1 Preface

The mathematical framework employed in cryptography is the one offered by abstract algebra, in particular group theory and finite fields theory. These notes are provided as a support to the course and are by no means to be intended as a full fledged algebra course. For a complete tractation on the subject, we refer the interested reader to one or more of the following:

P.M.Cohn, *Classic Algebra*, 2000, John Wiley
M.Artin, *Algebra - 2nd edition*, 2010 Addison Wesley
Lidl R., Niederreiter H., *Introduction to finite fields and their applications* 1997, Cambridge University Press.

2 Elements of group theory

An algebraic structure is a pair $(\mathbf{S}, \Omega)$, where $\mathbf{S}$ is a set, commonly referred to as the support of the structure and Ω is a set of operations (with specific properties) acting on the elements of $\mathbf{S}$. If the support $\mathbf{S}$ has a finite number of elements, the structure is said to be finite and $|\ \mathbf{S}\ |$ is the order of the structure. Two structures are particularly useful in cryptography: groups and finite fields.

Definition 2.1 (Group)**.** *A group is a pair* $(\mathbf{G}, *)$*, where* $\mathbf{G}$ *is the support of the structure and* $*$ *is a binary, internal operation on* G*, i.e. a relation associating every pair* (a, b) *of elements of* $\mathbf{G}$ *to one and only one element* $c \in \mathbf{G}$ *(thus defined as* $a * b$*), in such a way that the following properties hold:*

- *Associative property:* $\forall a, b, c \in \mathbf{G}\ \ (a * b) * c = a * (b * c)$*,*
- *Existence of a neutral element*[1]*:* $\exists e \in \mathbf{G} : \forall a \in \mathbf{G}\ \ a * e = e * a = a$
- *Existence of the inverses*[2]*:* $\forall a \in \mathbf{G}\ \exists \overline{a} \in \mathbf{G} : a * \overline{a} = \overline{a} * a = e$

If the operation also exhibits the following,

- *Commutative property:* $\forall a, b \in \mathbf{G}\ \ a * b = b * a$

the group is said to be abelian *or* commutative*.*

The group operation is a generic binary operation, but we will denote it in the following part of these notes employing either:

- Additive notation: the operation will be denoted by $+$ and the neutral element will be called zero and denoted by 0. The inverse element of a will be denoted as $-a$ and may be called the opposite of a.
- Multiplicative notation: the operation $*$ will be called product, and denoted with either $\cdot$ or the simple concatenation of the two involved elements. The neutral element will be called unity and denoted with 1 and the inverse of the element a will be denoted by a^{-1}.

We observe that, thanks to the associativity of the operation, it is possible to define without problems the product of more than two elements of $\mathbf{G}$, without the need for parenthesization. In particular, the integer exponent powers can be defined as :

- $a^n = a \cdot a \cdot ... \cdot a$ repeated n times, if $n > 0$
- $a^n = e$, if $n = 0$
- $a^n = a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}$ repeated $(-n)$ times, if $n < 0$

The associativity and the definitions of inverse and neutral element make the usual properties of powers work:

- $a^n \cdot a^m = a^{n+m}$
- $(a^n)^m = a^{nm}$

[1] If there were two neutral elements e_1, e_2, they would be equal as $e_1 = e_1 * e_2 = e_2$

[2] Given a, if there were two inverse elements b, c, they would be equal as $b = b * e = b * (a * c) = (b * a) * c = e * c = c$

Observe that, employing additive notation, the n-th power of an element a will be denoted as na. Consequentially, the properties of the powers will be rewritten as

- $(na)+(ma) = (n+m)a$: This has nothing to do with distributive property, as our structure has only one operation, $+$)
- $m(na) = (mn)a$: This has nothing to do with the associativity between n and m , as they are not elements of $\mathbf{G}$, but merely indicating the number of repetitions of an addition

