CS-E4500 Advanced Course in Algorithms (5 cr)

Problem Set 7 *Spring 2019*

1. A finite field of prime power order.

   (a) Find a monic irreducible polynomial of degree 2 in $\mathbb{Z}_3[x]$.

   (b) Using your solution to part (a), present addition and multiplication tables for $\mathbb{F}_9$. For each nonzero element of $\mathbb{F}_9$, present its multiplicative inverse in $\mathbb{F}_9$.

   Hints: For part (a), observe that a nonconstant polynomial $f \in F[x]$ of degree at most 3 is irreducible if and only if f does not have a root in F. For part (b), observe that both tables have $9 = 3^2$ rows and columns. Also observe that you can determine the multiplicative inverses by studying the multiplication table.

2. Multiplicative order of elements. Using your solution to Problem 1, find for each nonzero element of $\mathbb{F}_9$ its multiplicative order.

   Hint: A study of the multiplication table reveals the multiplicative orders.

3. Formal derivative for polynomials. Let R be a commutative ring with $0_R \neq 1_R$. For a polynomial $f = \sum_{i=0}^{d} \varphi_i x^i \in R[x]$, define the *formal derivative* $f' \in R[x]$ of f by

$$f' = \sum_{i=1}^{d} i_R \varphi_i x^{i-1} \,,$$

   where $i_R = 1_R + 1_R + \ldots + 1_R$ obtained by taking the sum of i copies of the multiplicative identity 1_R of R.

   Show that the formal derivative satisfies each of the following properties:

   (a) $'$ is R-linear,

   (b) $'$ satisfies the Leibniz (product) rule $(fg)' = f'g + fg'$, and

   (c) $'$ satisfies the chain rule $(f(g))' = f'(g)g'$.

   Hints: To show linearity in part (a), take $f, g \in R[x]$, $\alpha, \beta \in R$ and use the definition to verify that $(\alpha f + \beta g)' = \alpha f' + \beta g'$. For part (b), conclude by linearity that it suffices to consider $f = x^n$ and $g = x^m$. For part (c), conclude by linearity that it suffices to consider $f = x^n$, and reduce to part (b).

4. Extended Fermat's little theorem. Let q be a prime power and let $d \in \mathbb{Z}_{\geq 1}$. Show that $x^{q^d} - x \in \mathbb{F}_q[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides d.

   Hints: Observe that q^d is a prime power and apply Fermat's little theorem to $\mathbb{F}_{q^d}$ to conclude that $x^{q^d} - x = \prod_{a \in \mathbb{F}_{q^d}} (x - a)$. Next, observe that $x^{q^d} - x$ is squarefree; that is, for all $g \in \mathbb{F}_q[x]$ of degree at least 1, it holds that g^2 does not divide $x^{q^d} - x$. Then show that for any monic irreducible $f \in \mathbb{F}_q[x]$ of degree n it holds that f divides $x^{q^d} - x$ if and only if n divides d. Assuming that f divides $x^{q^d} - x$, show that $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle f \rangle$ is (isomorphic to) a subfield of $\mathbb{F}_{q^d}$, implying that there exists an $e \in \mathbb{Z}_{\geq 1}$ with $(q^n)^e = q^d$, which implies that n divides d. Assuming that n divides d, show that $\gcd(f, x^{q^d} - x) =$

f in $\mathbb{F}_q[x]$ by identifying a root $a \in \mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle f \rangle$ of f and then showing that $x - a$ divides $\gcd(f, x^{q^d} - x)$ in $\mathbb{F}_{q^n}[x]$. To show that $x - a$ divides $x^{q^d} - x$, first use Fermat's little theorem in $\mathbb{F}_{q^n}[x]$ to conclude that $x - a$ divides $x^{q^n} - x$, and then, using the assumption that n divides d, establish that

$$q^d - 1 = (q^n - 1)m$$

with $m = q^{d-n} + q^{d-2n} + \ldots + 1$ and

$$x^{q^d-1} - 1 = (x^{q^n-1} - 1)(x^{(q^n-1)(m-1)} + x^{(q^n-1)(m-2)} + \ldots + 1)\,.$$

Deadline and submission instructions. This problem set is due no later than Sunday 17 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 7: [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 7: 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.