

# The wonderful world of arithmetic

And its applications to cryptography

Karst Koymans

Informatics Institute  
University of Amsterdam  
(version 1.6, 2011/11/16 20:09:32)

Thursday, November 17, 2011

## Table of Contents

### Numbers and basic arithmetic laws

- Commutative monoids and groups
- Combining addition and multiplication
- Primes
- Greatest common divisor

### Arithmetic in finite structures

- Modular arithmetic
- Euler's  $\varphi$
- Chinese Remainder Theorem

### Applications to cryptography

- RSA
- Diffie-Hellman

### Finite fields in general

- Galois fields
- Application to AES(Rijndael)

## The natural numbers

Properties of (commutative) monoids

$$\mathbb{N} = \langle \{0, 1, 2, \dots\}, +, 0 \rangle$$

### Laws

$x + y = y + x$	(Commutativity)
$(x + y) + z = x + (y + z)$	(Associativity)
$x + 0 = x$	(Neutral element)

### Non-law

$\forall x \exists y (x + y = 0)$	(Existence of inverses)
-----------------------------------	-------------------------

## The integers

Properties of a (commutative) group

$$\mathbb{Z} = \langle \{\dots, -2, -1, 0, 1, 2, \dots\}, +, 0 \rangle$$

### Laws

$x + y = y + x$	(Commutativity)
$(x + y) + z = x + (y + z)$	(Associativity)
$x + 0 = x$	(Neutral element)
$\forall x \exists y (x + y = 0)$	(Existence of inverses)

# Commutative (Abelian) groups

An axiomatization

$$\mathbb{G} = \langle G, \star, e, (\cdot)^{-1} \rangle$$

## Laws

$x \star y = y \star x$	(Commutativity)
$(x \star y) \star z = x \star (y \star z)$	(Associativity)
$x \star e = x$	(Neutral element)
$x \star x^{-1} = e$	(Existence of inverses)

# The field of rational numbers

## Groups

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{Q} \setminus \{0\}, \cdot, 1 \rangle$$

can be combined into

## A field

$$\langle \mathbb{Q}, +, \cdot, 0, 1 \rangle$$

defining the field of rational numbers.

# Examples

and non-examples

## Examples (No groups)

$$\langle \mathbb{Z}, \cdot, 1 \rangle$$

$$\mathbb{Q} = \langle \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}, \cdot, 1 \rangle$$

## Examples (Groups)

$$\langle \mathbb{Q} \setminus \{0\}, \cdot, 1 \rangle$$

$$\langle \mathbb{R} \setminus \{0\}, \cdot, 1 \rangle$$

$$\langle \mathbb{C} \setminus \{0\}, \cdot, 1 \rangle$$

Here  $\mathbb{R}$  is the set of reals ( $\sqrt{2}, e, \pi, \dots$ )  
and  $\mathbb{C}$  is the set of complex numbers adding  $i = \sqrt{-1}$ .

# General fields

and their axiomatization

A **field**  $\langle F, \oplus, \star, 0, 1 \rangle$  consists of

- ▶ A commutative group  $\langle F, \oplus, 0 \rangle$
- ▶ and a commutative group  $\langle F \setminus \{0\}, \star, 1 \rangle$
- ▶ satisfying

## Distributivity

$$(x \oplus y) \star z = (x \star z) \oplus (y \star z) \quad \text{(Distributivity)}$$

- ▶ but not satisfying

## “Wrong” distributivity

$$(x \star y) \oplus z = (x \oplus z) \star (y \oplus z) \quad \text{(Wrong distributivity)}$$

## Primes

and unique factorization

$$\begin{aligned}\mathbb{P} &= \{2, 3, 5, 7, 11, 13, \dots\} \\ &= \{p_0, p_1, p_2, p_3, p_4, p_5, \dots\}\end{aligned}$$

### Theorem

Every natural number  $n > 0$  can be written in an essentially unique way as a product of primes:

$$n = \prod_{i=0}^{k-1} p_i^{a_i}$$

### Example

$$126 = 2 \cdot 3 \cdot 3 \cdot 7 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1 = p_0^1 \cdot p_1^2 \cdot p_2^0 \cdot p_3^1$$

## Greatest common divisor

Euclid's algorithm

### Theorem

For all  $a, b \in \mathbb{Z}$  we can find  $p, q \in \mathbb{Z}$  such that

$$\gcd(a, b) = p \cdot a + q \cdot b$$

Finding  $p$  and  $q$  can be done using Euclid's algorithm.

