Zahlentheorie – Blatt 8

Abgabe am 13.6.2017 bis 10:30 Uhr

1	2	3	4	Σ

.....
Name und Matr-Nr.

Bitte drucken Sie diese Seite aus und verwenden Sie sie als Deckblatt für Ihre Lösungen.

Wie üblich sind alle Antworten zu begründen/beweisen.

Aufgabe 1 (4 Punkte):

Sei $q \in \mathbb{N}$ so, dass Primitivwurzeln modulo q existieren. Zeigen Sie:

(a) Die Anzahl der Primitivwurzeln modulo q ist $\phi(\phi(q))$.

(b) Für beliebige n gilt: $\#\{a \in \mathbb{Z}/q\mathbb{Z} \mid a^n = 1\} = \mathrm{ggT}(n, \phi(q))$.

Aufgabe 2 (4 Punkte):

(a) Sei $(G, \cdot)$ eine endliche abelsche Gruppe, und sei $a \in G$. Zeigen Sie: Sind $n \in \mathbb{N}$ und $p \in \mathbb{P}$ so, dass $a^n \neq 1$ aber $a^{pn} = 1$ ist, so ist $\mathrm{ord}(a)$ durch p^r teilbar, wobei $p^r \parallel pn$. (Zur Erinnerung: „$p^r \parallel m$“ bedeutet, dass p^r die größte p-Potenz ist, die m teilt.)

(b) Finden Sie die kleinste natürliche Zahl $q \geq 3$, so dass $X^{1000} \equiv -1 \mod q$ (mindestens) eine Lösung hat. Geben Sie für dieses q eine Lösung an, zeigen Sie, dass dies eine Lösung ist, und zeigen Sie auch, dass es für kleinere q keine Lösung gibt.
Hinweis: Teil (a) kann nützlich sein.

Aufgabe 3 (4 Punkte):

Sei $p \geq 3$ eine Primzahl, sei $r \geq 1$, und sei $q = p^r$.

(a) Zeigen Sie die folgende Formel für die Anzahl der zu q teilerfremden Quadrate modulo q:

$$\#\{a^2 \mid a \in (\mathbb{Z}/q\mathbb{Z})^\times\} = \frac{p-1}{2} \cdot p^{r-1}.$$

(b) Zeigen Sie die folgende Formel für die Anzahl aller Quadrate modulo q:

$$\#\{a^2 \mid a \in \mathbb{Z}/q\mathbb{Z}\} = \frac{p-1}{2} \cdot \left\lfloor \frac{p^{r+1}}{p^2-1} \right\rfloor + 1$$

Hinweis: Können Sie eine Bijektion angeben zwischen den Quadraten modulo q, die nicht zu q teilerfremd sind, und allen Quadraten modulo $p^{r'}$ für ein geeignetes r'?

Aufgabe 4 (4 Punkte):

Sei p eine Primzahl, n eine natürliche Zahl, und sei $s := 1^n + 2^n + \cdots + (p-1)^n$. Zeigen Sie:

(a) Ist n durch $p-1$ teilbar, so ist $s \equiv -1 \mod p$.

(b) Ist n nicht durch $p-1$ teilbar, so ist $s \equiv 0 \mod p$.

Hinweis zu (b): Verwenden Sie die Existenz einer Primitivwurzel.