# Week 4: More Cryptography and Modular Arithmetics

Hans Georg Schaathun

12th November 2015

**Period** 9–15 September 2015

**Reading** Stein *et al* cover this material in Chapter 2.

**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.

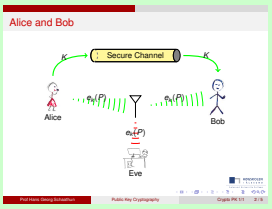
## 1 Wedneday 9 September

This session is devoted to playing around with small numbers, and explore how the elements of $\mathbb{Z}_n$ behave for varying values of $n$. The objective is to learn how to construct public-key cryptosystems, a problem which we will return to next week when we master some of the fundamental mathematics. Just to make sure that we do not forget why we do the math's, let's start with two high-level talks to explain what public-key cryptography is.

THEORY

After a week on Classic Cryptography, it is time to get on with modern solutions, suitable for practical applications in our time. This video gives a high-level perspective of public-key cryptography.

**Related reading:** Stein *et al.* 93–95 or Rosen p. 295.



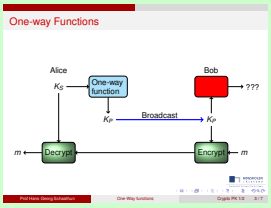

OGG

MP4

Slides

THEORY

Public-key cryptography depends on one-way functions, and there is only a small number of such functions to choose from. This video gives an overview.




OGG

MP4

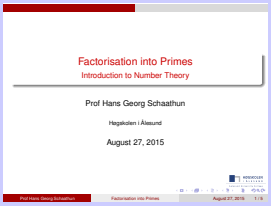
Slides

## 1.1 Factorisation and the highest common factor

WORKED EXAMPLE

A prime number is a natural number which is only divisible by one and itself. A number which is not prime is known as a composite number, which can be written as a product of primes.

**Problem 1.1** *Factorise* 135.




OGG

MP4

Slides

**Exercise 1.1** *Factorise the following integers:*

1. 12
2. 56
3. 123
4. 1024
5. 1025

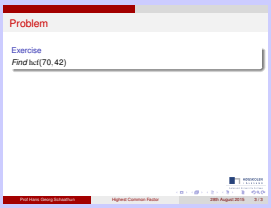
*How do you find the answer for each integer? (What are you looking for? Do you have a systematic approach or do you look for any particular patterns?)*

**Exercise 1.2** *Which are the zero divisors of* $\mathbb{Z}_{75}$*?*

WORKED EXAMPLE

**Definition 1** *The highest common factor (HCF) of two integers* $a$ *and* $b$ *is the largest number* $q$ *such that* $q \mid a$ *and* $q \mid b$*. We write* $\mathrm{hcf}(a,b) = q$ *or* $\gcd(a,b) = q$*.*

**Problem 1.2** *Find* $\mathrm{hcf}(70, 42)$




OGG

MP4

Slides

**Exercise 1.3** *Find*

1. $\mathrm{hcf}(6, 4)$
2. $\mathrm{hcf}(7, 3)$

3. $\text{hcf}(18, 12)$

4. $\text{hcf}(19, 8)$

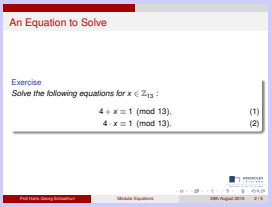
## 1.2 Equations

**Related reading:** Stein *et al.* p. 105–110 or Rosen p. 272–275

WORKED EXAMPLE

**Problem 1.3** *Solve the following equations for* $x \in \mathbb{Z}_{13}$ *:*

$$4 + x \equiv 1 \pmod{13}, \tag{1}$$
$$4 \cdot x \equiv 1 \pmod{13}. \tag{2}$$




OGG

MP4

Slides

**Exercise 1.4** *Solve the following equations*

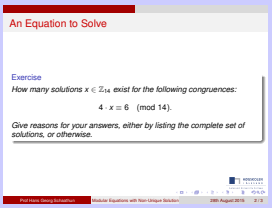
$$3 + x \equiv 1 \pmod{8}, \tag{3}$$
$$3 \cdot x \equiv 1 \pmod{8}, \tag{4}$$
$$4 \cdot x + 2 \equiv 8 \pmod{15}. \tag{5}$$

WORKED EXAMPLE

**Problem 1.4** *How many solutions* $x \in \mathbb{Z}_{14}$ *exist for the following congruence:*

$$4 \cdot x \equiv 6 \pmod{14}.$$

*Give reasons for your answers, either by listing the complete set of solutions, or otherwise.*




