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

SS 2009
20. Mai 2009

Algorithmische Zahlentheorie

Übungsblatt 5

Aufgabe 17

a) Sei p eine ungerade Primzahl. Man zeige: Die Gleichung

$$ax^2 + bx + c = 0, \qquad p \nmid a,$$

hat im Körper $\mathbb{F}_p$ genau $1 + (\frac{b^2-4ac}{p})$ Lösungen.

b) Man löse in $\mathbb{F}_{101}$ die Gleichung

$$7x^2 + 13x + 71 = 0.$$

Aufgabe 18 Sei $k \geqslant 3$ und $a \in \mathbb{Z}$ ungerade.

a) Man zeige: Die Kongruenz

$$x^2 \equiv a \bmod 2^k$$

ist genau dann lösbar, wenn $a \equiv 1 \bmod 8$. Wieviele Lösungen gibt es in diesem Fall?

b) Man gebe eine Methode an, wie man aus einer Lösung von $x^2 \equiv a \bmod 2^k$ eine Lösung von $x^2 \equiv a \bmod 2^{k+1}$ konstruieren kann.

c) Man bestimme alle Lösungen der Kongruenz

$$x^2 \equiv 17 \bmod 1024.$$

Aufgabe 19

Sei p eine Primzahl der Form $p = 2q + 1$, wobei q ebenfalls prim ist (Sophie-Germain-Primzahl). Man zeige: Genau dann ist 2 Primitivwurzel modulo p, wenn $p \equiv \pm 3 \bmod 8$.

Aufgabe 20

Sei p eine Primzahl $\equiv 3 \bmod 4$ und a ein Quadrat in $\mathbb{F}_p^*$.

a) Man zeige: Unter den zwei Lösungen der Gleichung

$$x^2 = a \qquad \text{in } \mathbb{F}_p^*$$

gibt es genau eine, die selbst ein Quadrat ist. Diese werde mit $\sqrt{a}$ bezeichnet.

b) Die Folge $(x_n)_{n\geqslant 0}$ in $\mathbb{F}_p^*$ werde definiert durch

$$x_0 := a; \qquad x_{n+1} := \sqrt{x_n} \quad \text{für alle } n \geqslant 0.$$

Man zeige: Die Folge (x_n) ist rein periodisch.

---

b.w.

c) Ein gerichteter Graph Γ_p werde wie folgt definiert:

i) Die Knoten sind die $(p-1)/2$ Quadrate in $\mathbb{F}_p^*$.

ii) Zwei Knoten x und y sind genau dann durch einen Pfeil von x nach y verbunden, wenn

$$y = \sqrt{x}.$$

Man zeichne die Graphen Γ_{23} und Γ_{31}

d) Man zeige: Der Graph Γ_p zerfällt in einen isolierten Punkt und punktfremde Zyklen. Genau dann gibt es in Γ_p einen Zyklus der Länge $(p-3)/2$, wenn $q := (p-1)/2$ prim und 2 eine Primitivwurzel modulo q ist.

e)* Sei p die Primzahl

$$p = \frac{10^{19}-1}{9} = 1111\,11111\,11111\,11111$$

Sei C der Zyklus in Γ_p, auf dem 2 liegt. Man berechne die Länge von C und bestimme die kleinste ungerade Primzahl, die auf C liegt.

Abgabetermin: Freitag, 29. 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.