Matheschülerzirkel
Universität Augsburg
Schuljahr 2013/2014
Klasse 11./12., Gruppe 2

Zirkelzettel vom 15. März 2014

Zahlentheoretische Grundlagen

Ein *Ring* ist eine algebraische Struktur mit einer Addition und Multiplikation, die mit der gewöhnlichen Addition und Multiplikation von ganzen Zahlen zu tun haben können, aber nicht unbedingt müssen. Von einem Ring fordert man die folgenden Axiome:

$$\begin{aligned} 0 + x = x &= x + 0 \\ x + y &= y + x \\ x + (y + z) &= (x + y) + z \end{aligned}$$

$$\begin{aligned} 1 \cdot x = x &= x \cdot 1 \\ x \cdot y &= y \cdot x \\ x \cdot (y \cdot z) &= (x \cdot y) \cdot z \end{aligned}$$

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z \\ (x + y) \cdot z &= x \cdot z + y \cdot z \end{aligned}$$

Dabei bezeichnen die Symbole „0“ und „1“ zwei besondere Elemente des Rings, nicht unbedingt die bekannten Zahlen Null und Eins. Man nennt sie wegen ihrer besonderen Bedeutung *Null-* und *Einselement*. Ein weiteres Axiom besagt, dass es zu jedem Element x ein weiteres Element geben soll, bezeichnet $-x$, das bezüglich der Addition invers zu x ist:

$$x + (-x) = 0 = (-x) + x.$$

Weitere Axiome fordert man von Ringen nicht.

Aufgabe 1. *Beispiele und Nichtbeispiele für Ringe*

Mache dir klar:

a) Die rationalen Zahlen bilden bezüglich der gewöhnlichen Addition und Multiplikation einen Ring.

b) Die ganzen Zahlen bilden bezüglich der gewöhnlichen Addition und Multiplikation einen Ring.

c) Die natürlichen Zahlen bilden bezüglich der gewöhnlichen Addition und Multiplikation *keinen* Ring.

d) Die ganzen Zahlen bilden *keinen* Ring, wenn man als Addition paradoxerweise die Subtraktion und als Multiplikation die übliche Multiplikation nimmt.

Für die Kryptographie gehören die *Restklassenringe* zu den wichtigsten Ringen.

Aufgabe 2. *Restklassenarithmetik*

Sei m eine feste positive Zahl. Dann besteht der *Restklassenring* $\mathbb{Z}/(m)$ (oft auch „$\mathbb{Z}_m$“ geschrieben) aus den verschiedenen Resten, die bei Division durch m auftreten können:

$$\mathbb{Z}/(m) = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Wenn man faul ist, lässt man die Oberstriche auch weg. In $\mathbb{Z}/(m)$ addiert und multipliziert man fast wie gewohnt – nur dass man nach jedem Rechenschritt die Ergebnisse *modulo* m vereinfachen kann.

a) Überzeuge dich davon, dass in $\mathbb{Z}/(6)$ folgende Rechnung stimmt:

$$\overline{4} + \overline{7} = \overline{11} = \overline{5}.$$

b) Ergänze unten stehende Tabellen für die Addition und Multiplikation in $\mathbb{Z}/(4)$.

c) Ein Element x eines Rings heißt genau dann *invertierbar*, wenn es ein weiteres Element y mit der Eigenschaft $xy = 1$ gibt. Das Element y heißt dann auch *Inverses* von x. Welche Elemente von $\mathbb{Z}/(4)$ sind invertierbar?

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	
$\overline{1}$				
$\overline{2}$				
$\overline{3}$			$\overline{1}$	

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	
$\overline{1}$				
$\overline{2}$				
$\overline{3}$			$\overline{2}$	

Aufgabe 3. *Falsche binomische Formel*

Für ganze Zahlen x, y gilt bekanntermaßen die *binomische Formel*:

$$(x + y)^2 = x^2 + 2xy + y^2.$$

a) Beweise diese Formel rechnerisch.

b) Gib einen geometrischen Beweis, der etwas mit Quadraten der Seitenlängen x und y zu tun hat.

