Übungsblatt 11 für Analyse von Algorithmen (19.12.2012)

51.) Sei K ein Körper. Für ein Polynom $f = \sum_k a_k x^k \in K[x]$ ist die formale Ableitung f' durch $f' = \sum_k (k+1)a_{k+1}x^k$ definiert (wobei k als Abkürzung für $k = 1 + 1 + \cdots + 1 = k \cdot 1$ steht). Man zeige die Ableitungsregeln $(fg)' = f'g + fg'$ und $(f^m)' = mf^{m-1}f'$.

52.) Es sei $f = f_1^{e_1} \cdots f_r^{e_r}$ die eindeutige Zerlegung eines normierten Polynoms über einem endlichen Körper in normierte irreduzible Polynome. Man formuliere einen Algorithmus, der bei Eingabe von f das Produkt $g = f_1 \cdots f_r$ bestimmt, ohne dass die Faktoren f_j bestimmt werden.
Hinweis: Man starte mit dem $\mathrm{ggT}(f, f')$.

53.) Man zeige: Über einem endlichen Körper mit q Elementen gilt für jedes $m \ge 1$

$$x^{q^m} - x = \prod f(x),$$

wobei das Produkt auf der rechten Seite über alle normierten irreduziblen Polynome $f(x)$ gebildet wird, deren Grad ein Teiler von m ist.
Hinweis: Man verwende die Eigenschaft, dass $x^{q^m} - x = \prod(x - \alpha)$ ist, wobei das Produkt über alle Elemente aus $\mathbb{F}_{q^m}$ gebildet wird, und fasse entsprechend zusammen.

54.) Sei q eine ungerade Primzahlpotenz und $S = \{b^2 : b \in \mathbb{F}_q^\times\}$ der Menge der Quadrate in $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$. Man zeige, dass S eine Untergruppe von $\mathbb{F}_q^\times$ der Ordnung $(q-1)/2$ ist und

$$S = \{a \in \mathbb{F}_q^\times : a^{(q-1)/2} = 1\}, \qquad \mathbb{F}_q^\times \setminus S = \{a \in \mathbb{F}_q^\times : a^{(q-1)/2} = -1\}.$$

55.) Für ein Element $a \in \mathbb{F}_{2^k}$ ist die Spur durch

$$\mathrm{Sp}(a) = \sum_{i=0}^{k-1} a^{2^i}$$

definiert. Man zeige, dass $\mathrm{Sp} : \mathbb{F}_{2^k} \to \mathbb{F}_2$ eine lineare Abbildung ist, bei der 0 und 1 gleichoft angenommen werden.