Mathematical Background

Prof. Dr. Rudolf Mathar, Georg Böcherer, Paul de Kerret

22.04.2010, Cryptography I.

Basics from Algebra

Definition 1. *A set $\mathcal{G}$ together with a law of composition $\circ : \mathcal{G} \times \mathcal{G} \to \mathcal{G}, (a,b) \mapsto a \circ b$ is called a* group *if the following holds:*

- $(a \circ b) \circ c = a \circ (b \circ c)$ *for all* $a, b, c \in G$ *(associativity).*
- *There exists* $e \in G$ *with* $a \circ e = e \circ a = a$ *for all* $a \in G$ *(neutral element).*
- *For each* $a \in G$ *there exists* $a' \in G$ *such that* $a \circ a' = a' \circ a = e$ *(inverse element).*

Definition 2. *A group is said to be* commutative *or* Abelian *if*

$$a \circ b = b \circ a, \forall a, b \in G. \tag{1}$$

Definition 3. *A set $\mathcal{R}$ together with two laws of composition $+ : \mathcal{R} \times \mathcal{R} \to \mathcal{R}, (a,b) \mapsto a+b$ and $\cdot : \mathcal{R} \times \mathcal{R} \to \mathcal{R}, (a,b) \mapsto a \cdot b$ is called a* ring *if the following holds:*

- $(\mathcal{R}, +)$ *is an Abelian group.*
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(associativity).*
- *For each* $a \in \mathcal{R}$ *there exists* $u \in \mathcal{R}$ *such that* $a \cdot u = u \cdot a = a$ *(neutral element).*
- $(a+b) \cdot c = a \cdot c + b \cdot c$ *and* $c \cdot (a+b) = c \cdot a + c \cdot b, \forall a, b, c \in \mathcal{R}$ *(distributivity).*

A ring is said to be commutative *if* $a \cdot b = b \cdot a, \forall a, b \in \mathcal{R}$.

Definition 4. *Let $(\mathcal{R}, +, \cdot)$ be a commutative ring and let $\mathcal{I} \subseteq \mathcal{R}$. $\mathcal{I}$ is called* ideal of $\mathcal{R}$ *if the following holds:*

- $(\mathcal{I}, +)$ *is a group.*
- $i \cdot r \in \mathcal{I}, \forall i \in \mathcal{I}, r \in \mathcal{R}$.

Definition 5. *A set F together with two laws of composition $+ : F \times F \to F, (a,b) \mapsto a+b$ and $\cdot : F \times F \to F, (a,b) \mapsto a \cdot b$ is called a* field *if the following holds:*

- $(F, +)$ *is an Abelian group.*
- $(F \setminus \{0\}, \cdot)$ *is an Abelian group.*
- $c \cdot (a+b) = c \cdot a + c \cdot b, \forall a, b, c \in F$.

Modular Arithmetic

Definition 6. *Two integers $a, b \in \mathbb{Z}$ are said to be* congruent modulo $n \in \mathbb{N}$, *if their difference $a - b$ is an integer multiple of n. We say that a is congruent to b modulo n and write it as*

$$a \equiv b \mod n. \tag{2}$$

Proposition 1. *For $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, the following equivalence holds:*

$$a \equiv b \mod n \Leftrightarrow \exists k \in \mathbb{Z} : a = b + kn. \tag{3}$$

Proposition 2. *For $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, it holds that*

a) $a \equiv 0 \mod n$, if and only if $n|a$.

b) $a \equiv a \mod n$ (reflexive).

c) $a \equiv b \mod n$, if and only if $b \equiv a \mod n$ (symmetric).

d) if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$ (transitive).

e) if $a \equiv b \mod n$ and $c \equiv d \mod n$, then

$$a + c \equiv b + d \mod n, \quad a - c \equiv b - d \mod n, \quad a \cdot c \equiv b \cdot d \mod n. \tag{4}$$

Proof. a) $a \equiv 0 \mod n \quad \Leftrightarrow \exists k \in \mathbb{Z} : a = kn \quad \Leftrightarrow n|a$.

b) $a - a = 0 \mod n$.

c) if $a \equiv b \mod n \quad \Leftrightarrow \exists k \in \mathbb{Z} : a - b = nk \quad \Leftrightarrow \exists k \in \mathbb{Z} : b - a = n(-k)$.

d) $\exists k, \ell \in \mathbb{Z} : a = b + nk, b = c + \ell \Rightarrow a = c + n(k + \ell) \quad \Rightarrow a \equiv c \mod n$.

e) $\exists k, \ell \in \mathbb{Z} : a = b + nk, c = d + \ell n \Rightarrow a + c = b + d + n(k + \ell) \Rightarrow a + c \equiv b + d \mod n$.