Example 2.1 (Examples of group structures)**.**

1. $(\mathbb{Z}, +)$ *is an abelian (commutative) group*
2. *The set* $\{A \in M_n(\mathbb{R}) \mid det\ A \neq 0\}$ *of square, nonsingular matrices over* $\mathbb{R}$*, with the usual matrix product is a* non *commutative group.*
3. $(\{1, -1, i, -i\}, \cdot)$ *is a finite abelian group*
4. *The set of bijective applications of a set* $\mathbf{X}$ *in itself, together with the usual composition of applications is a* non *abelian group.*
   If the set $\mathbf{X}$ *is finite and* $\mid \mathbf{X} \mid = n$*, the group is finite, has order* $n!$ *and is known as symmetric group over* $\mathbf{X}$ *(known also as* S_n*).* S_3 *is the smallest example of non-commutative finite group. E.g.,* $\pi_1 = (13)(2)$*,* $\pi_2 = (132)$*,* $\pi_1 \circ \pi_2 \neq \pi_2 \circ \pi_1$*.*

Definition 2.2 (Subgroup)**.** *A subset* $\mathbf{H}$ *of a group* $(\mathbf{G}, \cdot)$ *is a subgroup of* $\mathbf{G}$ *if the "group properties" hold for* $(\mathbf{H}, \cdot)$*, where* $\cdot$ *is the same operation in* $(\mathbf{G}, \cdot)$*.*

Note that to check whether $(\mathbf{H}, \cdot)$ is a subgroup of $(\mathbf{G}, \cdot)$ it is sufficient that one of these three criteria holds.

1. $(\mathbf{H}, \cdot)$ is a subgroup of $(\mathbf{G}, \cdot)$ if and only if $\forall h, k \in \mathbf{H}$ we have that $h \cdot k \in \mathbf{H}$ and $h^{-1} \in \mathbf{H}$.
2. $(\mathbf{H}, \cdot)$ is a subgroup of $(\mathbf{G}, \cdot)$ if and only if $\forall h, k \in \mathbf{H}$ we obtain that $h \cdot k^{-1} \in \mathbf{H}$.
3. Let $\mathbf{H}$ a finite subset of $\mathbf{G}$, $(\mathbf{H}, \cdot)$ is a subgroup of $(\mathbf{G}, \cdot)$ if and only if $\forall h, k \in \mathbf{H}$ we have that $h \cdot k \in \mathbf{H}$.

Example 2.2. *Examples of subgroups of* $(\mathbf{G}, \cdot)$

1. *The subsets* $\{e\}$ *and* $\mathbf{G}$ *are trivial subgroup of the group* $(\mathbf{G}, \cdot)$*.*
2. *The set* $\mathbf{P}$ *of all the even numbers is a subgroup of* $(\mathbb{Z}, +)$*.*
3. *The set* $n\mathbb{Z}$ *of all numbers that are a multiple of* n *is a subgroup of* $(\mathbb{Z}, +)$*.*
4. *The set* $\{A \in M_n(\mathbb{R}) \mid det\ A = \pm 1\}$ *is a subgroup of the group of non-singular square matrices with respect to the matrix-product* $(\{A \in M_n(\mathbb{R}) \mid det\ A \neq 0\}, \cdot)$
5. *The set* $\{1, -1\}$ *is a subgroup of* $(\{1, -1, i, -i\}, \cdot)$

Definition 2.3 (Coset)**.** *Let* $(\mathbf{G}, \cdot)$ *be a group,* $\mathbf{H}$ *one of its subgroups and* g *a generic element* $g \in \mathbf{G}$*; the subset* $\mathbf{H} \cdot g = \{h \cdot g \mid h \in \mathbf{H}\}$ *(respectively,* $g \cdot \mathbf{H} = \{g \cdot h \mid h \in \mathbf{H}\}$*) of* $\mathbf{G}$ *is called "the right (resp. left) coset*[3]*" of* $\mathbf{H}$ *in* $\mathbf{G}$ *with representative element* g*.*

If we are willing to rewrite the former definition in additive notation, the right coset of $\mathbf{H}$ in $\mathbf{G}$ having g as representative element will be denoted by $\mathbf{H} + g$ and will contain the elements $\{h + g \mid h \in \mathbf{H}\}$.