### Definition

$a$  and  $b$  are called **relatively prime** if  $\gcd(a, b) = 1$ .

### Theorem

If  $a$  and  $b$  are relatively prime Euclid's algorithm calculates  $p$  and  $q$  such that

$$p \cdot a + q \cdot b = 1$$

## Greatest common divisor

an example

We want to find the gcd (greatest common divisor) of 49 and 35:

### Euclid's reduction

$$49 = 1 \cdot 35 + 14 \implies \gcd(49, 35) = \gcd(35, 14)$$

$$35 = 2 \cdot 14 + 7 \implies \gcd(35, 14) = \gcd(14, 7)$$

$$14 = 2 \cdot 7 + 0 \implies \gcd(14, 7) = \gcd(7, 0) = 7$$

### Euclid's reversal

$$7 = 35 - 2 \cdot 14 \quad \wedge \quad 14 = 49 - 1 \cdot 35$$

$$\begin{aligned}7 &= 35 - 2 \cdot (49 - 1 \cdot 35) \\ &= -2 \cdot 49 + 3 \cdot 35\end{aligned}$$

## Clock Arithmetic

$24 = 0$  (or  $12 = 0$ )

$$\blacktriangleright \mathbb{Z}_{24} = \{0, 1, 2, \dots, 23\}$$

$$\blacktriangleright 23 + 1 \equiv 24 \equiv 0 \pmod{24}$$

### Definition

$$a \equiv b \pmod{n} \iff n \mid (a - b) \iff \exists k(kn = (a - b))$$

### Theorem

$\equiv \pmod{n}$  is an equivalence relation on  $\mathbb{Z}$  which is also a congruence.

$\mathbb{Z}_n$  is the set of integers modulo  $n$ .

### Corollary

Addition and multiplication can be performed  $\pmod{n}$  as usual.

# Clock Arithmetic

## Examples

### Examples

$$\begin{aligned}
 22 + 5 &\equiv 3 \pmod{24} \\
 22 \cdot 5 &\equiv 110 \equiv 14 \pmod{24} \\
 -2 \cdot 5 &\equiv -10 \equiv 14 \pmod{24} \\
 2 \cdot 12 &\equiv 24 \equiv 0 \pmod{24} \\
 2 &\not\equiv 0 \pmod{24} \\
 12 &\not\equiv 0 \pmod{24}
 \end{aligned}$$

$\mathbb{Z}_{24}$  has “divisors of zero”

# Multiplication tables

for  $\mathbb{Z}_n \setminus \{0\}$

### Example ( $\mathbb{Z}_5 \setminus \{0\}$ )

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

### Example ( $\mathbb{Z}_6 \setminus \{0\}$ )

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

# Prime fields

## Theorem

$\langle \mathbb{Z}_p, +, \cdot, 0, 1 \rangle$  is a field if and only if  $p$  is prime.

$\mathbb{Z}_n^* = \langle \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}, \cdot, 1 \rangle$  is a group for all  $n \in \mathbb{N}, n > 1$ .

### Example ( $\mathbb{Z}_{12}^*$ )

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

### Example ( $\mathbb{Z}_{10}^*$ )

·	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

# Euler's $\varphi$ -function

and the Euler-Fermat theorem

## Definition

$\varphi(n)$  is the number of elements of  $\mathbb{Z}_n^*$ :

$$\varphi(n) = |\mathbb{Z}_n^*|$$

## Theorem

For all  $a \in \mathbb{Z}_n^*$  (that means  $\gcd(a, n) = 1$ )

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

## Example

$$\varphi(10) = 4$$

$$\varphi(12) = 4$$

## Chinese Remainder Theorem

### Theorem

Whenever  $n_1, \dots, n_k \in \mathbb{N}$  are *pairwise relatively prime* we can solve the set of equations

$$x \equiv a_1 \pmod{n_1}$$

...

$$x \equiv a_k \pmod{n_k}$$

The solution  $x$  is unique  $\pmod{n_1 \cdot \dots \cdot n_k}$ .

