Mathematisches Institut
der Universität München
Andreas Fackler

Sommersemester 2009
Lösungsvorschlag für Übungsblatt 7

Klausurenkurs Algebra

Aufgabe 1 (Frühjahr 2006, Thema 3, Aufgabe 1)

(a) Sei $m = \prod_{i=1}^{k} p_i^{e_i}$ die Primfaktorzerlegung von m und sei q eine weitere von den p_i verschiedene Primzahl. Dann gilt für alle $l \geq 1$:

$$\varphi\left(q^l \cdot \prod_{i=1}^{k} p_i^{e_i+1}\right) = (q-1)q^{l-1} \prod_{i=1}^{k} (p_i - 1)p_i^{e_i},$$

was ein Vielfaches von m ist.

(b) Es gibt unendlich viele Zehnerpotenzen, aber nur endlich viele Restklassen modulo m. Daher gibt es eine Restklasse modulo m, die unendlich viele Zehnerpotenzen enthält, das heißt, es gibt $k_1, k_2, \ldots$, so dass

$$10^{k_1} \equiv 10^{k_2} \equiv \ldots \mod m$$

ist. Dann besteht für jedes i die Zahl $10^{k_i} + 10^{k_{i+1}} + \ldots + 10^{k_{i+m-1}}$ nur aus Nullen und Einsen, aber es gilt:

$$10^{k_i} + 10^{k_{i+1}} + \ldots + 10^{k_{i+m-1}} \equiv 10^{k_1} + 10^{k_1} + \ldots + 10^{k_1} \equiv m \cdot 10^{k_1} \equiv 0 \mod m$$

Aufgabe 2 (Herbst 2007, Thema 3, Aufgabe 5)

Sei $g : \mathbb{F}_q \to \mathbb{F}_q$ beliebig. Das Polynom

$$f(x) = \sum_{a \in \mathbb{F}_q} g(a) \prod_{b \in \mathbb{F}_q \setminus \{a\}} \frac{x-b}{a-b}$$

stellt offenbar g dar.

Aufgabe 3 (Herbst 2007, Thema 3, Aufgabe 3)

Aus $p | \Phi_n(z) | z^n - 1$ folgt $z^n \equiv 1 \mod p$. Also ist z eine primitive n-te Einheitswurzel im Körper $\mathbb{F}_p$. Damit ist z keine primitive d-te Einheitswurzel für $d \neq n$, also gilt auch $p \nmid z^d - 1$.

Aufgabe 4 **(Herbst 2006, Thema 3, Aufgabe 4)**

Sei ζ eine primitive m-te Einheitswurzel. Dann enthält $\mathbb{F}_p[\zeta]$ bereits alle m-ten Einheitswurzeln. Folglich hat das Minimalpolynom jeder Einheitswurzel den gleichen Grad $k = [\mathbb{F}_p[\zeta] : \mathbb{F}_p]$, und Φ_m ist das Produkt dieser Minimalpolynome. Daraus folgt auch, dass $k|\Phi_m$. Der Frobeniushomomorphismus bildet die Nullstellen des Minimalpolynoms von ζ aufeinander ab: ζ^p ist wieder eine Nullstelle des gleichen Polynoms, aber erst ζ^{p^k} ist wieder gleich ζ. Es folgt also $\zeta^{p^k-1} = 1$ un daraus folgt $m|p^k-1$, da ζ eine primitive m-te Nullstelle ist. Für ein $l < k$ kann nicht $\zeta^{p^k} = \zeta$ sein, also ist für $l < k$: $m \nmid p^k - 1$.