CS-E4500 Advanced Course in Algorithms (5 cr)

Problem Set 8 *Spring 2019*

1. Factor the polynomial $1 + x + x^2 + 2x^3 + x^4 \in \mathbb{Z}_3[x]$.

   Hints: You can either use a general-purpose factoring algorithm or try to discover factors in some other way. Maybe the polynomial has roots in $\mathbb{Z}_3$?

2. Square-and-multiply modular exponentiation. Let q be a prime power. Present an algorithm that, given $m \in \mathbb{Z}_{\geq 1}$, $f \in \mathbb{F}_q[x]$, and $g \in \mathbb{F}_q[x] \setminus \{0\}$ with $\deg f, \deg g \leq d \in \mathbb{Z}_{\geq 1}$ as input, computes $f^m \operatorname{rem} g$ in $O(M(d) \log m)$ operations in $\mathbb{F}_q$. Carefully justify the number of operations used by your algorithm.

   Hints: Use a recursive design that on each recursive call at least halves m. When you halve m, you may want to square f. Be careful to take remainders with g to control the degree of the intermediate results.

3. Formal derivative of a factorization. Let q be a prime power. Let $f \in \mathbb{F}_q[x]$ be monic with factorization $f = f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}$ into distinct irreducible monic polynomials $f_1, f_2, \ldots, f_r \in \mathbb{F}_q[x]$ and $d_1, d_2, \ldots, d_r \in \mathbb{Z}_{\geq 1}$. Show that the formal derivative of f satisfies

$$f' = d_1 f_1' \frac{f}{f_1} + d_2 f_2' \frac{f}{f_2} + \ldots + d_r f_r' \frac{f}{f_r} \in \mathbb{F}_q[x]\,.$$

   Above we write d_j for a sum of d_j copies of the multiplicative identity of $\mathbb{F}_q$.

   Hint: Recall Problem 3 in last week's problem set.

4. Squares and non-squares. Let q be a prime power and let $\gamma \in \mathbb{F}_q^\times$ be an element with multiplicative order $q - 1$. For $k \in \mathbb{Z}_{\geq 2}$ let us say that an element $\alpha \in \mathbb{F}_q$ is a *k^{th} power* if there exists an element $\beta \in \mathbb{F}_q$ with $\alpha = \beta^k$.

   (a) Let $k \geq 2$ divide $q - 1$. Show that $\alpha \in \mathbb{F}_q^\times$ is a k^{th} power if and only if there exists an $s \in \{0, 1, \ldots, q - 2\}$ such that $\gamma^s = \alpha$ and k divides s.

   (b) Suppose that q is odd. Show that $\mathbb{F}_q^\times$ has exactly $(q - 1)/2$ elements that are squares and exactly $(q - 1)/2$ elements that are non-squares. Show that for each square $\alpha \in \mathbb{F}_q^\times$ it holds that $\alpha^{(q-1)/2} = 1$, and for each non-square $\alpha \in \mathbb{F}_q^\times$ it holds that $\alpha^{(q-1)/2} = -1$.

   Hints: Recall that we write $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ for the multiplicative group of $\mathbb{F}_q$. In part (a), observe that since γ has multiplicative order $q - 1$, for any $\mu \in \mathbb{F}_q^\times$ it holds that there exists a unique $s \in \{0, 1, \ldots, q - 2\}$ such that $\mu = \gamma^s$. For part (b), use part (a) with $k = 2$ to characterize the squares and the non-squares. Recall Fermat's little theorem and observe that $x^2 - 1 = 0$ has at most two solutions.

Deadline and submission instructions. This problem set is due no later than Sunday 24 March 2019, 20:00 (8pm), Finnish time. Please submit your solutions as a single PDF file via e-mail to the lecturer (`petteri.kaski(atsymbol)aalto.fi`). Please use the precise title

```
CS-E4500 Problem Set 8: [your-student-number]
```

with “[your-student-number]” replaced by your student number. For example, assuming that my student number is 123456, I would carefully title my e-mail

```
CS-E4500 Problem Set 8: 123456
```

and attach to the e-mail a single PDF file containing my solutions. Please note that the submissions are automatically processed and archived, implying that failure to follow these precise instructions may result in your submission not being graded.