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

Einführung in Algebra und Zahlentheorie – Übungsblatt 13 – finito – Musterlösung

Aufgabe 1 (4 Punkte)
Sei $p \geq 3$ eine Primzahl. Zeige:

a) Jede natürliche Zahl a mit $\left(\frac{a}{p}\right) = -1$ besitzt mindestens einen Primfaktor $q|a$ mit $\left(\frac{q}{p}\right) = -1$.

b) Es gibt unendlich viele Primzahlen, die kein Quadrat modulo p sind.

Lösung:

a) Das ist die Multiplikativität des Legendresymbols. Sei $a = q_1 \cdot ... \cdot q_r$, $q_i \in \mathbb{P}$ die Zerlegung von a in Primzahlen.
Annahme: Wäre $\left(\frac{q_i}{p}\right) = 1$ für alle i, dann wäre $\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right) \cdot ... \cdot \left(\frac{q_r}{p}\right) = 1$. WIDERSPRUCH

b) In der Vorlesung haben wir gesehen, dass $\{1, ..., p-1\}$ $\frac{p-1}{2}$ viele Quadrate modulo p enthält, insbesondere also auch ein Nichtquadrat modulo p. Es gibt also mindestens eine Zahl a und nach Aufgabenteil a) also auch mindestens eine Primzahl q, die kein Quadrat modulo p ist.
Annahme: Sei diese Menge endlich, $l_1, ..., l_r$ seien alle Primzahlen mit $\left(\frac{l_i}{p}\right) = -1$, insbesondere gilt $l_i \nmid p$ für alle i.
Definiere $x := l_1 \cdot l_2^2 \cdot ... \cdot l_r^2 + p$. Nach Konstruktion gilt $l_i \nmid x$ für alle i. $(*)$
Weiterhin gilt $\left(\frac{x}{p}\right) = \left(\frac{l_1 \cdot l_2^2 \cdot ... \cdot l_r^2}{p}\right) = \left(\frac{l_1}{p}\right) \cdot \left(\frac{l_2^2 \cdot ... \cdot l_r^2}{p}\right) = -1 \cdot 1 = -1$.
Nach a) gibt es einen Primteiler q von x mit $\left(\frac{q}{p}\right) = -1$. Wegen $(*)$ und da die l_i alle Primzahlen mit dieser Eigenschaft waren, haben wir einen Widerspruch.

Zusatz: Das mag willkürlich wirken, entspricht doch aber genau dem Primzahl-Gedanken Euklids: Gäbe es nur endlich viele Primzahlen $l_1, ..., l_r$, so finden wir eine neue als Primteiler von $l_1 \cdot ... \cdot l_r + 1$. Dabei könnten wir auch Potenzen der l_i betrachten, wir müssen nur dafür sorgen, dass jedes l_i den ersten Summanden (ohne +1) teilt, denn dann teilt es nicht die ganze Zahl.
In unserem Fall ersetzt $+p$ die Rolle von $+1$ – und wir müssen nur die Eigenschaft, Nichtquadrat zu sein, bekommen: Das Legendresymbol gibt uns doch vor, wie das geht, nimm jedes l_i zweifach bis auf eine ungerade Anzahl viele.
So kommen wir auf unser x.

Aufgabe 2 (4 Punkte)
Sei $R = \mathbb{Z}/524\mathbb{Z}$.

a) Wie viele Quadrate gibt es in R?

b) Wie viele $x \in R$ gibt es mit der Eigenschaft $x^2 = 20$? Wie viele $y \in R$ erfüllen $y^2 = 443$?

(*Hinweis:* Der chinesische Restsatz könnte helfen.)

Lösung: Vorüberlegung: Wir benutzen $524 = 4 \cdot 131$, wobei 131 eine Primzahl ist. Es ist also $R = \mathbb{Z}/524\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/131\mathbb{Z}$ nach dem chinesischen Restsatz.

a) Wir zählen die Quadrate in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/131\mathbb{Z}$. Es gilt:
$([a]_4, [b]_{131}) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/131\mathbb{Z}$ ist genau dann ein Quadrat, wenn $([c]_4, [d]_{131}) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/131\mathbb{Z}$ existiert mit $([a]_4, [b]_{131}) = ([c]_4, [d]_{131})^2 = ([c]_4^2, [d]_{131}^2)$, also genau dann, wenn $[a]_4$ ein Quadrat in $\mathbb{Z}/4\mathbb{Z}$ und $[b]_{131}$ ein Quadrat in $\mathbb{Z}/131\mathbb{Z}$ ist.