Example 2.3. *Consider the group* $\mathbf{G} = (\mathbb{Z}, +)$ *and the subgroup* $\mathbf{H} = (5\mathbb{Z}, +)$*. Given a generic element* $g \in \mathbf{G} \setminus \mathbf{H}$*, we can build the following the set:*

$$\mathbf{H} + g = g + \mathbf{H} = \{g + 5l, l \in \mathbb{Z}\} = \{a \in \mathbb{Z}, a \equiv g \bmod 5\}.$$

The last equality is justified by the observation that considering two elements of the set, say them $g + 5l_1$*,* $g + 5l_2$*, the modulo 5 divides their difference (i.e., the result of the first plus the opposite of the second) thus each element in the set can be expressed as the remainder of the division of* g *by* 5 *plus a multiple of* 5*. The set* $\mathbf{H} + g = g + \mathbf{H}$ *is a right and a left coset of* $\mathbf{H} = (5\mathbb{Z}, +)$*.*
Each coset includes an infinite number fo elements, although it is easy to recognize only five distinct cosets $\mathbf{H}$*,* $\mathbf{H} + 1$*,* $\mathbf{H} + 2$*,* $\mathbf{H} + 3$*,* $\mathbf{H} + 4$*.*

Definition 2.4 (Equivalence relation of group modulo a subgroup)**.**
Let $(\mathbf{G}, \cdot)$ *be a group and* $(\mathbf{H}, \cdot)$ *one of his subgroups, the binary relation* $\sim_{\mathbf{H}}$ *between two elements* g, k *of the group* $\mathbf{G}$ *denoted as* $g \sim_{\mathbf{H}} k$ *is defined as:*

$$g \sim_{\mathbf{H}} k \iff g = h \cdot k, \text{ for some } h \in \mathbf{H} \iff g \cdot k^{-1} \in \mathbf{H}$$

and is stated as "g *is equivalent to* k *modulo* $\mathbf{H}$*" as it is an* equivalence relation *(i.e., a relation between two elements of the group exhibiting the symmetric, reflexive and transitive property).*

Indeed, since $\mathbf{H}$ is a group, the existence of a single neutral element allows to state that $e = g \cdot g^{-1} \in \mathbf{H} \Leftrightarrow g \sim_{\mathbf{H}} g$ (reflexive prop.);
the existence of the inverse of every element in a group allows to state that if $g \sim_{\mathbf{H}} k \Leftrightarrow g \cdot k^{-1} \in \mathbf{H}$ then also $(g \cdot k^{-1})^{-1} = k \cdot g^{-1} \in \mathbf{H} \Leftrightarrow k \sim_{\mathbf{H}} g$ (symmetric prop.).
Finally, if $g \sim_{\mathbf{H}} k$ and $k \sim_{\mathbf{H}} l$, noting that $g \cdot k^{-1} \in \mathbf{H}$, and $k \cdot l^{-1} \in \mathbf{H}$, $g \cdot k^{-1} \cdot k \cdot l^{-1} \in \mathbf{H} \Leftrightarrow g \sim_{\mathbf{H}} l$ (transitivity prop.).