OGG

MP4

Slides

**Exercise 1.5** *How many solutions* $x \in \mathbb{Z}_{12}$ *exist for each of the following congruences:*

$$3 \cdot x \equiv 3 \pmod{15}, \tag{6}$$
$$3 \cdot x \equiv 5 \pmod{15}, \tag{7}$$
$$5 \cdot x \equiv 3 \pmod{15}, \tag{8}$$
$$5 \cdot x \equiv 5 \pmod{15}. \tag{9}$$

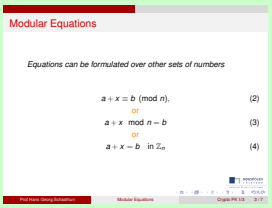
*Give reasons for your answers, either by listing the complete set of solutions, or otherwise.*

THEORY

**Lemma 1** *If* $a$ *has a multiplicative inverse* $a^{-1} \in \mathbb{Z}_n$*, then the equation*

$$a \cdot x = b \quad \text{in } \mathbb{Z}_n$$

*has the solution* $x = a^{-1} \cdot b$*.*




OGG

MP4

Slides

**Exercise 1.6** *Given $b$ in $\mathbb{Z}_n$. What general statements can be made about the number of possible solutions to the equation $a \cdot b = 1$ in $\mathbb{Z}_n$?*

**Exercise 1.7** *Look at the following congruences:*

$$4x \equiv 3 \pmod{29}, \tag{10}$$
$$4x \equiv 3 \pmod{81}, \tag{11}$$
$$4x \equiv 3 \pmod{128}, \tag{12}$$
$$4x \equiv 64 \pmod{128}. \tag{13}$$

*How many solutions does each of these congruences have? How much can you say without checking every possible value of $x$? Is there any relationship between the coefficient of $x$ (4 in all cases) and the modulus (29,81,128,128). Discuss this in your group.*

## 2 Thursday 10 September

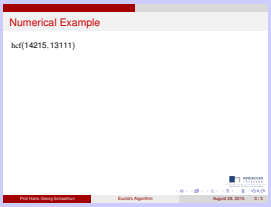
For this session we introduce two important algorithms to compute the highest common factor and the multiplicative inverses for large numbers.

**Related reading:** Stein *et al.* 110–119 or Rosen p. 263–272

WORKED EXAMPLE

For large numbers we need an algorithm to find the highest common factor. It is time to demonstrate it.

**Problem 2.1** *Calculate* $\text{hcf}(44215, 43111)$.




OGG

MP4

Slides

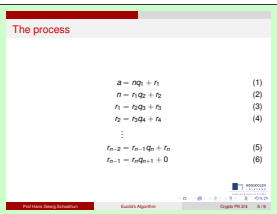
**Exercise 2.1** *Using Euclid's Algorithm, find*

1. $\text{hcf}(121, 77)$
2. $\text{hcf}(108, 54)$

THEORY

In this video we show how the Euclidean algorithm is defined to find $\text{hcf}(a, b)$ for arbitrary numbers $a$ and $b$

**Related reading:** Stein *et al.* p. 114-115 or Rosen p. 266-268




OGG

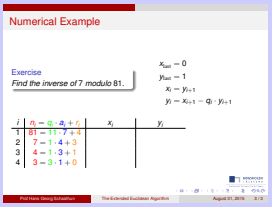
MP4

Slides

**Worked Example**

The Euclidean algorithm finds the highest common factor, and is useful for large numbers. The Extended Euclidean algorithm finds multiplicative inverses (when they exist).

**Problem 2.2** *Find the inverse of* 7 *modulo* 81.




OGG

MP4

Slides

**Exercise 2.2** *Find the multiplicative inverses of*

1. 12 mod 55.
2. 7 mod 26.
3. 7 mod 29.

**Exercise 2.3** *Solve the following congruence for* $x$. *Use the Extended Euclidean Algorithm to find the inverses that you need.*

1. $4x \equiv 17 \pmod{121}$
2. $10x + 19 \equiv 0 \pmod{171}$

**Exercise 2.4** *Consider the affine cipher*

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2 \mod n.$$

*The decryption function can be written on the same form*

$$d_{k_1',k_2'}(y) = k_1' \cdot y + k_2' \mod n,$$

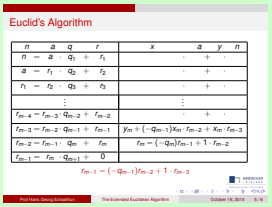
*for suitable choices of* $(k_1', k_2')$. *Find the decryption key* $(k_1', k_2')$ *for each of the following encryption keys:*

1. $(19, 17)$ mod 26.
2. $(19, 17)$ mod 29.