In $\mathbb{Z}/4\mathbb{Z}$ gibt es zwei Quadrate: $([0]_4)^2 = ([2]_4)^2 = [0]_4$ und $([1]_4)^2 = ([3]_4)^2 = [1]_4$.
In $\mathbb{Z}/131\mathbb{Z}^\times$ gibt es nach Vorlesung $\frac{131-1}{2} = 65$ Quadrate, hinzu kommt 0 als Quadrat, also insgesamt 66 Quadrate.
Insgesamt gibt es also $2 \cdot 66 = 132$ Quadrate.

b)
- Wir zählen die Anzahl der Lösungen $x^2 = 20$ in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/131\mathbb{Z}$. Dabei ist $20 = ([20]_4, [20]_{131})$. Ein Paar $x = ([a]_4, [b]_{131})$ löst $x^2 = 20$, wenn $([a]_4)^2 = [20]_4 = [0]_4$ in $\mathbb{Z}/4\mathbb{Z}$ und $([b]_{131})^2 = [20]_{131}$ in $\mathbb{Z}/131\mathbb{Z}$.

  Es gibt zwei Lösungen für $[a]_4$: $[0]_4, [2]_4$.
  $\mathbb{Z}/131\mathbb{Z}$ ist ein Körper und wegen $1 \neq -1$ gibt es genau zwei oder keine Lösung für $[b]_{131}$.
  Es ist $\left(\frac{20}{131}\right) = \left(\frac{2^2}{131}\right) \cdot \left(\frac{5}{131}\right) = \left(\frac{5}{131}\right) \overset{QRG}{=} \left(\frac{131}{5}\right) \cdot (-1)^{\frac{131-1}{2} \cdot \frac{5-1}{2}} = \left(\frac{131}{5}\right) = \left(\frac{1}{5}\right) = 1$.
  Also ist 20 ein Quadrat modulo 131 und es gibt wie oben gesehen zwei Lösungen für $[b]_{131}$.

  Insgesamt gibt es vier Lösungspaare $([a]_4, [b]_{131})$ in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/131\mathbb{Z}$, also auch vier Lösungen der Gleichung $x^2 = 20$ in R.
- Analoge Überlegungen stellen wir für die Gleichung $y^2 = 443$ an, stellen aber schnell fest, dass $443 \equiv 3$ kein Quadrat modulo 4 ist. Also gibt es keine Lösung von $y^2 = 443$.

Aufgabe 3 (4 Punkte)
Seien p, q zwei ungerade Primzahlen mit $p = q + 9a$ für ein $a \in \mathbb{Z}$. Zeige die folgenden Aussagen:

a) $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$ und $\left(\frac{-q}{p}\right) = \left(\frac{a}{p}\right)$.

b) Für $a \equiv 0$ modulo 4 gilt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

c) Finde einen Zusammenhang zwischen den Legendresymbolen $\left(\frac{a}{p}\right)$, $\left(\frac{a}{q}\right)$ für $a \equiv 2$ modulo 4.
(*Hinweis*: Der Zusammenhang ist abhängig von p.)

Lösung: Vorüberlegung: Ist $p = 3$, so gilt $3|p - 9a = q$, also $q = 3$, $a = 0$, und analog für $q = 3$ gilt $p = 3$, $a = 0$. Gilt aber $p = q = 3, a = 0$, so sind a) und b) offensichtlich erfüllt und die Voraussetzungen an c) nicht gegeben.
Ohne Einschränkung sei in dieser Aufgabe stets $p, q \neq 3$.

a) $\left(\frac{p}{q}\right) = \left(\frac{q+9a}{q}\right) = \left(\frac{9a}{q}\right) = \left(\frac{9}{q}\right) \cdot \left(\frac{a}{q}\right) = 1 \cdot \left(\frac{a}{q}\right)$, denn $9 = 3^2$ ist Quadrat modulo q, aber nicht 0 modulo q.
Analog gilt $\left(\frac{-q}{p}\right) = \left(\frac{9a-p}{p}\right) = \left(\frac{9a}{p}\right) = \left(\frac{9}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$.

