Übungsblatt 12 für Analyse von Algorithmen (9.1.2013)

56.) Es sei $f(x) \in \mathbb{F}_q$ ein Polynom mit $f' = 0$ und es bezeichne p die Charakteristik von $\mathbb{F}_q$. Man zeige, dass dann $f(x) = g(x)^p$ ist für ein Polynom $g(x) \in \mathbb{F}_q$.

57.) Man formuliere (z.B. mit Hilfe von Beispiel 55) einen Faktorisierungsalgorithmus für Polynome $f(x) \in \mathbb{F}_{2^k}[x]$.

58.) Es sei n eine naürliche Zahl mit Primfaktoren $p_1, \ldots, p_r$ Man zeige, dass ein normiertes Polynom $f(x) \in \mathbb{F}_q$ vom Grad n genau dann irreduzibel ist, wenn $f(x) | x^{q^n} - x$ gilt und wenn $\mathrm{ggT}(f(x), x^{q^{n/p_j}} - x) = 1$ für alle $j = 1, \ldots, r$ gilt.

59.) Ein Polynom $f(x) \in \mathbb{F}_q$ heißt *primitiv*, wenn $f(x)$ irreduzibel ist und eine Nullstelle von $f(x)$ ein erzeugendes Element der multiplikativen Gruppe von $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f(x))$ ist. Wie kann man (algorithmisch) feststellen, ob ein gegebenes Polynom primitiv ist?
Hinweis: Man beachte, dass die Restklasse $\alpha = x \bmod f(x)$ ein erzeugendes Element von $\mathbb{F}_q[x]/(f(x))$ sein muss.

60.) Es sei $C_m = \{g, g^2, \ldots, g^m = 1\}$ eine zyklische Gruppe der Ordnung m mit erzeugendem Element g. Man zeige:

$$\#\{x \in C_m : x^k = 1\} = \mathrm{ggT}(k, m).$$