MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
PROF. DR. O. FORSTER

SS 2017
21. Juni 2017

Einführung in die Zahlentheorie

Übungsblatt 8

Aufgabe 29

Sei G eine (multiplikativ geschriebene) endliche abelsche Gruppe (z.B. $G = (\mathbb{Z}/N)^*$) und seien $x, y \in G$ Elemente mit $\mathrm{ord}(x) =: k$ und $\mathrm{ord}(y) =: \ell$. Man beweise:

a) Falls $\gcd(k, \ell) = 1$, gilt $\mathrm{ord}(xy) = k\ell$.

b) Im allgemeinen Fall sei $d := \gcd(k, \ell)$ und $y' := y^d$. Dann gilt

$$\mathrm{ord}(xy') = \mathrm{lcm}(k, \ell) = k\ell/d.$$

Aufgabe 30

Sei G eine (multiplikativ geschriebene) endliche abelsche Gruppe der Ordnung $n := \#G$ mit Primfaktorzerlegung

$$n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}.$$

Zu jedem $j = 1, \ldots, r$ gebe es ein Element $x_j \in G$ mit

$$x_j^{n/p_j} \neq 1.$$

Man beweise, dass G zyklisch ist und konstruiere aus den x_j ein erzeugendes Element von G.

Aufgabe 31

Für die Primzahlen $p = 29$ und $p = 31$ bestimme man jeweils alle Lösungen der Kongruenzen

i) $x^8 \equiv 1 \bmod p$,

ii) $x^8 \equiv 7 \bmod p$,

iii) $x^8 \equiv 14 \bmod p$.

Aufgabe 32

Sei p eine ungerade Primzahl, g eine Primitivwurzel modulo p und $\log_g : (\mathbb{Z}/p)^* \to \mathbb{Z}/(p-1)$ der zugehörige diskrete Logarithmus.

a) Man beweise: $\log_g(-1) = \dfrac{p-1}{2}$.

b) Ist g' eine weitere Primitivwurzel modulo p, so gilt

$$\log_g(g') \log_{g'}(g) \equiv 1 \bmod (p-1).$$