Example 2.4. *Consider the group* $\mathbf{G} = (\mathbb{Z}, +)$ *and the subgroup* $\mathbf{H} = (5\mathbb{Z}, +)$*. Given* $g, k \in \mathbf{G}$*, stating that "*g is equivalent to k modulo $\mathbf{H}$*", i.e.,* $g \sim_{\mathbf{H}} k$ *means that* $g - k \in \mathbf{H}$*, that is* $g - k$ *is a multiple of* 5*, which is also stated (with this choice of the group and subgroup) as "*g is congruent to k modulo 5*".*

An element $b \in \mathbf{G}$ is in the right coset $\mathbf{H} \cdot g$ if $b = h \cdot g$ for some $h \in \mathbf{H}$. Furthermore, $b = h \cdot g \Rightarrow b \cdot g^{-1} \in \mathbf{H}$, thus the set of b values equivalent to g (i.e., the equivalence class $[g]$) coincides with the right coset $\mathbf{H} \cdot g$:

$$[g] = \mathbf{H} \cdot g$$

[3] In italian "coset" is translated as "laterale"

As a consequence, the set of equivalence classes of $\mathbf{G}$ modulo $\mathbf{H}$ (or the set of cosets of $\mathbf{G}$ given the subgroup $\mathbf{H}$) defines a **partition** of $\mathbf{G}$.

Indeed, if $u \in [g_1]$ then $g_1 \sim u$ thus, by transitivity, u is equivalent to any other element in $[g_1]$, therefore $[u] = [g_1]$. Now if $u \in [g_1] \cap [g_2]$ we can conclude[4] that $[g_1] = [g_2]$. Thus, given g_1, g_2, their equivalence classes are either identical or disjoint. In other words, every element of $\mathbf{G}$ belongs to one and only one equivalence class (right coset) and so the equivalence classes (right cosets) form a partition of $\mathbf{G}$.

Given a set of representatives of all distinct right cosets of $\mathbf{H}$ (i.e., a set of representatives of the equivalence classess of $\mathbf{G}$ modulo $\mathbf{H}$), say it R, we have that:

$$\mathbf{G} = \bigcup_{g \in R} \mathbf{H} \cdot g$$

It is worth noting that $\forall\, g \in \mathbf{G}$, the map $\mathbf{H} \mapsto (\mathbf{H} \cdot g)$, is bijective. Indeed, assuming $h_1 \neq h_2$, the non-injectivity would mean that $h_1 \mapsto h_1 \cdot g$, and $h_2 \mapsto h_2 \cdot g$ and consequentially $h_1 g = h_2 g \Rightarrow h_1 = h_2$ (contradiction). To acknowledge the surjectivity of the map, it is sufficient to note that the set $\{h \cdot g, \forall h \in \mathbf{H}\}$ yields all the elements of the coset $\mathbf{H} \cdot g$ by definition.

From the said bijectivity, the number of elements in a coset $\mathbf{H} \cdot g$ coincides with the number of elements in the subgroup $\mathbf{H}$, i.e., $|\mathbf{H}| = |\mathbf{H} \cdot g|$.
Note that if you compose g with all the elements of $\mathbf{H}$ you obtain at most $|\mathbf{H}|$ outcomes. In order to prove that there are at least $|\mathbf{H}|$ outcomes, consider that in a right coset if $h_1 \cdot g = h_2 \cdot g$ with different $h_1, h_2 \in \mathbf{H}$, then you have a contradiction as composing both members of the previous equality with $(h_2 \cdot g)^{-1}$ yields $h_1 = h_2$.

Example 2.5. *Consider* $\mathbf{G} = (\mathbb{Z}, +)$, $\mathbf{H} = (5\mathbb{Z}, +)$ *and a generic element* $g \in \mathbf{G}$, *the* ***congruence modulo 5*** *defines an equivalence relation, with the coset* $\mathbf{H} + g$ *being constructed as* $5k + g$, *where* k *is any integer in* $\mathbb{Z}$ *(n.b.,* $(5k_1 + g) - (5k_2 + g) = 5(k_1 - k_2) \in \mathbf{H}$*).*
The equivalence classes (cosets), in this case are:
{...,-5,0,5,10,...}, {...-4,1,6,11,...}, {...-3,2,7,...}, {...-2,3,8,...}, {-1,4,9,...}.
Usually, we denote each class by choosing a representative element that coincides with the smaller non-negative element of the equivalence class: [0],[1],[2],[3],[4].