b) Wegen $4|a$ folgt $4|9a = p - q$, also $p \equiv q$ modulo 4.
Im **Fall 1** ist $p \equiv q \equiv 1$ modulo 4, $\frac{p-1}{2}$ und $\frac{q-1}{2}$ beide gerade.
Im **Fall 2** ist $p \equiv q \equiv 3$ modulo 4, $\frac{p-1}{2}$ und $\frac{q-1}{2}$ beide ungerade.

Nach a) müssen wir zeigen, dass $\left(\frac{a}{q}\right) = \left(\frac{p}{q}\right) \overset{(!)}{=} \left(\frac{-q}{p}\right) = \left(\frac{a}{p}\right)$. Mit dem ersten Erweiterungssatz und dem quadratischen Reziprozitätsgesetz gilt:
$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
Im Fall 1 ist $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$, im Fall 2 ist $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$. In beiden Fällen ist $(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$ und damit die geforderte Gleichheit gezeigt.

c) Wegen $a \equiv 2$ modulo 4, ist auch $p - q = 9a \equiv 2$ modulo 4, also ist insbesondere genau einer der Faktoren $\frac{p-1}{2}, \frac{q-1}{2}$ gerade. $(*)$

Wieder reicht es $\left(\frac{a}{q}\right) = \left(\frac{p}{q}\right)$ und $\left(\frac{a}{p}\right) = \left(\frac{-q}{p}\right)$ zu vergleichen und wie in b) gilt
$\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) \overset{(*)}{=} (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)$.
Wir erhalten die Bedingung $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, falls $p \equiv 1$ modulo 4 und $\left(\frac{a}{q}\right) = -\left(\frac{a}{p}\right)$, falls $p \equiv 3$ modulo 4.

Aufgabe 4 (4 Punkte)
In dieser Aufgabe zeigen wir, dass für eine Primzahl $p \in \mathbb{P}$ das Polynom $\Phi_p(X) := \frac{X^p-1}{X-1} \in \mathbb{Z}[X]$ irreduzibel in $\mathbb{Q}[X]$ ist.

a) Zunächst zeigen wir folgenden Spezialfall des „Lemmas von Gauß“:
Sei $f \in \mathbb{Z}[X]$ normiert und irreduzibel in $\mathbb{Z}[X]$. Dann ist f auch irreduzibel in $\mathbb{Q}[X]$.
(*Hinweis:* Den größten gemeinsamen Teiler der Koeffizienten eines Polynoms $f \in \mathbb{Z}[X]$ bezeichnen wir als *Inhalt* $\mathrm{Inh}(f)$. Du darfst ohne Rechnung benutzen, dass der *Inhalt* multiplikativ ist, dass also $f = g \cdot h \Rightarrow \mathrm{Inh}(f) = \mathrm{Inh}(g) \cdot \mathrm{Inh}(h)$ gilt.)

b) Zeige nun, dass Φ_p irreduzibel über $\mathbb{Q}[X]$ ist.
(*Hinweis:* Betrachte $\Phi_p(X + 1)$ und erinnere dich an eine alte Übungsaufgabe.)

Nächste Woche lernen wir Φ_p als p-tes *Kreisteilungspolynom* kennen.

Lösung:

a) Sei f reduzibel über $\mathbb{Q}$, etwa $f = gh$ mit $\mathrm{grad}(g)$, $\mathrm{grad}(h)$ jeweils > 1.
Es gibt ein $N \in \mathbb{N}$ (z.B. der Hauptnenner aller Koeffizienten von g), so dass $gN \in \mathbb{Z}[X]$. Dann ist $g' := \frac{gN}{\mathrm{Inh}(gN)}$ ein primitives Polynom in $\mathbb{Z}[X]$ und es gilt $f = gh = g'h'$ mit $h' = \frac{h \cdot \mathrm{Inh}(gN)}{N} \in \mathbb{Q}[X]$.
Es gibt $M \in \mathbb{N}$ (z.B. der Hauptnenner aller Koeffizienten von h'), so dass $Mh' \in \mathbb{Z}[X]$. Dann ist $Mf = g'(Mh')$ ein Produkt von Polynomen in $\mathbb{Z}[X]$.
Wegen der Multiplikativität der Inhalte und da f und g' primitiv sind (bei f folgt das aus der Normiertheit), gilt $\mathrm{Inh}(Mh') = \mathrm{Inh}(Mf) = M$, aber dann war $h' = \frac{Mh'}{M}$ bereits in $\mathbb{Z}[X]$, also $f = g'h'$ eine Zerlegung von f in $\mathbb{Z}[X]$, wobei wegen $\mathrm{grad}(g') = \mathrm{grad}(g)$, $\mathrm{grad}(h') = \mathrm{grad}(h)$ die Polynome g', h' keine Einheiten sind.

