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!

Exercise 2.1 (Touching $\mathbb{F}_4$). (4+2 points)

Consider polynomials of degree less than 2 over the field $\mathbb{F}_2$. Define addition and multiplication of them modulo the polynomial $x^2 + x + 1$.

(i) Write down the complete list of elements. 1

(ii) Write down the addition table. 1

(iii) Write down the multiplication table. 2

We can now consider polynomials over $\mathbb{F}_4$. The polynomial $f = t^2+t+1 \in \mathbb{F}_4[t]$ one example. Factor it (over $\mathbb{F}_4$). +2

Exercise 2.2 (The finite field $\mathbb{F}_{256}$). (4 points)

The finite field of 256 elements plays a central role in cryptography. Its elements are polynomials of degree less than 8 with coefficients in the two-element field $\mathbb{F}_2$. Each element is of course given by eight bits, which we can also read as a hexadecimally written byte, so that, for example, $x^7 + x^4 + 1$ is given by $(10010001)_2$, which can be read as `0x91`. Addition and multiplication in the field are the usual addition and multiplication of polynomials, apart from the rule that the result is reduced modulo the polynomial $x^8 + x^4 + x^3 + x + 1$. Carry out the following computations:

(i) Add $x^5 + x + 1$ and $x^7 + x^6 + 1$. 1

(ii) Multiply `0x23` and `0xC1`. 1

(iii) Calculate the inverse of `0x23`. 2

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 $x \cdot (x-1) \cdot (x-2) \in \mathbb{Z}_3[x]$. 1

(ii) Show that for any $a \in \mathbb{Z}_p$, we have $f(a) = 0$. 1

1 (iii) 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 $f = \prod_{a \in \mathbb{Z}_p}(x-a)$.

+2 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!