Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

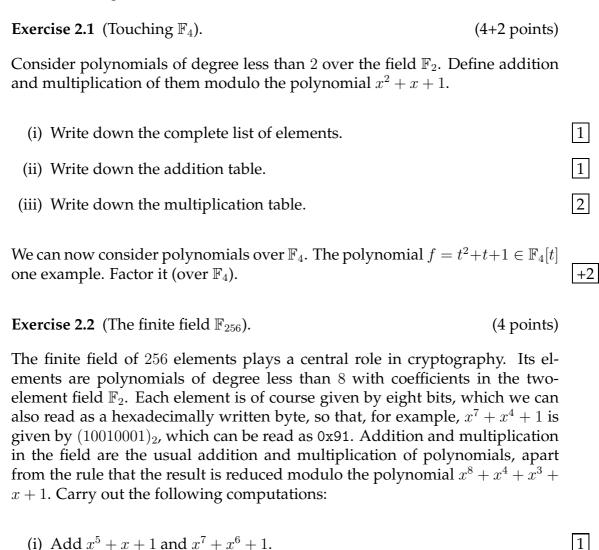
2. Exercise sheet

Hand in solutions until Thursday, 07 November 2013, 07:59:59

Note the changed hand-in deadline!

(ii) Multiply 0x23 and 0xC1.

(iii) Calculate the inverse of 0x23.



Exercise 2.3 (A strange polynomial).

(6+2 points)

Consider for a prime p the polynomial $f = x^p - x \in \mathbb{Z}_p[x]$. Our goal is to factor this polynomial.

- (i) To get some feeling for it, compute $x \cdot (x-1) \cdot (x-2) \in \mathbb{Z}_3[x]$.
- (ii) Show that for any $a \in \mathbb{Z}_p$, we have f(a) = 0.
- [1] Show that for any polynomial $g \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ with g(a) = 0 the polynomial $x a \in \mathbb{Z}_p[x]$ divides g.
- [2] (iv) Show that $\prod_{a \in \mathbb{Z}_p} (x-a)$ divides f. Hint: In $\mathbb{Z}_p[x]$ any polynomial of degree n can have at most n roots.
- 1 (v) Conclude $f = \prod_{a \in \mathbb{Z}_p} (x a)$.
- Extend the result for prime powers $q = p^e$ for a prime p and an integer exponent $e \in \mathbb{N}_{>1}$. Hint: Finite fields!