Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 12

Aufgabe 1 (3 Punkte)
Sei K ein Körper. Zeige, dass es in $K[X]$ unendlich viele Assoziiertenklassen irreduzibler Polynome gibt.

Aufgabe 2 (4 Punkte + 1 Zusatzpunkt)
Wir schreiben das Jahr 1973. Zwischen den benachbarten Staaten Gaußland und Euklidistan herrschen Spannungen, die jederzeit in einen Krieg münden können. Jedes der Länder ist darauf bedacht, möglichst viele Informationen aus dem anderen Land zu beschaffen, Spionage und das Anwenden von Verschlüsselungsverfahren werden bereits in der Schule gelehrt.
Dem gaußischen Geheimdienst KGV liegt eine geheime Botschaft aus Euklidistan vor. Leider können sie die Nachricht nicht lesen, wenn es ihnen nicht gelingt, den geheimen Schlüssel, die Mersenne-Zahl $M := M_{131} = 2^{131} - 1$, in Primfaktoren zu zerlegen.
Leider sind die Computer im Jahre 1973 noch lange nicht weit genug entwickelt, um diese Zahl auszurechnen und einen Brute-Force-Ansatz zu versuchen, die Spionage-Abteilung funktioniert dafür ausgezeichnet. Soeben erreicht die KGV-Zentrale folgender Hinweis ihres Mannes Gegétè Primanov: „habe neue Informationen über M – Primteiler kleiner als 787“
Dies wird nicht reichen, um die Zahl komplett zu faktorisieren, ist aber ein guter Anfang. Den gaußischen Agenten gelingt es, eine Vermutung für einen Primteiler p aufzustellen. Mit geeigneter Reduktion, die sie mit Papier und Stift oder ihren veralteten Taschenrechnern (die immerhin bereits einfache Subtraktionen und Multiplikationen durchführen können) ausführen können, gelingt es ihnen, tatsächlich nachzuweisen, dass p ein Faktor von M ist.

Aus sicherer Ferne wollen wir gerne nachvollziehen, was hier passiert ist. Mache das gleiche, was auch die Agenten gemacht haben! Stelle eine Vermutung auf, was p sein könnte, und beweise, dass p tatsächlich ein Primteiler von M ist.

Einen Zusatzpunkt erhältst du, wenn du den Krieg zwischen Gaußland und Euklidistan verhinderst und für Weltfrieden sorgst.[1]

Aufgabe 3 (4 Punkte) (*Dies ist wieder einmal eine alte Klausuraufgabe – zumindest fast.*)
Es sei $a \in \mathbb{Z}$ beliebig.

a) Zeige, dass es unendlich viele Primzahlen p gibt, sodass die Restklasse von a in $\mathbb{F}_p$ eine dritte Potenz ist.
Hinweis: Betrachte natürliche Zahlen der Form $x^3 - a$.

b) Finde für $a = 5$ zwei verschiedene Primzahlen > 25, die die Bedingung aus a) erfüllen.

In der Vorlesung waren arithmetische Funktionen ein Thema. Zu diesen findet man auf dieser Seite gar keine Aufgabe. Der schlaue Student schließt messerscharf, dass es eine Rückseite geben muss. Tatsächlich, dreh das Blatt doch einmal um.[2]

[1] Man könnte vermuten, der Übungsleiter habe einen Clown gefrühstückt. Das wird wohl so sein.
[2] Ja, hat er...

Aufgabe 4 (5 Punkte)
Sei $\mathcal{A}$ der Ring der arithmetischen Funktionen. Die eulersche φ-Funktion φ, die konstante Funktion $\eta \equiv 1$ und die kanonische Einbettung $\mathrm{Id}_{\mathbb{N}}$ sind Elemente aus $\mathcal{A}$. Zeige:

a) Die Menge aller multiplikativen arithmetischen Funktionen ist eine Untergruppe von $\mathcal{A}^\times$.

b) Es ist $\mathrm{Id}_{\mathbb{N}} = \eta * \varphi$.

(*Hinweis:* Es ist in a) relativ einfach zu zeigen, dass ein Untermonoid vorliegt. Um zu zeigen, dass die Inverse β einer arithmetischen multiplikativen Funktion (die Inverse existiert, nicht wahr?) selbst multiplikativ ist, könnte folgender Ansatz helfen: Es reicht zu zeigen (wieso?), dass $\beta(p^e \cdot m) = \beta(p^e) \cdot \beta(m)$ für alle $p \in \mathbb{P}$, $e \in \mathbb{N}_0$ und für alle zu p teilerfremden $m \in \mathbb{N}$ gilt. Diese Aussage kann etwa mit doppelter Induktion nach e und m bewiesen werden.
In b) genügt es, die Monoid-Eigenschaft aus a) zu kennen. Wieso reicht es, die Aussage für Primpotenzen zu beweisen?)

Sommerfest der Fakultät

Freitag, 13. Juli 2012

ab 17.30: Fußballturnier der Institute
abends gemütliches Beisammensein mit Musik und Grillen
mehr Infos unter
`http://www.math.kit.edu/event/sommerfest/de`

Abgabe bis Dienstag, 10. Juli, 9:40 Uhr im Abgabekasten, direkt vor der großen Übung um 9:45 Uhr oder auch vorher direkt bei deinem Übungsleiter.