Probestudium 2018
- Übungsblatt 1 -

Prof. Dr. Werner Bley
Dominik Bullach
Martin Hofer
Pascal Stucky

Aufgabe 1 (mittel)
Sei $m \in \mathbb{Z}$. Wir definieren für zwei ganze Zahlen a und b

$$a \equiv b \mod m \quad :\Longleftrightarrow \quad m \mid (a-b)\,.$$

Seien $a, b, c \in \mathbb{Z}$. Zeigen Sie:

(a) Es gilt $a \equiv b \mod m$ genau dann, wenn $b \equiv a \mod m$.

(b) Sei $a \equiv b \mod m$ und $b \equiv c \mod m$. Dann folgt $a \equiv c \mod m$.

Aufgabe 2 (einfach)
Bestimmen Sie alle $x \in \{0, ..., 8\}$, sodass

(a) $x \equiv 7 + 8 \mod 9$,

(b) $x \equiv 5 \cdot 6 \mod 9$,

(c) $5x \equiv 1 \mod 9$,

(d) $6x \equiv 0 \mod 9$,

(e) $x^2 \equiv 7 \mod 9$,

(f) $3x^2 + 6 \equiv 0 \mod 9$,

(g) $x \equiv 7^{2018} \mod 9$.

Aufgabe 3 (einfach)

(a) Berechnen Sie $(3 + 2i) \cdot (5 + 8i)$.

(b) Sei $z = x + yi \in \mathbb{C}$. Zeigen Sie: $z^{-1} = \frac{x - yi}{x^2 + y^2}$.

Aufgabe 4 (mittel)

(a) Berechnen Sie ρ^n für $n \in \mathbb{N}$ und $\rho = \frac{-1 + i\sqrt{3}}{2}$.

(b) Zeichnen Sie das Ergebnis in der Gaußschen Zahlenebene ein.

(c) Zeigen Sie, dass $C_3 = \{\rho, \rho^2, \rho^3\}$ mit der komplexen Multiplikation eine Gruppe bildet.

Aufgabe 5 (mittel)
Sei p eine Primzahl. Zeige $\sqrt{p} \notin \mathbb{Q}$.

Lösungsskizzen

Aufgabe 1

(a) Bei einer „genau dann, wenn“-Aussage sind zwei Richtungen zu zeigen. Für die eine Richtung können wir $a \equiv b \mod m$ als gegeben annehmen. In diesem Fall gilt $m \mid (a-b)$, d.h. es existiert eine ganze Zahl k, sodass

$$a - b = km$$

gilt. Damit erhalten wir

$$b - a = -(a-b) = -km\,,$$

d.h. $m \mid b-a$. Nach Definition bedeutet das $b \equiv a \mod m$.

Für die andere Richtung setzen wir $b \equiv a \mod m$ voraus und wollen nun zeigen, dass daraus $a \equiv b \mod m$ folgt. Der Beweis hierfür funktioniert genauso wie für die andere Richtung, wir müssen nur in der obigen Argumentation a und b vertauschen.

(b) Aus $a \equiv b \mod m$ folgt, dass es eine ganze Zahl k gibt, sodass $a - b = km$ gilt. Genauso erhalten wir aus $b \equiv c \mod m$ eine ganze Zahl l mit $b - c = lm$. Wir möchten nun prüfen ob $a \equiv c \mod m$ gilt, also ob m ein Teiler von $a - c$ ist. Hierfür betrachten wir

$$a - c = a - c + b - b = (a-b) + (b-c) = km + lm = (k+l)m\,.$$

Somit gilt $m \mid (a-c)$ und daher folgt $a \equiv c \mod m$.

Aufgabe 2

(a) $x = 6$.

(b) $x = 3$.

(c) Durch Ausprobieren erhalten wir $x = 2$. Dies ist das multiplikative Inverse von 5 beim Rechnen modulo 9, d.h. wenn wir modulo 9 durch 5 teilen wollen, müssen wir mit 2 multiplizieren.

(d) Ausprobieren liefert hier $x \in \{0, 3, 6\}$. Insbesondere folgt hier aus $xy = 0$ nicht automatisch $x = 0$ oder $y = 0$. Fasst man $6x$ als Polynom auf, so erkennt man hier, dass ein Polynom von Grad 1 modulo 9 mehr als eine Nullstelle haben kann, in diesem Fall drei Nullstellen.

(e) Wir finden durch ausprobieren $x \in \{4, 5\}$.

(f) Umstellen liefert $3x^2 \equiv -6 \equiv 3 \mod 9$. Man beachte, dass hier nicht durch 3 geteilt werden darf. Nun kann man erneut die Werte ausprobieren und erhält $x \in \{1, 2, 4, 5, 7, 8\}$. Auch hier sehen wir, dass ein Polynom von Grad 2 modulo 9 sechs verschiedene Nullstellen haben kann.