Theorem 2.1 (Lagrange's theorem)**.** *Let* $(\mathbf{G}, \cdot)$ *be a* **finite** *group of order* n. *If* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$, *then its order divides* n, *i.e,* $|\mathbf{H}| \mid n$.

Proof. Consider the relation $\sim_{\mathbf{H}}$ defined before: the $\sim_{\mathbf{H}}$-equivalence classes are distinct (i.e., are a partition of $\mathbf{G}$), have the same size and are in finite number. Denoting this number with r, we have that $|\mathbf{G}| = r|\mathbf{H}|$ □

We note that, in the general case, the inverse of Lagrange's theorem does not hold. However, the following theorem holds:

[4]Indeed, if the intersection is not the empty set, then $u \sim g_1$ and $u \sim g_2$ implies that $u = h_1 g_1 = h_2 g_2 \Rightarrow g_1 = (h_1^{-1} \cdot h_2) g_2 \Rightarrow g_1 \sim g_2 \Rightarrow [g_1] = [g_2]$; if the intersection is the empty set, then $[g_1] \neq [g_2]$

Theorem 2.2 (Inverse of Lagrange's theorem for **abelian** groups)**.**
Let $(\mathbf{G}, \cdot)$ *be a finite* abelian *group of order* n*.*
For each divider m *of* n *(i.e.,* $m \mid n$*), there exists at least a subgroup* $\mathbf{H}$ *with order* m*.*

As a consequence of Lagrange's theorem, we obtain the following

Definition 2.5 (Subgroup Index)**.**
Let $(\mathbf{G}, \cdot)$ *be a finite group and* $\mathbf{H}$ *one of its subgroups. It is possible to define the index of the subgroup* $\mathbf{H}$ *as the number of cosets of* $\mathbf{H}$ *in* $\mathbf{G}$*.*
This number is commonly indicated with $[\mathbf{G} : \mathbf{H}]$*, and can be obtained as* $\frac{|\mathbf{G}|}{|\mathbf{H}|}$*.*

2.1 Cyclic Groups

Definition 2.6 (Cyclic Group)**.**
Let $(\mathbf{G}, \cdot)$ *be a group. If the set of elements obtained iterating the group operation* $\cdot$ *on an element* $g \in \mathbf{G}$ *(i.e.,* $g^0 = e, g, g \cdot g = g^2$*,* $g^2 \cdot g = g^3, \ldots$*), denoted as* $\langle g \rangle$*, coincides with* $\mathbf{G}$*, then the group is said to be cyclic.*
We define g *as the* generator *of* $(\mathbf{G}, \cdot)$*.*

Definition 2.7 (Order of an element)**.**
Let $(\mathbf{G}, \cdot)$ *be a group and* g *be one of its elements. We define the* order of g *in* $(\mathbf{G}, \cdot)$*, denoting it with* $|g|$ *or* $o(g)$*, or* $\texttt{ord}(g)$*, the* **smallest positive integer** n *(assuming it exists) such that* $g^n = e$*.*
If n *exists, the element* $g \in \mathbf{G}$ *is said to be periodic, or with a finite order. Conversely, if there is no positive integer* n *such that* $g^n = e$*, the element* g *is said to have order* ∞ *(or zero order).*