## Simple example for the CRT

Example ( $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$ )

$\mathbb{Z}_{12}$	$\mathbb{Z}_3$	$\mathbb{Z}_4$
0	0	0
1•	1•	1•
2	2•	2
3	0	3•
4	1•	0
5•	2•	1•
6	0	2
7•	1•	3•
8	2•	0
9	0	1•
10	1•	2
11•	2•	3•

## Euler's function special case

Product of two primes

### Theorem

Let  $p, q \in \mathbb{P}$  be two primes ( $p \neq q$ ) and let  $n = pq$ .

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$$

$$\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

$$\varphi(pq) = \varphi(p)\varphi(q)$$

$$\varphi(p) = p - 1$$

$$\varphi(q) = q - 1$$

In general  $\varphi(n)$  is hard to calculate, but for  $n = pq$ , where  $p$  and  $q$  are known primes, this is easy:  $\varphi(n) = (p - 1)(q - 1)$

## RSA

Its definition

### Definition (RSA)

RSA works with public information (Uppercase) and private information (lowercase)

- ▶ A public modulus  $N = pq$ , which is the product of two private (secret) primes. Notice that  $\varphi(N) = (p - 1)(q - 1)$ , which is (as far as we know) hard to calculate if you do not know the primes  $p$  and  $q$ .
- ▶ A public exponent  $E \in \mathbb{Z}_{\varphi(N)}^*$ .
- ▶ A private exponent  $d$  such that  $Ed \equiv 1 \pmod{\varphi(N)}$ .  $d$  can easily be calculated using Euclid's algorithm.
- ▶  $(N, E)$  is called the **public** key.
- ▶  $(p, q = \frac{N}{p}, d)$  is called the **private** key.
- ▶  $(N = pq, E, d)$  is called a **public/private** key "pair".

## RSA

Its principle of operation

### Theorem

Let a message be represented as an integer  $m < N$ . Let this message be encoded as  $C \equiv m^E \pmod{N}$ . Then  $m \equiv C^d \pmod{N}$ .

### Proof.

Let  $C \equiv m^E \pmod{N}$  and  $Ed = 1 + k\varphi(N)$ .  
Then

$$\begin{aligned} C^d &\equiv (m^E)^d \pmod{N} \equiv m^{Ed} \pmod{N} \\ &\equiv m^{(1+k\varphi(N))} \pmod{N} \\ &\equiv m(m^{\varphi(N)})^k \pmod{N} \\ &\equiv m1^k \pmod{N} \equiv m \pmod{N} \end{aligned}$$

Who spots the minor omission in this proof? □

## Difficult problems

### Definition (The factorization problem)

The **integer factorization problem**, that is to reconstruct  $p$  and  $q$  from  $N = pq$ , is supposed to be a hard problem.

### Definition (The discrete logarithm problem)

The **discrete logarithm problem**, that is to reconstruct  $x$  from  $X = G^x \pmod{P}$ , is supposed to be a hard problem.

## Diffie-Hellman

Its definition

### Theorem

$\mathbb{Z}_P^*$  is a **cyclic group** for all primes  $P \in \mathbb{P}$ .

Let  $G$  be a generator of this group.

$$\mathbb{Z}_P^* = \{G, G^2, G^3, \dots, G^{P-1} = 1\}$$

### Definition (Diffie-Hellman)

Let two parties choose secret numbers  $x, y < P$  and publish  $X \equiv G^x \pmod{P}$  and  $Y \equiv G^y \pmod{P}$ .

The two parties now have a **shared secret**:  $G^{xy} \pmod{P}$ .

X knows

$$G^{xy} \equiv (G^y)^x \equiv Y^x \pmod{P}$$

Y knows

$$G^{xy} \equiv (G^x)^y \equiv X^y \pmod{P}$$

## Finite fields

and their cyclic multiplicative subgroup

### Theorem

For any finite field  $\mathbb{F}$

- ▶  $|\mathbb{F}| = p^n$ , where  $p$  is a prime called the characteristic of  $\mathbb{F}$ , being the smallest number for which the  $p$ -time repetition  $1 + 1 + \dots + 1$  is equal to 0.
- ▶ For any prime  $p$  and natural number  $n > 0$  there is exactly one field, denoted  $GF(p^n)$  or  $\mathbb{F}_{p^n}$ , with  $p^n$  elements (up to isomorphism).
- ▶ The multiplicative group of  $\mathbb{F}$  is always cyclic
- ▶  $GF(p) \cong \mathbb{Z}_p$
- ▶  $GF(p^n) \not\cong (\mathbb{Z}_p)^n$
- ▶  $GF(p^n) \not\cong \mathbb{Z}_{p^n}$

## The ring of polynomials over a finite field

### Definition

$\mathbb{F}[X] = \{a_n X^n + \dots + a_1 X + a_0 \mid a_i \in \mathbb{F}, i = 0 \dots n, a_n \neq 0\}$  is the **ring of (formal) polynomials** in the variable  $X$ .  $n$  is called the **degree** of the polynomial.

