Endliche Körper und Codierung

Übung, LVA 405.351

C. Fuchs

3. Übungsblatt, WS 2018/19 — 24.10.2018

1. Man zeige, dass für jedes $n \geq 1$ das Produkt aller normierten irreduziblen Polynome über $\mathbb{F}_p$ deren Grad n teilt, gleich $x^{p^n} - x$ ist.

2. Sei $I_p(n)$ die Anzahl der normierten irreduziblen Polynome vom Grad n über $\mathbb{F}_p$. Dann gilt
$$p^n = \sum_{d|n} d I_p(d)$$
für alle $n \in \mathbb{N}$.

3. Die Möbius-Funktion auf $\mathbb{N}$ ist definiert durch
$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1, \\ (-1)^k & \text{falls } n \text{ ein Produkt von } k \text{ verschiedenen Primzahlen ist,} \\ 0 & \text{falls } n \text{ nicht quadratfrei ist.} \end{cases}$$
Seien h und H Abbildungen von $\mathbb{N}$ nach $\mathbb{Z}$. Zeige, dass
$$H(n) = \sum_{d|n} h(d) \iff h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right)$$
jeweils für alle $n \in \mathbb{N}$ (Möbius'sche Inversionsformel).

4. Man zeige mit Hilfe der Möbius'schen Inversionsformel, dass
$$I_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$
gilt und folgere daraus, daß zum jedem $n \geq 1$ stets ein irreduzibles Polynom über $\mathbb{F}_p$ vom Grad n existiert.