□

Proposition 3. *The relation $\equiv$ is an equivalence relation and defines equivalence classes on $\mathbb{Z}$ denoted as $a + m\mathbb{Z} := \{a + mz | z \in \mathbb{Z}\}$*

Proof. The proposition follows directly from *b*), *c*), and *d*). □

Definition 7. *The set of classes $\{a + m\mathbb{Z}|, a \in \mathbb{Z}\}$ is denoted $\mathbb{Z}/m\mathbb{Z}$. It contains m elements and can be identified with the set $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$.*

Definition 8. *Two integers $m, n \in \mathbb{N}$ are said to be relatively prime if* $\gcd(m, n) = 1$.

Theorem 1. 1) (Bézout) *Let $m, n \in \mathbb{Z}$ be any two integers, then there exist $p, q \in \mathbb{Z}$ (called Bézout numbers or Bézout coefficients) such that*

$$mp + nq = \gcd(m, n). \tag{5}$$

2) *Two integers m and n are relatively prime if there exist $p, q \in \mathbb{Z}$ such that*

$$mp + nq = 1. \tag{6}$$

Proposition 4. *$(\mathbb{Z}_m, +)$ is an Abelian group.*

Proof. We verify that the necessary conditions for the group are fulfilled:

a) We first show that the law $+$ is well defined on $\mathbb{Z}_m$: $a, b \in \mathbb{Z}_m \Rightarrow a+b \in \mathbb{Z}_m$ (closure).

b) $a, b, c \in \mathbb{Z}_m, a + (b + c) = (a + b) + c$ (associativity).

c) $0 \in \mathbb{Z}_m$ (neutral element).

d) $\forall a, -a \in \mathbb{Z}_m$ (inverse element).

$\square$

Proposition 5. *a invertible in $(\mathbb{Z}_m, \cdot)$ is equivalent to* $\gcd(a, m) = 1$.

Proof. "$\Rightarrow$": Assume a is invertible:

$$\exists b \in \mathbb{Z}_m : ab \equiv 1 \mod m \quad \Rightarrow \exists k \in \mathbb{Z} : ab - mk = 1, \tag{7}$$

and from Bézout's Theorem we can conclude that a and m are relatively prime. This is also easily obtained using that $d|a$ and $d|m$, such that $d|ab - mk = 1$.

"$\Leftarrow$": Assume $d = \gcd(a, m) = 1$, from Bézout's Theorem, $\exists p, q, \in \mathbb{Z} : ap + qm = 1$ which implies that $ap \equiv 1 \mod m$ and a is invertible in $\mathbb{Z}_m$. $\square$

Definition 9. *The set of all invertible elements of $\mathbb{Z}_m$ is called the* multiplicative group *of $\mathbb{Z}_m$ and denoted as $\mathbb{Z}_m^*$.*

Definition 10. *The Euler function φ is defined on $\mathbb{Z}$ as $\varphi(m) = |\mathbb{Z}_m^*|$, where $|\cdot|$ denotes the cardinal operator.*

Proposition 6. *$(\mathbb{Z}_m^*, \cdot)$ is an Abelian group.*

Proof.

- Associativity and commutativity are straightforward.
- $\forall a, b \in \mathbb{Z}_m^*, (a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ (closure).
- $\forall n \in \mathbb{Z}_m^*, n \cdot n^{-1} = 1 \in \mathbb{Z}_m^*$ (neutral element).
- $\forall n \in \mathbb{Z}_m^*, \exists n^{-1} \in \mathbb{Z}_m : n^{-1}n = 1 \Rightarrow n^{-1} \in \mathbb{Z}_m^*$ (inverse element).

$\square$

Proposition 7. *If m is prime, $\mathbb{Z}_m^*$=$\mathbb{Z}_m \setminus \{0\}$, and $\mathbb{Z}_m$ is a field.*

Proposition 8. *If $n = p_1^{k_1} \cdots p_r^{k_r}$ where the p_i is are distinct primes, then*

$$\varphi(n) = \varphi(p_1)p_1^{k_1-1} \cdots \varphi(p_r)p_r^{k_r-1} = (p_1 - 1)p_1^{k_1-1} \cdots (p_r - 1)p_r^{k_r-1}. \tag{8}$$

Particularly, $\varphi(p) = p - 1$ for p prime.

Theorem 2. *(Fermat,Euler) Let $a \in \mathbb{Z}_n^*$. Then*

$$a^{|\mathbb{Z}_n^*|} = a^{\varphi(n)} \equiv 1 \mod n. \tag{9}$$

In particular Fermat's little theorem *states that if p is prime and* $\gcd(a, p) = 1$ *(a and p are* relatively prime*), then $a^{p-1} \equiv 1 \mod p$.*

A straightforward generalization is then that if p is prime and m and n are positive integers such that $m \equiv n \mod p - 1$ then $\forall a \in \mathbb{Z}, a^m \equiv a^n \mod p$.