- Note that $o(g) = |\langle g \rangle|$, this is true because if $o(g) = \infty$ then also in $\langle g \rangle$ we have that $g^n \neq g^m \forall n \neq m$ (otherwise $g^n = g^m \Rightarrow g^{n-m} = e \Rightarrow o(g) \leq \texttt{abs}(n - m)$); on the other hand, if $o(g) = n$, this integer is the smallest value such taht $g^n = e$ which means that $\langle g \rangle = \{g, g^2, \ldots, g^{n-1}, g^n = g^0 = e\}$ includes also all distinct elements because if it would not be case then there will be a pair of powers g^i, g^j with $0 \leq i \neq j < n$ such that $g^i = g^j \Rightarrow g^{\texttt{abs}(i-j)} = e \Rightarrow |\langle g \rangle| \leq \texttt{abs}(i - j) < n$ contradicting the minimality of the value n, therefore $o(g) = |\langle g \rangle|$.
- Note that taking a generic element $g \in (\mathbf{G}, \cdot)$, if $o(g) = n$ then $g^n = e \Leftrightarrow g^{n-1} \cdot g = e$ this implies that $g^{-1} = g^{n-1}$, and in general $g^{-i} = g^{n-i}$, thus every element in the set of powers $\langle g \rangle = \{g^0, g, g^2, \ldots, g^{n-1}\}$ admits an inverse, which implies that it is a subgroup of $\mathbf{G}$.

Example 2.6 (Examples of cyclic groups)**.**

1. $(\mathbb{Z}, +)$ *is a cyclic group. Its generators are* 1 *and* -1*, thus we can write* $(\langle 1 \rangle, +) = (\langle -1 \rangle, +) = (\mathbb{Z}, +)$
2. *The group of even numbers under addition* $(\mathbf{E}, +)$ *is a cyclic subgroup of* $(\mathbb{Z}, +)$ *generated by either* 2 *or* -2
3. $(\{1, -1, i, -i\}, \cdot)$ *is a finite cyclic subgroup, generated by either* i *or* $-i$ *(neutral element* 1*)*

4. $(\{1,-1\},\cdot)$ *is a cyclic group, generated by* -1

Every cyclic group is trivially Abelian (follows directly from the properties of powers).

Theorem 2.3 (Subgroup of a cyclic group)**.**
Every subgroup of a cyclic group is cyclic.

Proof. Let $(\langle g\rangle,\cdot)$ be a cyclic group and let $\mathbf{H}$ be a subgroup of $\langle G\rangle$.

In case $\mathbf{H}$ contains only the neutral element e (denoted, from now on as 1), $\mathbf{H}=\langle 1\rangle$ is trivially cyclic.

In case $\mathbf{H}\neq\langle 1\rangle$ then $g^n\in\mathbf{H}$ for some integer n (since every element in $\mathbf{G}$ has the form g^n and $\mathbf{H}$ is a subgroup of $\mathbf{G}$).

Let m be the smallest positive integer such that $g^m\in\mathbf{H}$ and consider an arbitrary element $b\in\mathbf{H}$. Then, $b=g^n$ for some n. Dividing n by m, we obtain that $n=mq+r$, where $q=\lfloor n/m\rfloor$ and $0\leq r<m$.
We can thus state that $g^r=g^n\cdot(g^m)^{-q}\in\mathbf{H}$, due to the closure property of the group operation. However, m was the smallest positive integer such that $g^m\in\mathbf{H}$ and $0\leq r<m$, so $r=0$.
Therefore $n=qm$ and $b=g^n=(g^m)^q$.
We conclude that any arbitrary element $b=g^n\in\mathbf{H}$ is generated by g^m so $\mathbf{H}=\langle g^m\rangle$ is cyclic. □

Example 2.7 (Integers and residue classes modulo n)**.**
$(\mathbb{Z},+)$ *is cyclic group, therefore any of its subgroups is also cyclic.*
We note that the non-trivial subgroups of $(\mathbb{Z},+)$ *are in the form of:*
$\mathbf{H}=\{h\cdot n|h\in\mathbb{Z}\}$ *with* $n>1$.
We now consider the cosets $\mathbf{H},\mathbf{H}+1,\ldots,\mathbf{H}+i\ldots\mathbf{H}+(n-1)$ *which are the equivalence classes modulo* n *as:*

$$a,b\in\mathbf{H}+i,\ \Leftrightarrow(a \bmod n)\equiv(b \bmod n)\Leftrightarrow\exists h\in\mathbb{Z}\ s.t.\ a-b=hn$$

