Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 2

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen										**Gruppe**	**Tutor**
1a	b	c	d	eα	eβ	f	g	2a	b	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	1	1	1	8 Punkte=100%	

Aufgabe 1

Betrachten wir den Chinesischen Restesatz:
Sind $r, s \in N$ teilerfremd und $n=rs$, so ist die Abbildung $\mathbb{Z}_n \to \mathbb{Z}_r \times \mathbb{Z}_s$, $x \mapsto (x\,\%\,r, x\,\%\,s)$, ein Ringisomorphismus. Dies verallgemeinert sich sofort auf: Sind $r, s, t \in N$ paarweise teilerfremd und $n=rst$, so ist die Abbildung $\mathbb{Z}_n \to \mathbb{Z}_r \times \mathbb{Z}_s \times \mathbb{Z}_t$, $x \mapsto (x\,\%\,r, x\,\%\,s, x\,\%\,t)$, ein Ringisomorphismus. Hat man schließlich die Primfaktorzerlegung $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_N^{\alpha_N}$, so ist $\mathbb{Z}_n \to \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_N^{\alpha_N}}$, $x \mapsto (x\,\%\,p_1^{\alpha_1}, x\,\%\,p_2^{\alpha_2}, x\,\%\,p_N^{\alpha_N})$ ein Ringisomorphismus. Man sollte sich also für die Struktur der multiplikativen Gruppe der Ringe $\mathbb{Z}_{p^\alpha}$ interessieren.

Übrigens: Ein Element von $\mathbb{Z}_{p^\alpha}$ läßt sich im Ziffernsystem zur Basis p als α-stellige Zahl darstellen.

Sei im Folgenden p eine ungerade Primzahl und $\alpha \geq 1$.

a) Man berechne die Elementezahl $|\mathbb{Z}_{p^\alpha}^*|$
b) Beschreiben Sie, wie Sie in $|\mathbb{Z}_{p^\alpha}^*|$ eine (p-1)-elementige Untergruppe konstruieren. (Experimentieren Sie zunächst mit p=3 und $\alpha = 2,3,4$.)
c) Man finde in $|\mathbb{Z}_{p^4}^*|$ eine p-elementige, eine p^2-elementige und eine p^3-elementige Untergruppe.

d) Man setze voraus, daß die multiplikative Gruppe $\mathbb{Z}_p^*$ zyklisch ist und zeige, daß auch die multiplikative Gruppe $\mathbb{Z}_{p^\alpha}^*$ zyklisch ist. (Analysieren Sie zunächst den Fall $\alpha = 2$.)

e) Sei $n = p^\alpha \cdot m$, p eine ungerade Primzahl, $\alpha \geq 2$, m ebenfalls ungerade und m und p teilerfremd. Aus dem Chinesischen Restesatz und den vorigen Aufgabenteilen folgt, daß es in $\mathbb{Z}_n^*$ ein Element der Ordnung p gibt.

α) Zeigen Sie, daß *n* keine Carmichael-Zahl sein kann. (Eine Carmichael-Zahl ist also quadratfrei)
β) Finden Sie in $\mathbb{Z}_{525}^*$ ein Element der Ordnung 5 und führen Sie "per Hand" die Probe durch, daß es sich tatsächlich um ein Element der Ordnung 5 handelt.

f) *n* ist genau dann Carmichael-Zahl wenn für jeden Primteiler *p* von *n* gilt: *p*-1 ist Teiler von *n*-1. Benutzen Sie dies, um zu zeigen: Ist $m \in \mathbb{N}$ und sind $p = 6m+1, q = 12m+1, r = 18m+1$ Primzahlen, so ist *n=pqr* eine Carmichael-Zahl.

g) finden Sie 10 Carmichael-Zahlen.

Aufgabe 2

a) Ist $x \in \mathbb{R}$, so bezeichnet man mit $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich *x* sind. Gauß hat entdeckt, daß für $x \geq 2$ gilt $\pi(x) \simeq \frac{x}{\log x}$ und dann sogar die bessere Approximation $\pi(x) \simeq \int_2^x \frac{\mathrm{d}\,t}{\log\, t}$ gefunden.

Benutzen Sie partielle Integration, um zu zeigen, daß $\lim_{x\to\infty} \frac{\int_2^x \frac{\mathrm{d}\,t}{\log\, t}}{\frac{x}{\log x}} = 1$.

(Machen Sie sich zunächst eine Vorstellung von den Funktionen $\pi(x)$, $x \mapsto \int_2^x \frac{\mathrm{d}\,t}{\log\, t}$, $x \mapsto \frac{x}{\log\, x}$.)

b) Gehen Sie aus von $\pi(x) \simeq \frac{x}{\log x}$. Tun Sie so, als sei dies eine Gleichung. Schätzen Sie ab, wie groß die Zahl *h* sein muß, damit sich im Intervall $[2^{1024}, 2^{1024}+h]$ eine Primzahl befindet, damit also $\pi(2^{1024}+h) - \pi(2^{1024}) \geqslant 1$.

Damit läßt sich abschätzen, wie oft man bei dieser Größenordnung von Zahlen einen Primzahltest durchführen muß, um schließlich eine Primzahl zu finden.