Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 6

bitte heften Sie dieses Blatt vor Ihre Lösungen

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

1. Die Möbiusfunktion ist bekanntlich so definiert:
$\mu(1):=1$.
$\mu(n):=0$, falls in der Primfaktorzerlegung $n=p_1^{\alpha_1}\cdot\ldots\cdot p_m^{\alpha_m}$ mindestens ein $\alpha_i>1$.
$\mu(n):=(-1)^m$ sonst.

a) Man zeige für alle $n\in\mathbb{N}$: $\mu(n)=\sum_{\substack{1\leq k\leq n\\ \mathrm{ggT}(k,n)=1}} \exp\left(\frac{2\pi i k}{n}\right)$

b) Was fällt Ihnen an den Werten der Funktion $\rho(n):=\sum_{d/n}\mu^2(d)$ auf? (Beweis!)

c) Berechnen Sie die Anzahl der irreduziblen Polynome vom Grad 17 in $\mathbb{Z}_5[X]$.

2. Man zeige, daß a) $\limsup_{n\to\infty}\frac{\varphi(n)}{n} = 1$, b) $\liminf_{n\to\infty}\frac{\varphi(n)}{n} = 0$.

3. Sei G eine beliebige Gruppe. Das Element $a\in G$ besitze die Ordnung $d\in\mathbb{N}$.
Man zeige: a^k besitzt Ordnung d genau dann, wenn ggT(d, k)=1.

4. Sei G eine endliche kommutative Gruppe. Man zeige:
a) Sind $a,b\in G$ und sind ord(a)=m, ord(b)=n teilerfremd, so ist ord(ab)=mn.
b) Benutzen Sie b), um zu zeigen: Sind $a,b\in G$ und ord(a)=m, ord(b)=n, so gibt es ein $c\in G$ mit ord(c)=kgV(m, n).
c) Ist d das Maximum der Ordnung aller Elemente von G, so ist die Ordnung jedes Elements ein Teiler von d .