Exercises Week 12
Advanced Encryption Standard (cont.)

Hans Georg Schaathun

12th November 2015

Period 4–10 November 2015

Reading Stein *et al.* do not cover this material. You should read the AES Standard from NIST, and you can read more about finite fields in Rosen.

Programme This document details the programme for the week, including exercises and pointers to other material. It is available in two versions:

1. as a PDF document.
2. as a web site. This depends on MathML and may require firefox/iceweasel to display correctly.

The web version includes inline video. The pdf version shows a still image from the video, providing a hyperlink directly to the video on the web site.

1 Wednesday 4 November 2015

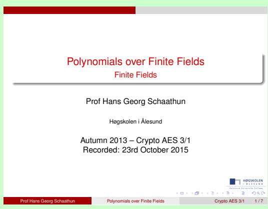
Theory

Polynomials, can be defined over finite fields, just as they can over real numbers. A polynomial has the form

$$p(x) = a_k x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_2 x^2 + a_1 x + a_0,$$

for some indeterminate x.

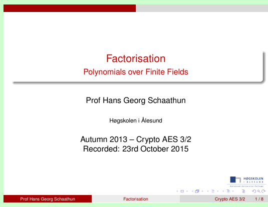
The set of polynomials over some ring forms a new ring.



OGG MP4 Slides

THEORY

Polynomials share key properties with integers. We can add and multiply polynomials, and we can factor them into *irreducible* polynomials.



OGG

MP4

Slides

Exercise 1.1 *Factorise* $x^2 - 1$ *over* $\mathbb{Z}_3$*, i.e. write* $x^2 - 1$ *as a product of two polynomials.*

Exercise 1.2 *Is it possible to factorise* $x^2 + 1$ *over* $\mathbb{Z}_3$*? Why/why not?*

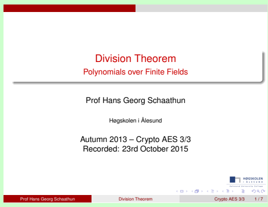
THEORY

Theorem 1 *Given two polynomials* $f(x)$ *and* $g(x)$*, where* $g(x) \neq 0$*, there are polynomials* $q(x)$ *and* $r(x)$ *such that*

$$f(x) = q(x)g(x) + r(x) \tag{1}$$

$$\deg r < \deg g \tag{2}$$

If also $f(x) = q_1(x)g(x) + r_1(x)$*, then* $q_1 = q$ *and* $r_1 = r$*.*



OGG

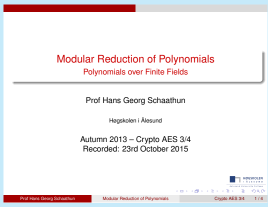
MP4

Slides

EXERCISE EXAMPLE

Problem 1.1 *Calculate* $f(x) \mod p(x)$ *for the following definitions:*

1. $f(x) = x^4 + x^2 + 1$; $p(x) = x^4 + x + 1$
2. $f(x) = x^7 + x^6 + x^3 + x^2 + 1$; $p(x) = x^4 + x + 1$



OGG

MP4

Slides

THEORY

Definition 1 *Let* R *be a ring and* $R[x]$ *the ring of polynomials over* R*. For any* $p \in R[x]$ *and* $f, g \in R[x]$*, we say that* f *and* g *are congruent modulo* p*, writing*

$$f(x) \equiv g(x) \pmod{p(x)},$$

if there is $q \in R[x]$ *such that*

$$f(x) + q(x)p(x) = g(x).$$

OGG

MP4

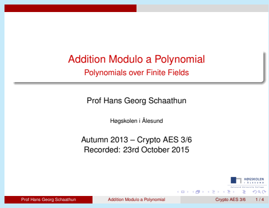
Slides

Exercise Example

Problem 1.2 *Consider the following polynomials over* $\mathbb{Z}_2$*:*

$$p(x) = x^4 + 1 \tag{3}$$
$$f(x) = x^3 + x + 1 \tag{4}$$
$$g(x) = x^2 + 1 \tag{5}$$
$$\tag{6}$$

Calculate $f(x) + g(x) \mod p(x)$.



