

Diskrete Mathematik

Übungsblatt 9

Aufgabe 1. a) Mit Ausnahme von 3 ist jede Primzahl von der Form $3n + 1$ oder $3n - 1$. Überlegen Sie, dass eine Zahl der Form $3n - 1$ immer einen Primteiler der Form $3n - 1$ hat und variieren Sie nun den Beweis von Euklid, um zu zeigen, dass es unendlich viele Primzahlen der Form $3n - 1$ gibt.

b) Mit Ausnahme von 2 ist jede Primzahl von der Form $4n + 1$ oder $4n - 1$. Überlegen Sie, dass eine Zahl der Form $4n - 1$ immer einen Primteiler der Form $4n - 1$ hat und variieren Sie den Beweis von Euklid, um zu zeigen, dass es unendlich viele Primzahlen der Form $4n - 1$ gibt.

(Nur so am Rande: Was schätzen Sie, wieviele Primzahlen der Form $3n - 1$ es ungefähr zwischen 1 und x gibt, wenn x sehr groß ist?)

Aufgabe 2. a) Stellen Sie die Multiplikationstafel von $(\mathbb{Z}/12\mathbb{Z})^*$ auf. Wie haben wir diese Gruppe auf Blatt 7 genannt?

b) Berechnen Sie $7^{350} \pmod{15}$ und $2^{1000} \pmod{15}$.

c) Lösen Sie die Gleichung $83x = 3$ in $\mathbb{Z}/119\mathbb{Z}$.

Aufgabe 3. a) Sei K ein Körper. Zeigen Sie, dass die Gleichung $x^2 = 1$ in K genau die Lösungen 1 und -1 hat. (Tip: 3. Binomische Formel und Nullteilerfreiheit von K). Sei nun p eine Primzahl. Welche Elemente $x \in (\mathbb{Z}/p\mathbb{Z})^*$ sind also selbstinvers, d.h. erfüllen $x = x^{-1}$?

b) Zeigen Sie: Ist $p \neq 2$ eine Primzahl, so gilt $(p - 1)! \equiv 1 \pmod{p}$.

(Tip: $(p - 1)!$ ist das Produkt über alle Elemente in $(\mathbb{Z}/p\mathbb{Z})^*$. Fassen Sie die Elemente $\{x, x^{-1}\}$ zusammen und unterscheiden Sie die Fälle, dass diese Menge ein oder zwei Elemente hat.)

c) Zeigen Sie: Ist n keine Primzahl, so ist $(n - 1)! \not\equiv -1 \pmod{n}$.

(Tip: Überlegen Sie zunächst, dass $(n - 1)! \equiv 0 \pmod{p}$ für einen Primfaktor p von n gilt.)

Bemerkung: Aus den Teilen b) und c) folgt ein für theoretische Zwecke nützliches Primzahlkriterium - das Kriterium von Wilson -, das jedoch wegen des großen Rechenaufwandes leider vollkommen unpraktikabel ist.

Aufgabe 4. Der an sich sehr fromme Mathematiker Leonhard Euler kam eines Nachts in die Situation, mit dem Teufel ein Spiel spielen zu müssen. Euler holte ein Säckchen mit Bohnen und stellte 23 Becher im Kreis auf, 22 weiße und einen schwarzen. In letzteren legte er eine Bohne. Die

Spielregel war nun folgende:

Der erste Spieler nehme eine Bohne und gebe sie in den Becher links neben den schwarzen. Der zweite Spieler nehme 2 Bohnen und gebe nacheinander je eine in die links anschließenden beiden Becher. Dann nehme der erste Spieler 4 Bohnen und lege nacheinander je eine in die links anschließenden 4 Becher usw. Jeder Spieler nehme also, wenn er an der Reihe ist, so viele Bohnen, wie sich bereits in allen Bechern zusammen befinden, und lege, anschließenden an den zuletzt "bedienten" Becher, in die folgenden Becher im Kreis herum immer je eine Bohne. Verloren hat derjenige Spieler, der die *letzte* der Bohnen, die er diesmal zu verteilen hat, in den schwarzen Becher gibt. Der Teufel begann.

Hatte das Spiel überhaupt ein Ende? Wer gewann (gegebenenfalls)?

Abgabe am Montag, dem 3. Januar, bis 14.00 Uhr in die Zettelkästen im Emmy-Noether-Raum.