**Theory**

It is useful to know how the Extended Euclidean Algorithm is derived and how we can prove that it is correct.

**Related reading:** Stein *et al.* p. 114-115 or Rosen p. 266-268




OGG

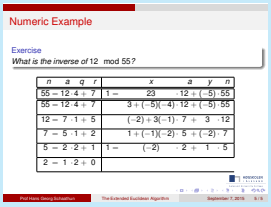
MP4

Slides

**Exercise Example**

If you need another worked example, we can offer this one, recorded 2014.

**Exercise 2.5** *What is the inverse of* 12 mod 55*?*




OGG

MP4

Slides

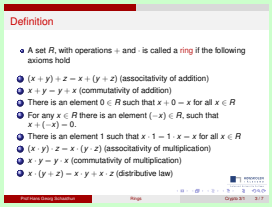
## 3 Last lectures of the week

At this stage it is useful to tie up some of the concepts with which we have worked and introduce two important mathematical objects: the *ring* and the *field*. When you watch these videos, remember that $\mathbb{Z}_n$ is a ring; and if $p$ is a prime, then $\mathbb{Z}_p$ is a field. If it does not make complete sense at this stage, don't worry; we will revisit these topics later.

**Related reading:** Stein *et al.* p. 98-101 or Rosen p. 808+

**Theory**

The sets $\mathbb{Z}_n$ is an example of a ring. Let's get the definition.



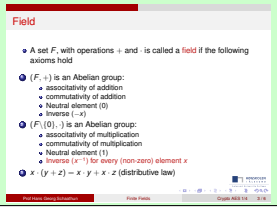

OGG MP4 Slides

**Definition 2** *A set $R$, with operations $+$ and $\cdot$ is called a* ***ring*** *if the following axioms hold*

1. $(x+y)+z = x+(y+z)$ *(associtativity of addition)*
2. $x+y = y+x$ *(commutativity of addition)*
3. *There is an element* $0 \in R$ *such that* $x+0 = x$ *for all* $x \in R$
4. *For any* $x \in R$ *there is an element* $(-x) \in R$*, such that* $x+(-x) = 0$.
5. *There is an element* $1$ *such that* $x \cdot 1 = 1 \cdot x = x$ *for all* $x \in R$
6. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(associtativity of multiplication)*
7. $x \cdot y = y \cdot x$ *(commutativity of multiplication)*
8. $x \cdot (y+z) = x \cdot y + x \cdot z$ *(distributive law)*

**Theory**

A field is a ring with the additional property that every non-zero element has a multiplicative inverse. A finite field is a field with a finite number of elements.




OGG

MP4

Slides

## 4 Compulsory Assignment (Tuesday 15 September)

**Definition 3** *The multiplicative inverse of $x \in \mathbb{Z}_n$ is the number $x^{-1}$ with the property that $xx^{-1} = x^{-1}x = 1$*

**Exercise 4.1** *Consider the following elements $x$ in their respective rings. Find $x^{-1}$ for the following elements:*

1. $x = 7 \in \mathbb{Z}_{26}$
2. $x = 1 \in \mathbb{Z}_2$

**Definition 4** *The negative element (additive inverse) of $x \in \mathbb{Z}_n$ is the number $-x$ with the property that $x + (-x) = (-x) + x = 0$*

**Exercise 4.2** *Consider the following elements $x$ in their respective rings. Find $-x$ for the following elements:*

1. $x = 8 \in \mathbb{Z}_{26}$
2. $x = 1 \in \mathbb{Z}_2$

**Exercise 4.3** *Using Euclid's Algorithm, find*

1. $\text{hcf}(63, 14)$
2. $\text{hcf}(963, 312)$

**Exercise 4.4** *Find the multiplicative inverses of*

1. $28 \mod 81$.
2. $52 \mod 121$.

**Definition 5** *Exponentiation $\alpha^k$ is defined as the product $\alpha \cdot \alpha \cdot \ldots \cdot \alpha$ with exactly $k$ factors.*

**Exercise 4.5** *Write down all the powers of 2 in $\mathbb{Z}_{11}$ in a table. How many distinct values do you get before it starts repeating itself?*

**Exercise 4.6** *Write down all the powers of 2 in $\mathbb{Z}_9$ in a table. How many distinct values do you get before it starts repeating itself?*

**Exercise 4.7** *Compare Exercises 4.5 and 4.6. What is the relationship between the number of distinct values and the modulus $n$? Does $n$ have any properties which can tell us how many distinct powers to expect?*