OGG

MP4

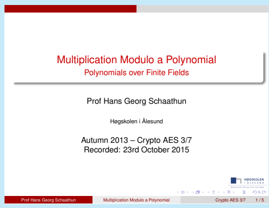
Slides

Exercise Example

Problem 1.3 *Consider the following polynomials over* $\mathbb{Z}_2$*:*

$$p(x) = x^4 + 1 \tag{7}$$
$$f(x) = x^3 + x + 1 \tag{8}$$
$$g(x) = x^2 + 1 \tag{9}$$
$$\tag{10}$$

Calculate $f(x) \cdot g(x) \mod p(x)$.



OGG

MP4

Slides

Exercise 1.3 *Let*

$$f(x) = x^2 + 1, \tag{11}$$
$$g(x) = x^3 + x + 1 \tag{12}$$

be polynomials over $\mathbb{Z}_2$*. Calculate*

1. $f(x) + g(x)$
2. $f(x) \cdot g(x)$

Exercise 1.4 *If* $f(x)$ *has degree* k_1 *and* $g(x)$ *has degree* k_2*, what degree does* $f(x) \cdot g(x)$ *have? What degree does* $f(x) + g(x)$ *have?*

Exercise 1.5 *How many polynomials of degree 3 exist over* $\mathbb{Z}_2$*? Give reasons for your answer. Did you use any counting principle?*

Exercise 1.6 *Find all the irreducible polynomials of degree 3 over* $\mathbb{Z}_2$*.*

Exercise 1.7 *Consider the following polynomials over $\mathbb{Z}_2$:*

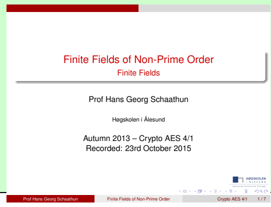
$$p(x) = x^4 + 1 \quad (13)$$
$$f(x) = x^3 + x + 1 \quad (14)$$
$$g(x) = x^2 + 1 \quad (15)$$
$$(16)$$

1. *Calculate* $f(x) + g(x) \mod p(x)$.
2. *Calculate* $f(x) \cdot g(x) \mod p(x)$.

2 Thursday 5 November 2015

Theory

If p is prime and $m(x)$ is an irreducible polynomial over $\mathbb{Z}_p$, then $\mathbb{Z}_p[x]/(m(x))$ is a field.



OGG

MP4

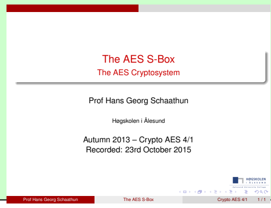
Slides

Exercise 2.1 *How many elements does $\mathbb{Z}_p[x]/(m(x))$ have?*

What counting principles do you use?

Theory

Confusion in AES works on a single byte, i.e. as a function $S : \mathrm{GF}(2^8) \to \mathrm{GF}(2^8)$. This is usually implement as a look-up table called an *S-box*, but it also has an algebraic definition.



OGG

MP4

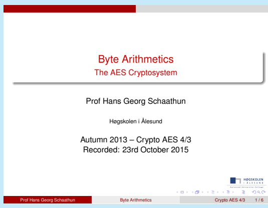
Slides

Exercise Example

AES considers a byte as an element

$$x \in \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1).$$

Let's have a look at multiplication and addition in this field.



OGG

MP4

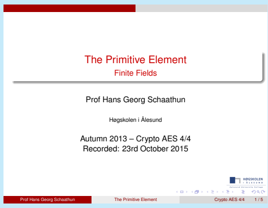
Slides

Exercise Example

The element $\alpha = x$ is a primitive element in

$$x \in \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1).$$

If you consider the sequence $[\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \ldots]$, how many distinct elements do you get?



OGG

MP4

Slides

Exercise Example

Problem 2.1 *Consider two polynomials over* $\mathbb{Z}_3$*:*

$$f(x) = x^6 + 2x^5 + x^3 + 2x + 1$$
$$g(x) = x^4 + 2x + 1$$

Find $q(x)$ *and* $r(x)$ *to satisfy the division theorem,* $f(x) = q(x)g(x) + r(x)$ *with* $\deg r < \deg g$.

OGG

MP4

Slides

Exercise 2.2 *Consider two polynomials over* $\mathbb{Z}_2$*:*

$$f(x) = x^7 + x^5 + x^2 + x + 1$$
$$g(x) = x^4 + x^3 + 1$$

Find $q(x)$ *and* $r(x)$ *to satisfy the division theorem,* $f(x) = q(x)g(x) + r(x)$ *with* $\deg r < \deg g$.

