Mathematik I, Logik und Algebra, WS2011/12
M. Hortmann

Blatt 11

bitte heften Sie dieses Blatt vor Ihre Aufgaben

Namen								**Gruppe**	**Tutor**
1a	b	2	3a	b	4a	b	c	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	1	6 Punkte=100%	

Aufgabe 1

a) Berechnen Sie mit Hilfe des erweiterten Euklidischen Algorithmus das multiplikativ inverse Element von 593 im Ring $\mathbb{Z}_{7031}$. Dokumentieren Sie alle Rechenschritte. Führen Sie auch eine Probe durch.

b) Man setze m=79, k=89. Damit ist n=mk=7031. Da ggT(m,k)=1, ist die Abbildung $\Phi:\mathbb{Z}_n\to\mathbb{Z}_m\times\mathbb{Z}_k$, die gegeben ist durch $x\mapsto(x\%m\,,x\%k)$ ein Ringisomorphismus.

Finden Sie mit Hilfe des erweiterten Euklidischen Algorithmus, wie in der Vorlesung gezeigt, Elemente $x\,,y\in\mathbb{Z}_n$ mit $\Phi(x)=(1,0)$ und $\Phi(y)=(0,1)$, und anschließend ein Element $z\in\mathbb{Z}_n$ mit $\Phi(z)=(57,58)$.

Aufgabe 2

Gegeben sei das Polynom $f=X^5+6X^4+6X^3+X^2+2X+5\ \in\ \mathbb{Z}_7[X]$. Finden Sie Elemente $a_1,\ldots,a_5\in\mathbb{Z}_7$ (die nicht notwendig alle verschieden sein müssen), so daß $f=(X-a_1)(X-a_2)(X-a_3)(X-a_4)(X-a_5)$.[1]

1 Die meisten Polynome in $\mathbb{Z}_7[X]$ lassen sich nicht so darstellen.

Aufgabe 3

a) Das Polynom $f = X^2 + 1 = 101$ ist irreduzibel in $\mathbb{Z}_3[X]$. Deshalb ist der Quotientenring $\mathbb{Z}_3[X]/<f>$ ein Körper. Wegen grad(f)=2 besitzt dieser Körper 9 Elemente, nämlich alle Polynome in $\mathbb{Z}_3[X]$ vom Grad kleiner 2. Berechnen Sie in diesem Körper die Additions- und Multiplikationstabelle, indem Sie alle Polynome vom Grad kleiner 2 addieren bzw. multiplizieren: falls dann das Resultat einen Grad größer als 1 besitzt, teilen Sie durch f und nehmen den Rest.

Füllen Sie also die folgenden Tabellen und dokumentieren Ihre Nebenrechnungen:

+	0	1	2	10	11	12	20	21	22
0									
1									
2									
10									
11									
12									
20									
21									
22									

*	1	2	10	11	12	20	21	22
1								
2								
10								
11								
12								
20								
21								
22								

Hinweis: die Erstellung der ersten Tabelle ist trivial.
Sehen Sie, daß die Additions- bzw. Multiplikationstafeln für $\mathbb{Z}_3$ in den obigen vorkommen?

b) Bestimmen Sie einen Erzeuger der multiplikativen Gruppe von K.

Aufgabe 4

Die Teilmenge der komplexen Zahlen mit ganzzahligem Real- und Imaginärteil bildet bezüglich der Addition und Multiplikation komplexer Zahlen einen Ring, den sogenannten Ring der Gaußschen Zahlen G.

Wichtig ist die sogenannte Normabbildung $N: G \to \mathbb{Z}$, die gegeben ist durch
$z = a + bi \mapsto a^2 + b^2 = z\bar{z}$.

a) Man rechne nach, daß $\forall z, w \in G$: $N(zw) = N(z)N(w)$.

b) Man erinnere sich an den Begriff der Einheit in einem Ring: Einheiten sind diejenigen Elemente, welche ein multiplikativ Inverses besitzen. Die Einheiten bilden eine Gruppe. Man zeige, daß die Einheitengruppe von G gleich $\{1, -1, i, -i\}$ ist.

c) Ähnlich wie in $\mathbb{Z}$ gibt es auch in G Primzahlen: $z \in G$ ist prim, wenn es sich nicht als Produkt von Nichteinheiten schreiben läßt. Man zeige, daß 3 Primzahl in G ist, 2 aber nicht.