Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2009
13. Mai 2009

Algorithmische Zahlentheorie

Übungsblatt 4

Aufgabe 13

Unter dem Exponenten einer endlichen abelschen Gruppe G versteht man die kleinste ganze Zahl $r \geqslant 1$, so dass

$$x^r = 1 \qquad \text{für alle } x \in G.$$

a) Für die Gruppe $G := (\mathbb{Z}/1512)^*$ bestimme man die Ordnung $\varphi(1512)$ und den Exponenten r.

b) Für jeden Teiler $s \mid r$ bestimme man die Anzahl der Elemente $x \in (\mathbb{Z}/1512)^*$, deren Ordnung gleich s ist.

Aufgabe 14

Sei p eine ungerade Primzahl mit $p \equiv 2 \bmod 3$.
a) Man zeige: Für jedes $a \in \mathbb{Z}/p$ ist die Gleichung

$$x^3 = a$$

in $\mathbb{Z}/p$ eindeutig lösbar.

b) Man löse die Gleichung

$$x^3 = 71 \quad \text{in } \mathbb{Z}/101.$$

Aufgabe 15

Sei p eine ungerade Primzahl mit $p \equiv 1 \bmod 3$.
a) Man zeige: Für $a \in (\mathbb{Z}/p)^*$ ist die Gleichung

$$x^3 = a$$

in $(\mathbb{Z}/p)^*$ genau dann lösbar, wenn $a^{(p-1)/3} = 1$. In diesem Fall gibt es 3 Lösungen.

b) Man bestimme in $(\mathbb{Z}/223)^*$ alle Lösungen der Gleichungen

$$x^3 = 1, \qquad y^3 = 2.$$

---

b.w.

Aufgabe 16

Sei $m \geqslant 3$ eine ganze Zahl mit $\gcd(m, 10) = 1$.

a) Man beweise: Die Periodenlänge der Dezimalbruch-Entwicklung von $1/m$ ist gleich der Ordnung der Restklasse von 10 in der multiplikativen Gruppe $(\mathbb{Z}/m)^*$.

b) Man bestimme die Zahl $m < 100$, so dass die Dezimalbruch-Entwicklung von $1/m$ eine möglichst lange Periode hat.

c)* Die folgende Ziffernfolge A ist ein Abschnitt der Dezimalbruch-Entwicklung von $1/p$,

$$A: \qquad 778\,14817\,84977$$

mit der Primzahl $p := 2\,22222\,22223$. Man bestimme die vorausgehenden und die nachfolgenden 10 Ziffern der Dezimalbruch-Entwicklung. An welcher Stelle hinter dem Komma beginnt der obige Abschnitt? Wie groß ist die Periodenlänge?

d)** Die folgende Ziffernfolge B ist ein Abschnitt der Dezimalbruch-Entwicklung von $1/q$,

$$B: \qquad 659\,89985\,68984\,09865\,51570$$

wobei q eine unbekannte 11-stellige Primzahl ist. Man bestimme q und beantworte die analogen Fragen wie in Teil c).

Abgabetermin: Freitag, 22. Mai 2009, 14 Uhr, Übungskasten im 1. Stock

Stern-Aufgaben sind nicht obligatorisch; ihre Lösung ergibt Extra-Punkte. Geht bis zum Abgabetermin des Blattes keine richtige Lösung ein, verlängert sich die Abgabefrist automatisch. Die Lösungen sind danach per Email an `forster@math.lmu.de` einzusenden. Die Abgabefrist endet nach Eingang der ersten richtigen Lösung.