Exercise 2.3 *Consider two polynomials over* $\mathbb{Z}_3$*:*

$$f(x) = x^6 + 2x^5 + x^3 + 2x + 1$$
$$g(x) = x^4 + 2x + 1$$

Find $q(x)$ *and* $r(x)$ *to satisfy the division theorem,* $f(x) = q(x)g(x) + r(x)$ *with* $\deg r < \deg g$.

Exercise 2.4 *Consider the polynomial*

$$p(x) = x^3 + 2x + 1$$

over $\mathbb{Z}_3$ *and the finite field* $Z_3/(p(x))$.

1. *Find a primitive element* $\alpha \in Z_3/(p(x))$.
2. *Tabulate all the powers of* α *with corresponding polynomials.*
3. *Use the table to calculate the following:*
   a) $(x^2 + 1) \cdot (2x + 1)$

b) $(x^2 + 2x + 1) \cdot (x + 2)$

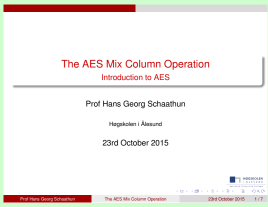
Exercise 2.5 *Using* $\mathrm{GF}(2^8)$ *as defined in the AES standard, i.e. modulo* $x^8 + x^4 + x^3 + x + 1$*, calculate the following products*

1. $(x^6 + x^3 + 1) \cdot (x^3 + x)$

3 Summary talks

THEORY

The MixColumn operation is a linear substitution. Being linear, it can feasibly operate on 32 bits, whereas the non-linear S-box works on 8 bits.



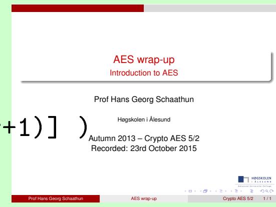
OGG

MP4

Slides

THEORY

The following is the AES encryption pseudo code from the standards document.



OGG MP4 Slides

```
Cipher( byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)] )
begin
   byte state[4,Nb]

   state = in

   AddRoundKey(state, w[0,Nb-1])

   for round = 1 step 1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MisColumns(state)
      AddRoundKey(state, w[round*Nb,(round+1)*Nb-1])
   end for

   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb,(Nr+1)*Nb-1])

   out = state
end
```

4 Compulsory Problems (Tuesday 10 November)

Exercise 4.1 *Consider the AES S-Box as described in the videos, slides, or standards. Show how you use the mathematical description to calculate the substitution of the following bytes (written in Hexadecimal):*

1. *01*
2. *A7*

Exercise 4.2 *Consider two polynomials over* $\mathbb{Z}_2$*:*

$$\begin{aligned} f(x) &= x^7 + x^6 + x^5 + x^4 + x^2 + x + 1 \\ g(x) &= x^3 + x + 1 \end{aligned}$$

Find $q(x)$ *and* $r(x)$ *to satisfy the division theorem,* $f(x) = q(x)g(x) + r(x)$ *with* $\deg r < \deg g$.

Exercise 4.3 *Using* $\mathrm{GF}(2^8)$ *as defined in the AES standard, i.e. modulo* $x^8 + x^4 + x^3 + x + 1$*, calculate the following products*

1. $(x^7 + x^2 + x + 1) \cdot (x + 1)$
2. $(x^6 + x^3 + 1) \cdot (x^5 + x^2 + 1)$

Exercise 4.4 *Which irreducible polynomials of degree 2 exist over* $\mathbb{Z}_5$*?*

Exercise 4.5 *What are the advantages and disadvantages of symmetric cryptography (e.g. AES) compared to asymmetric cryptography (e.g. RSA)?*

How are symmetric and asymmetric ciphers used in practice (e.g. in SSL)?

(Note, this was covered in the video on Hybrid Encryption *in Week 5.)*

Exercise 4.6 *We have seen that Euclid's Division Theorem applies to polynomials just as it does to integers. We can use this to apply Euclid's algorithm as well. Find the highest common factor of the two polynomials*

$$a(x) = x^4 + x^2 + x + 1, \tag{17}$$

$$b(x) = x^3 + 1. \tag{18}$$