insbesondere gilt, wenn m, n Potenzen verschiedener Primzahlen sind $(*)$.
Weiterhin ist $a = \prod_{p \in \mathbb{P}} p^{a_p}$ für passende $a_p \in \mathbb{N}$: Diese sind eindeutig und wurden in der Vorlesung mit $v_p(a)$ bezeichnet. Analog ist $b = \prod_{p \in \mathbb{P}} p^{b_p}$.
Dann gilt $g = \prod_{p \in \mathbb{P}} p^{\min(a_p, b_p)}$, $k = \prod_{p \in \mathbb{P}} p^{\max(a_p, b_p)}$.
(Alle Produkte sind in Wirklichkeit endlich und damit wohldefiniert, denn fast alle a_p, b_p sind 0, also fast alle Faktoren $p^{\cdots} = 1$.)

Dann aber ist $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/(\prod_{p \in \mathbb{P}} p^{a_p})\mathbb{Z} \times \mathbb{Z}/(\prod_{p \in \mathbb{P}} p^{b_p})\mathbb{Z} \cong \prod_{p \in \mathbb{P}} (\mathbb{Z}/p^{a_p}\mathbb{Z}) \times \prod_{p \in \mathbb{P}} (\mathbb{Z}/p^{b_p}\mathbb{Z}) \cong ...$
Für jedes p ist $\{a_p, b_p\} = \{\max(a_p, b_p), \min(a_p, b_p)\}$ und wir formen weiter um, indem wir zunächst nur die Faktoren sortieren:
$... \cong \prod_{p \in \mathbb{P}} (\mathbb{Z}/\min(a_p, b_p)\mathbb{Z}) \times \prod_{p \in \mathbb{P}} (\mathbb{Z}/\max(a_p, b_p)\mathbb{Z}) \overset{(*)}{\cong} \mathbb{Z}/(\prod_{p \in \mathbb{P}} \min(a_p, b_p))\mathbb{Z} \times \mathbb{Z}/(\prod_{p \in \mathbb{P}} \max(a_p, b_p))\mathbb{Z} \cong$
$\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$.