b) Ein Polynom $f(X) \in \mathbb{Z}[X]$ ist genau dann reduzibel über $\mathbb{Z}$, wenn $f(X + 1)$ reduzibel ist – klar, $f(X) = g(X)h(X) \Leftrightarrow f(X + 1) = g(X + 1)h(X + 1)$ und $g(X)$ bzw. $h(X)$ ist genau dann eine Einheit in $\mathbb{Z}[X]$ (also ± 1), wenn $g(X + 1)$ bzw. $h(X + 1)$ eine solche ist.
Also reicht es, zu zeigen, dass $\Phi_p(X + 1)$ irreduzibel ist:

$$\Phi_p(X+1) = \frac{(X+1)^p-1}{(X+1)-1} = \frac{(\sum_{i=0}^{p} \binom{p}{i} \cdot X^i) - 1}{X} = \frac{X^p + (\sum_{i=1}^{p-1} \binom{p}{i} \cdot X^i) + 1 - 1}{X} = X^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} \cdot X^{i-1}$$

Das ist ein Polynom mit Leitkoeffizient 1 und konstantem Term $\binom{p}{1} = p$.
Die anderen Koeffizienten sind von der Form $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, $i = 1, ..., p-1$. Die Primzahl p teilt den Zähler, aber wegen $i, p - i < p$ nicht den Nenner. Also ist p ein Teiler von $\binom{p}{i}$, denn p wird nicht weggekürzt.
Nach dem Eisensteinkriterium, das wir auf dem Übungsblatt 11 kennengelernt haben, ist $\Phi_p(X+1)$ irreduzibel über $\mathbb{Z}$.

Nachtrag zum Binomial-Koeffizienten:
Hiermit gleiche ich gerne den Hänger aus, den ich in der Übung bei der Frage hatte, wieso der Binomial-Koeffizient eine natürliche Zahl sei. Spaßeshalber sei hier die analytische Beweismethode aufgeführt.

Der Binomial-Koeffizient $\binom{n}{k} := \frac{n!}{k!(n-k)!}$, $0 \leq k \leq n$, ist eine natürliche Zahl für $k = 0$, $k = n$, denn dann ist $\binom{n}{k} = 1$.
Für $0 < k < n$ zeigen wir die Aussage induktiv nach n; der Induktionsanfang ist klar, für $n = 1$ gibt es nämlich gar kein anderes k. (Und wer das nicht mag, rechne es für $n = 2$ eben nach.)

Nebenrechnung: Für $0 < k < n$ ist $\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{(n-1-k)!k!} = ...$
(erweitern des ersten Bruchs mit k, erweitern des zweiten Bruchs mit $n - k$)
$... = \frac{k(n-1)!}{k!(n-k)!} + \frac{(n-k)(n-1)!}{(n-k)!k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$.
Mit der Induktionsvoraussetzung sehen wir, dass $\binom{n}{k}$ als Summe zweier natürlicher Zahlen wieder natürlich ist.

Das zeigt auch, dass wir die Binomial-Koeffizienten tatsächlich aus dem Pascal'schen Dreieck berechnen können, wie wir das gewohnt sind.

Die Aussage aus der Übung haben wir übrigens auch in der Vorlesung schon geglaubt, siehe Skript, Beweis von Hilfssatz 1.2.8. Auch in 2.5.7 haben wir mit dem Binomial-Koeffizienten gearbeitet und dessen Natürlichkeit bewiesen, nicht wahr?