(g) **Möglichkeit 1**: Wir berechnen zunächst einige Potenzen von 7 modulo 9:

$$\begin{aligned}
7^1 &\equiv 7 \mod 9\,,\\
7^2 &\equiv 49 \equiv 4 \mod 9\,,\\
7^3 &\equiv 7 \cdot 7^2 \equiv 7 \cdot 4 \equiv 28 \equiv 1 \mod 9\,,\\
7^4 &\equiv 7 \cdot 7^3 \equiv 7 \cdot 1 \equiv 7 \mod 9\,,\\
&\vdots
\end{aligned}$$

Man erkennt hier ein Muster, das sich nach drei Schritten wiederholt. Insbesondere gilt also $7^n \equiv 7 \mod 9$ für $n = 1, 4, 7, 10, ...$, $7^n \equiv 4 \mod 9$ für $n = 2, 5, 8, 11, ...$ und $7^n \equiv 1 \mod 9$ für $n = 3, 6, 9, 12, ...$ Da 2016 durch 3 teilbar ist (die Quersumme ist durch 3 teilbar), folgt also $7^{2016} \equiv 1 \mod 9$ und damit erhalten wir

$$7^{2018} \equiv 7^2 \cdot 7^{2016} \equiv 4 \cdot 1 \equiv 4 \mod 9\,.$$

Möglichkeit 2 Wir haben $7^2 = 49 \equiv 4 \mod 9$, daher gilt

$$7^{2018} = (7^2)^{1009} \equiv 4^{1009} \mod 9.$$

Leider ist 1009 eine Primzahl, daher können wir den gleichen Trick nicht nochmal anwenden. Jedoch ist

$$4^{1009} = 4 \cdot 4^{1008}$$

und wir haben $1008 = 3 \cdot 336$. Es gilt

$$4^3 = 64 \equiv 1 \mod 9,$$

daher ist also

$$4^{1008} = (4^3)^{336} \equiv 1^{336} \equiv 1 \mod 9$$

und das Endergebnis lautet folglich

$$7^{2018} \equiv 4 \cdot 4^{1008} \equiv 4 \cdot 1 \equiv 4 \mod 9.$$

Aufgabe 3

(a) Wir berechnen

$$\begin{aligned}(3+2i)\cdot(5+8i) &= 3\cdot 5 + 3\cdot 8i + 2i\cdot 5 + 2i\cdot 8i \\ &= 15 + 24i + 10i - 16 \\ &= -1 + 34i\,.\end{aligned}$$

(b) **Möglichkeit 1**: Wir berechnen

$$\begin{aligned}z\cdot\frac{x-yi}{x^2+y^2} &= (x+yi)\cdot\frac{x-yi}{x^2+y^2} \\ &= \frac{(x+yi)(x-yi)}{x^2+y^2} \\ &= \frac{x^2-(yi)^2}{x^2+y^2} \\ &= \frac{x^2+y^2}{x^2+y^2} = 1\,.\end{aligned}$$

Da das Inverse von z eindeutig ist, folgt somit $z^{-1} = \frac{x-yi}{x^2+y^2}$.

Möglichkeit 2: Wir erweitern mit $(x-iy)$ und verwenden die 3. Binomische Formel:

$$\frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x-iy}{x^2-(iy)^2} = \frac{x-iy}{x^2+y^2}.$$

Aufgabe 4

(a) Wir erhalten

$$\begin{aligned}&\rho^1 = \frac{-1+i\sqrt{3}}{2}\,, \\ &\rho^2 = \left(\frac{-1+i\sqrt{3}}{2}\right)\cdot\left(\frac{-1+i\sqrt{3}}{2}\right) = \frac{(-1+i\sqrt{3})^2}{4} = \frac{1-2i\sqrt{3}-3}{4} = \frac{2(-1-i\sqrt{3})}{4} = \frac{-1-i\sqrt{3}}{2}\,, \\ &\rho^3 = \rho\cdot\rho^2 = \left(\frac{-1+i\sqrt{3}}{2}\right)\cdot\left(\frac{-1-i\sqrt{3}}{2}\right) = \frac{(-1+i\sqrt{3})(-1-i\sqrt{3})}{4} = \frac{1+3}{4} = 1\,, \\ &\rho^4 = \rho\cdot\rho^3 = \rho\cdot 1 = \rho\,, \\ &\quad\vdots\end{aligned}$$

Wie bei Aufgabe 2(g) erkennen wir ein Muster, dass sich nach drei Schritten wiederholt. Wir wollen nun dieses Muster formal ausdrücken.

Dafür stellen wir zunächst fest, dass $\rho^n = 1$ gilt, wenn n ein Vielfaches von 3 ist, d.h. falls $n = 3k$ für ein $k \in \mathbb{N}$ gilt.

