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

Zirkelzettel vom 15. März 2014 und 29. 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:

$$0 + x = x = x + 0$$
$$x + y = y + x$$
$$x + (y + z) = (x + y) + z$$

$$1 \cdot x = x = x \cdot 1$$
$$x \cdot y = y \cdot x$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(x + y) \cdot z = x \cdot z + y \cdot z$$

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.

Kryptographische Verfahren

Aufgabe 7. *Eine Analogie für symmetrische Verschlüsselung*

Alice möchte Bob ein Paket per Post schicken, sie misstraut aber dem Postsystem. Daher versieht sie das Paket mit einem Vorhängeschloss, zu dem Alice und Bob beide Schlüssel besitzen.

a) Gegen welche Angriffe schützt dieses Verfahren?

b) Wo liegen seine Nachteile?

c) Was passiert, wenn Alice und Bob auf diese Weise weiter kommunizieren, Bob aber auf seinen Schlüssel nicht gut aufpasst?

d) Welche Nachteile treten auf, wenn mehrere Freunde mit diesem Verfahren sicher kommunizieren möchten?

Aufgabe 8. *Eine Analogie für asymmetrische Verschlüsselung*

Alice möchte wieder Bob ein Paket per Post schicken. Dazu versieht sie diesmal das Paket mit einem Vorhängeschloss, zu dem nur Bob den Schlüssel hat.

a) Gegen welche Angriffe schützt dieses Verfahren?

b) Welchen fundamentalen Vorteil hat dieses Verfahren gegenüber symmetrischer Verschlüsselung?

c) Wo liegen seine Nachteile?

Aufgabe 9. *Eine Analogie für ein Drei-Durchgänge-Protokoll*

Alice möchte abermals Bob ein Paket per Post schicken. Sie haben jedoch vorher keinerlei Schlösser oder Schlüssel ausgetauscht.

a) Überlege dir ein dreischrittiges Verfahren, das in diesem Fall angewendet werden kann!

b) Gegen welche Angriffe ist es sicher, gegen welche nicht?

Aufgabe 10. *Ein unsicheres Drei-Durchgänge-Protokoll: XOR*

Sind m_1 und m_2 zwei gleich lange Texte, so wollen wir mit „$m_1 \oplus m_2$“ denjenigen Text bezeichnen, den man erhält, wenn man von den einzelnen (ASCII- oder UTF-8-)Zeichen bitweise das *exklusive Oder* (XOR) nimmt. Ein Beispiel:

```
Text 1: "abc", in Bits: 01100001 01100010 01100011
Text 2: "0AZ", in Bits: 00110000 01000001 01011010
XOR:    "Q#9", in Bits: 01010001 00100011 00111001
```

a) Erkläre, wie die XOR-Verknüpfung funktioniert!

Alice möchte an Bob einen Text m schicken. Alice und Bob haben vorher nie miteinander kommuniziert und insbesondere keine gemeinsamen Schlüssel ausgemacht. Mit der XOR-Verknüpfung kann man trotzdem ein geeignetes kryptographisches Verfahren beschreiben:

1. Alice generiert einen zufälligen Schlüssel s_1, der genau so lang ist wie m. Sie schickt über eine unsichere Leitung an Bob die kodierte Nachricht $c := m \oplus s_1$.
2. Bob generiert seinerseits einen zufälligen Schlüssel s_2 gleicher Länge. Er schickt über eine unsichere Leitung an Alice die Nachricht $c' := c \oplus s_2$.
3. Alice übermittelt $c'' := c' \oplus s_1$ an Bob. Dann ist $c'' \oplus s_2$ gleich m, Bob kann also die geheime Nachricht lesen.

b) Erkläre, wieso das Verfahren überhaupt funktioniert, wieso also $c'' \oplus s_2 = m$ gilt.

c) Das Verfahren hat eine große Schwachstelle: Ein Mithörer kann sich ebenfalls den Inhalt von m erschließen. Erkläre, wie das geht!

d) Welche weiteren Nachteile hat das Verfahren?

Aufgabe 11. *Das RSA-Verfahren*

Das RSA-Verfahren ist eines der bekanntesten asymmetrischen Verschlüsselungsverfahren. Die Originalvariante ist unsicher, aber leichte Verbesserungen gelten als sicher – zumindest werden sie weltweit täglich eingesetzt.

Schlüsselpaarerzeugung. Wähle zufällig zwei verschiedene Primzahlen p und q und berechne ihr Produkt: $m := pq$ (der *Modulus*). Wähle zufällig eine zu $(p-1)\cdot(q-1)$ teilerfremde Zahl e. Berechne eine Zahl d, sodass $\overline{d}$ im Restklassenring $\mathbb{Z}/((p-1)(q-1))$ invers zu $\overline{e}$ ist.

Die Zahlen e und m bilden dann gemeinsam den *öffentlichen Schlüssel*, die Zahlen d und m den *privaten Schlüssel*.

Verschlüsselung. Die Verschlüsselung einer Nachricht k (die als Zahl ausgedrückt sein muss) ist die Restklasse $c := \overline{k}^e \in \mathbb{Z}/(m)$.

Entschlüsselung. Die Entschlüsselung eines Chiffrats c ist die Restklasse $c^d \in \mathbb{Z}/(m)$.

a) Wie kann man beim Schlüsselpaarerzeugungsschritt die Zahl d bestimmen? Wieso ist das immer möglich?

b) Wie kann man eine zu verschlüsselnde Nachricht als Zahl darstellen? Wieso muss man darauf achten, dass die resultierende Zahl kleiner als m ist? Was kann man machen, wenn die Zahl leider doch größer oder gleich m ist?

c) Beweise, dass das Verfahren funktioniert – beweise also, dass die Entschlüsselung der Verschlüsselung einer Restklasse $k \in \mathbb{Z}/(m)$ wieder dieselbe Restklasse k ergibt.

Verwende dazu den *Satz von Euler*: Sind a und m teilerfremde Zahlen, so gilt $\overline{a}^{\Phi(m)} = 1 \in \mathbb{Z}/(m)$. (Vielleicht beweisen wir diesen Satz später noch.) Zur Vereinfachung kannst du in deinem Beweis annehmen, dass k zu m teilerfremd ist.

d) Worauf basiert die Sicherheit des Verfahrens? Was müsste man können, um ohne Kenntnis des privaten Schlüssels aus einem Chiffrat k^e auf den Klartext k schließen zu können?

e) Wenn der öffentliche Schlüssel e und der Zahlenwert des Klartextes k „klein“ sind, ist das Verfahren unsicher. Begründe das!

f) Wenn m klein ist (etwa kleiner oder gleich der Anzahl der verschiedenen denkbaren Buchstaben), degradiert das RSA-Verfahren zu einer monoalphabetischen Verschlüsselung. Begründe das!