c) Beweise, dass die binomische Formel sogar in jedem Ring gilt. Dabei ist allgemein „a^2“ eine Abkürzung für $a \cdot a$ und „2“ eine Abkürzung für $1 + 1$ (was auch immer das in dem untersuchten Ring ergeben mag).

d) Beweise, dass im Ring $\mathbb{Z}/(2)$ außerdem die sogenannte *falsche binomische Formel* gilt:

$$(x + y)^2 = x^2 + y^2.$$

e) Wenn du aus der Informatik die logischen Gatter (wie UND, ODER, ...) kennst, interessiert dich vielleicht folgende Frage: Was haben die Addition und die Multiplikation von $\mathbb{Z}/(2)$ mit den logischen Gattern zu tun?

Aufgabe 4. *Euklidischer Algorithmus*

Eines der ältesten überlieferten numerischen Verfahren ist der *euklidische Algorithmus*. Mit seiner Hilfe kann man auf effiziente Art und Weise den größten gemeinsamen Teiler zweier ganzer Zahlen bestimmen – viel schneller, als wenn man erst die Zahlen in Primfaktoren zerlegen würde.

$$\begin{aligned}
42 &= 1 \cdot 26 + 16 \\
26 &= 1 \cdot 16 + 10 \\
16 &= 1 \cdot 10 + 6 \\
10 &= 1 \cdot 6 + 4 \\
6 &= 1 \cdot 4 + 2 \\
4 &= 2 \cdot 2 + 0
\end{aligned}$$

a) In diesem Beispiel wurde der euklidische Algorithmus verwendet, um den größten gemeinsamen Teiler von 42 und 26 zu ermitteln (dieser ist 2). Erschließe, wie das Verfahren funktioniert.

b) Bestimme mit dem euklidischen Algorithmus den größten gemeinsamen Teiler zweier Zahlen deiner Wahl.

c) Das Verfahren hört dann auf, wenn als Rest 0 auftritt. Erkläre, wieso das unabhängig von den Anfangszahlen stets nach endlich vielen Schritten der Fall ist! (Man sagt, dass der euklidische Algorithmus *terminiert*.)

d) Mit dem Algorithmus kann man durch *Rückwärtsauflösen* den größten gemeinsamen Teiler d zweier ganzer Zahlen x und y in der Form $d = ax+by$ für gewisse Hilfszahlen a und b schreiben. Versuche das in obigem Beispiel!

Eine Darstellung der Form $d = ax + by$ des größten gemeinsamen Teilers heißt auch *Bézoutdarstellung*. Es ist etwas sehr besonderes, dass es im Ring der ganzen Zahlen eine solche immer gibt.

Aufgabe 5. *Invertierbarkeit in Restklassenringen*

In den Restklassenringen ist nicht jedes Element invertierbar, das haben wir schon beim Beispiel mit $\mathbb{Z}/(4)$ gesehen. Es gilt folgende Regel: Ein Element $\overline{a}$ von $\mathbb{Z}/(m)$ ist genau dann invertierbar, wenn die Zahlen a und m zueinander teilerfremd sind.

a) Bestätige diese Regel im Beispiel $\mathbb{Z}/(4)$.

b) Erkläre, wie man den euklidischen Algorithmus verwenden kann, um in $\mathbb{Z}/(m)$ Inverse zu berechnen!

c) Welche Elemente sind in $\mathbb{Z}/(p)$ invertierbar, wenn p eine Primzahl ist?

Aufgabe 6. *Eulersche Phi-Funktion*

Die Anzahl der in $\mathbb{Z}/(m)$ invertierbaren Elemente schreibt man auch „$\Phi(m)$“. Sei im Folgenden p eine beliebige Primzahl.

a) Zeige: $\Phi(p) = p - 1$.

b) Zeige: $\Phi(p^2) = p^2 - p$.

c) Was ist $\Phi(p^3)$?

d) Was ist $\Phi(p^n)$?

Später werden wir verstehen, dass für teilerfremde Zahlen a, b die Rechenregel

$$\Phi(ab) = \Phi(a) \cdot \Phi(b)$$

gilt. Damit kann man die Werte der eulerschen Phi-Funktion recht effizient berechnen.