Wenn nun die Potenz von ρ um 1 größer ist als ein Vielfaches von 3 (d.h. $n = 3k + 1$ für ein $k \in \mathbb{N}$), dann können wir

$$\rho^n = \rho^{3k+1} = \rho^{3k} \cdot \rho = 1 \cdot \rho = \rho$$

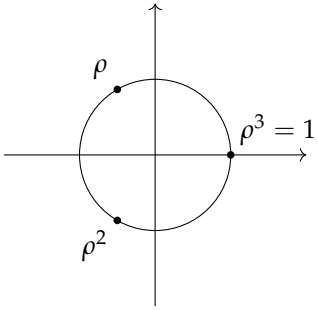
schreiben.

Falls die Potenz von ρ um 2 größer ist als ein Vielfaches von 3 (d. h. $n = 3k + 2$ für ein $k \in \mathbb{N}$), so erhalten wir analog zu obiger Überlegung $\rho^n = \rho^2$.

Jede natürliche Zahl n ist nun entweder ein Vielfaches von 3 oder ist entweder um 1 oder 2 größer. Mit den Überlegungen oben können wir also ρ^n für jede natürliche Zahl n ausdrücken:

$$\rho^n = \begin{cases} 1 & n \equiv 0 \mod 3, \\ \rho & n \equiv 1 \mod 3, \\ \rho^2 & n \equiv 2 \mod 3. \end{cases}$$

(b) Wir erhalten das folgende Bild:



Man erkennt, dass die Punkte alle auf dem Einheitskreis liegen und der Kreis durch die Punkte gedrittelt wird.

(c) Es ist $\rho^3 = 1$ und es gilt $1 \cdot z = z$ für alle $z \in \mathbb{C}$, also insbesondere auch für die Elemente von C_3, d. h. ρ^3 ist ein neutrales Element in C_3.

Die komplexe Multiplikation auf $\mathbb{C}$ ist assoziativ, also ist insbesondere auch die komplexe Multiplikation auf C_3 assoziativ. Das gleiche Argument zeigt, dass Multiplikation auf C_3 kommutativ ist.

Man prüft nun leicht folgende Verknüpfungstabelle nach:

$\cdot$	ρ	ρ^2	ρ^3
ρ	ρ^2	ρ^3	ρ
ρ^2	ρ^3	ρ	ρ^2
ρ^3	ρ	ρ^2	ρ^3

Daran kann man ablesen:

- Alle Einträge liegen wieder in C_3, d. h. C_3 ist bezüglich Multiplikation abgeschlossen.
- In jeder Zeile taucht das neutrale Element ρ^3 auf, sodass jedes Element ein Inverses besitzt. Genauer:

$$\begin{aligned} \rho^{-1} &= \rho^2 \,, \\ (\rho^2)^{-1} &= \rho \,, \\ (\rho^3)^{-1} &= \rho^3 \,. \end{aligned}$$

Insgesamt bildet die Menge C_3 also mit der komplexen Multiplikation eine abelsche Gruppe.

Aufgabe 5

Um diese Aussage zu zeigen, führen wir einen Widerspruchsbeweis. Damit ist Folgendes gemeint: Wir nehmen spaßeshalber an, die Aussage wäre falsch und betrachten die Konsequenzen dieser Annahme, bis wir auf einen Widerspruch stoßen. Daraus schließen wir dann, dass die Annahme falsch gewesen sein muss.

Ergo: Die Aussage ist wahr.

In diesem Fall nehmen wir also an, dass es eine Primzahl p gibt, für die $\sqrt{p} \in \mathbb{Q}$ erfüllt ist. Dies bedeutet, dass sich $\sqrt{p}$ als Bruch darstellen lassen muss. Wir finden also ganze Zahlen $a, b \in \mathbb{Z}$ mit

$$\sqrt{p} = \frac{a}{b}, \tag{$*$}$$

wobei natürlich $b \neq 0$ gelten muss. Außerdem dürfen wir voraussetzen, dass $\frac{a}{b}$ ein vollständig gekürzter Bruch ist. Letzteres heißt, dass a und b keinen gemeinsamen Primteiler besitzen.

Quadrieren wir die Gleichung $(*)$, so erhalten wir

$$p = \frac{a^2}{b^2} \quad \Leftrightarrow \quad b^2 \cdot p = a^2$$

als Ergebnis. Daraus lesen wir ab, dass $p \mid a^2$. Dies kann nur erfüllt sein, falls bereits $p \mid a$. Also gibt es ein $c \in \mathbb{Z}$ mit $a = c \cdot p$ und Einsetzen in die Gleichung oben beschert uns

$$b^2 \cdot p = c^2 \cdot p^2 \quad \Leftrightarrow \quad b^2 = c^2 \cdot p.$$

Der gewiefte Mathematiker wittert hier bereits den Widerspruch: Die Gleichung oben impliziert $p \mid b$, womit p sowohl b als auch a teilt. Dies widerspricht aber unserer Forderung der Teilerfremdheit an a und b.

Somit sind wir hier auf einen Widerspruch gestoßen und unsere Annahme $\sqrt{p} \in \mathbb{Q}$ muss falsch gewesen sein. Die logische Konsequenz ist nun $\sqrt{p} \notin \mathbb{Q}$.