Einführung in die Algebra und Diskrete Mathematik
Zweite Hoffnungsklausur, 07.10.2015
Musterlösung

Aufgabe 1 Wie viele (bezüglich der Multiplikation) invertierbare Elemente gibt es im Restklassenring $\mathbb{Z}_{600}$? Geben Sie konkret ein invertierbares Element ungleich 1 an und begründen Sie Ihre Wahl! (*3 Punkte*)

Lösung. Nach Definition der Eulerschen Phifunktion ist diese Anzahl gegeben durch

$$\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 600 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 160.$$

Ein invertierbares Element ist zum Beispiel 7, weil $\mathrm{ggT}(7, 600) = 1$. □

Aufgabe 2 Frau Obermayer sendet Herrn Unterberger den ersten Buchstaben ihres Vornamens als verschlüsselte Nachricht: 63. Herr Unterberger weiß, dass Frau Obermayer das RSA-Verfahren mit dem öffentlichen Schlüssel ($n = 65$, $e = 7$) verwendet hat ($A = 1$, $Z = 26$). Entschlüsseln Sie die Nachricht! Was hätte Frau Obermayer bei ihrer Verschlüssungsmethode anders machen müssen, damit ihre Botschaft nicht so leicht zu entschlüsseln gewesen wäre? (*6 Punkte*)

Lösung. Offenbar gilt $p = 13$ und $q = 5$, also $\phi = 12 \cdot 4 = 48$. Wir müssen nun das Inverse von $e = 7$ in $\mathbb{Z}_{48}$ finden. Zu lösen ist also die Kongruenz $7d \equiv 1 \pmod{48}$. Die Lösung $d = 7$ kann man entweder erraten oder mit dem Euklidischen Algorithmus ermitteln. Um nun den Klartext zu erhalten, muss die Potenz 63^7 modulo 65 berechnet werden. Am einfachsten geht das so:

$$63^7 \equiv (-2)^7 \equiv -128 \equiv 2 \pmod{65}.$$

Der Vorname von Frau Obermayer fängt also mit einem B an. Da n sehr einfach zu faktorisieren ist, ist ihre Verschlüsselung jedoch sehr unsicher, weshalb sie besser viel größere Primzahlen verwendet hätte, um den öffentlichen Schlüssel zu kreieren. □

Aufgabe 3 Wir betrachten die Menge $\mathbb{Z}[\sqrt{-7}] := \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}$. Wir definieren darauf folgende Operationen:

$$(a + b\sqrt{-7}) \oplus (c + d\sqrt{-7}) := (a + c) + (b + d)\sqrt{-7}$$
$$(a + b\sqrt{-7}) \odot (c + d\sqrt{-7}) := (ac - 7bd) + (ad + bc)\sqrt{-7}$$

1. Wie kann man begründen, dass $(\mathbb{Z}[\sqrt{-7}], \oplus, \odot)$ ein Integritätsbereich ist? (*1 Punkt*)

2. Zeigen Sie, dass $2 \in \mathbb{Z}[\sqrt{-7}]$ nicht prim ist. (*3 Punkte*)

3. Zeigen oder widerlegen Sie, dass $(\mathbb{Z}[\sqrt{-7}], \oplus, \odot)$ ein Körper ist. (*2 Punkte*)

Lösung. Das folgt im Wesentlichen daraus, dass $(\mathbb{Z}[\sqrt{-7}], \oplus, \odot)$ ein Unterring der komplexen Zahlen ist, die selbst einen Integritätsbereich bilden. Also kann es auch keine Nullteiler in $(\mathbb{Z}[\sqrt{-7}], \oplus, \odot)$ geben. Es gilt offenbar $2 \mid 8 = (1 + \sqrt{-7}) \odot (1 - \sqrt{-7})$. Wäre 2 prim, müsste daraus folgen, dass $2 \mid (1 + \sqrt{-7})$ oder $2 \mid (1 - \sqrt{-7})$. Aber keine der beiden Aussagen ist wahr. Somit ist 2 nicht prim. Außerdem ist 2 nicht invertierbar. Wäre nämlich 2 invertierbar, müsste es ein Element $c + d\sqrt{-7} \in \mathbb{Z}[\sqrt{-7}]$ geben mit $2(c + d\sqrt{-7}) = 1$. Das kann nur gelten, wenn $2c = 1$. Diese Gleichung ist in $\mathbb{Z}$ nicht lösbar, was den gewünschten Widerspruch liefert. Da wir somit ein nicht invertierbares Element gefunden haben, kann $\mathbb{Z}[\sqrt{-7}]$ kein Körper sein. □

Aufgabe 4 Ideale in Restklassenringe

1. Wir betrachten den Restklassenring $\mathbb{Z}_6$ und die Teilmenge $I = \{0, 2, 4\}$. Zeigen Sie, dass I ein Ideal von $\mathbb{Z}_6$ ist. (*3 Punkte*)

2. Geben Sie alle Ideale von $\mathbb{Z}_p$ an, wobei p eine Primzahl ist. Begründen Sie, warum es nicht noch andere Ideale geben kann. (*2 Punkte*)

Lösung. Bei a) müssen lediglich die drei Idealeigenschaften nachgerechnet werden. I ist offensichtlich nicht leer, Addition oder Subtraktion der Elemente in I führt nicht aus I heraus (man rechnet ja modulo 6), ebenso wenig die Multiplikation von Elementen in I mit irgendeinem Element in $\mathbb{Z}_6$. Da $\mathbb{Z}_p$ für primes p ein Körper und folglich ein einfacher Ring ist, gibt es in $\mathbb{Z}_p$ nur die trivialen Ideale $\{0\}$ und $\mathbb{Z}_p$. □