### Theorem

- ▶ In  $\mathbb{F}[X]$  one can add and multiply polynomials as usual.
- ▶ In  $\mathbb{F}[X]$  the equivalent of Euclid's algorithm works.
  - ▶ For any  $f(X) \in \mathbb{F}[X]$  and  $g(X) \in \mathbb{F}[X]$  there are  $q(X) \in \mathbb{F}[X]$  and  $r(X) \in \mathbb{F}[X]$  such that

$$f(X) = q(X)g(X) + r(X)$$

where  $r(X)$  has lower degree than  $g(X)$ .

- ▶ We write  $f(X) \equiv r(X) \pmod{g(X)}$

## The equivalents of the primes in $\mathbb{F}[X]$

### Definition

A polynomial  $g(X)$  is called **irreducible** in  $\mathbb{F}[X]$  if there are no lower degree ( $> 1$ ) polynomials  $h(X)$  and  $k(X)$  such that  $g(X) = h(X)k(X)$ .

### Theorem

- ▶ If  $g(X)$  is irreducible then

$$\mathbb{F}[X]_{g(X)} = \{f(X) \pmod{g(X)} \mid f(X) \in \mathbb{F}[X]\}$$

is a field.

- ▶ Taking  $\mathbb{F} = \mathbb{Z}_p$  for a prime  $p$  and  $g(X)$  an irreducible polynomial of degree  $n$  we get a field with  $p^n$  elements, giving an explicit construction for  $GF(p^n)$ .

## Examples of irreducible polynomials

### Example

- ▶  $X^2 + 1$  is not irreducible over  $GF(2)$   
(for we have  $X^2 + 1 = X^2 + 2X + 1 = (X + 1)^2$ )
- ▶  $X^2 + X + 1$  is irreducible over  $GF(2)$
- ▶  $GF(4) = GF(2^2) = \mathbb{Z}_2[X]_{X^2+X+1} = \{0, 1, X, X^2 = X + 1\}$
- ▶  $X^2 + X + 1$  is not irreducible over  $GF(3)$   
(for we have  $X^2 + X + 1 = X^2 + 4X + 4 = (X + 2)^2$ )
- ▶  $X^2 + 1$  is irreducible over  $GF(3)$
- ▶  $X^2 + 2X + 2$  is also irreducible over  $GF(3)$
- ▶  $GF(9) = GF(3^2) = \mathbb{Z}_3[X]_{X^2+2X+2} = \{0, X, X^2 = X + 1, X^3 = 2X + 1, X^4 = 2, X^5 = 2X, X^6 = 2X + 2, X^7 = X + 2, X^8 = 1\}$

## Use of Galois Fields in AES

- ▶ The *S-box* uses polynomials over  $GF(2)$ 
  - ▶ The inverse modulo the irreducible  $x^8 + x^4 + x^3 + x + 1$ 
    - ▶ Represent elements in  $GF(2^8)$  by  $\mathbf{XY}$  for hex digits  $\mathbf{X}, \mathbf{Y}$
  - ▶ Multiplication by  $x^4 + x^3 + x^2 + x + 1$  (**1f**) modulo the reducible  $x^8 + 1$
  - ▶ Addition of  $x^6 + x^5 + x + 1$  (**63**)
- ▶ *MixColumn* uses polynomials over  $GF(2^8)$  modulo the reducible polynomial  $x^4 + \mathbf{01}$ 
  - ▶ Multiplication with **03** $x^3 + \mathbf{01}x^2 + \mathbf{01}x + \mathbf{02}$  and for the inverse with **0B** $x^3 + \mathbf{0D}x^2 + \mathbf{09}x + \mathbf{0E}$
- ▶ *Key expansion* uses
  - ▶ Arithmetic in  $GF(2^8)$  for generating the constants  $C_i = x^i$  working modulo the irreducible polynomial  $x^8 + x^4 + x^3 + x + 1$
  - ▶ The polynomial  $x^3$  modulo  $x^4 + \mathbf{01}$  over  $GF(2^8)$  for rotations of columns