The set of the equivalence classes modulo n, $[0],[1],\ldots,[i]=\mathbf{H}+i,\ldots,[n-1]$ *where the representative element of each class is chosen as the smallest positive integer is usually denoted as* $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\{0,1,2,\ldots,n-1\}$.
It is easy to verify that $(\mathbb{Z}_n,+)$ *is a commutative cyclic group.*

Observation 2.1 (**Finite** Cyclic group properties)**.**
Let $(\mathbf{G},\cdot)$ *be a finite cyclic group and* $g\in\mathbf{G}$ *a generic element:*

- *Let* $|\mathbf{G}|=n$. $\mathbf{G}$ *is cyclic if and only if* $\exists g\in\mathbf{G}$ *such that* $|g|=n$.
- *If* $\exists t>0:g^t=1$, $|g|$ *divides* t. *We can deduce this observation from the fact that* g *has finite order* $|g|=m$, *dividing* t *by* m *we have that* $t=qm+r$, *with* $0\leq r<m$. *Thus* $g^r=g^{t-qm}=g^t\cdot(g^m)^{-q}=1$, *from which we derive* $r=0$, *which in turn implies that* $t=qm$, *that is* m *divides* t.
- *The set of all the powers of* g, $\{g,\ g^2,...,\ g^m,\ \ g^m=g^0=1\}$, *with* $m\leq n=|\mathbf{G}|$, *is a subgroup of* $(\mathbf{G},\cdot)$ *generated by* g, *with* $m=|\langle g\rangle|$ *as* $g^{-1}=g^{m-1}$ *and thus, for a generic* $0\leq h\leq(m-1)$, $g^{-h}=g^{m-h}$. *Consequentially, for the Lagrange's theorem:* $m\mid n$ *or* $|\langle g\rangle|\mid|\mathbf{G}|$.

- *If $(\mathbf{B}, \cdot)$ is a finite group with prime order, then $(\mathbf{B}, \cdot)$ is cyclic.*
  (This is true because for the Lagrange Th. it admits only subgroups with cardinality equal to 1 or equal to the order of $\mathbf{B}$ ... the trivial subgroups, i.e., $(\{1\}, \cdot)$ and itself, thus any element different from the neutral element is a generator.

- *If $|g| = n$ then $|g^h| = \frac{n}{\gcd(n,h)}$.*
  To prove this observation, let r be the order of $|g^h|$,
  we have that $(g^h)^r = g^{r\,h} = 1 \Rightarrow n|(r\,h)$.
  Consequentially, there exists an integer m such that $r\,h = m\,n$. In turn, dividing both members by $\gcd(n,h)$ we get:

$$r\,\frac{h}{\gcd(n,h)} = m\,\frac{n}{\gcd(n,h)}$$

  Observe that $\frac{h}{\gcd(n,h)}$ and $\frac{n}{\gcd(n,h)}$ are coprime by construction, we can thus conclude that:

$$\frac{n}{\gcd(n,h)} \mid r$$

  By contrast, (being r=$|g^h|$) we can observe that

$$(g^h)^{\frac{n}{\gcd(n,h)}} = (g^n)^{\frac{h}{\gcd(n,h)}} = 1 \Rightarrow r \mid \frac{n}{\gcd(n,h)}$$

  thus the only possible option is $r = \frac{n}{\gcd(n,h)}$

- *Given $(\mathbf{G}, \cdot)$=$\langle g \rangle$ and $|\mathbf{G}|$=n, elements g^h with h coprime with n generate $\mathbf{G}$.*
  The number of possible distinct generators of $(\mathbf{G}, \cdot)$ is the number of positive integers that are coprime with n and smaller than n.
  Indeed, if h and n are coprime, $\gcd(h,n) = 1$, thus $|g^h| = \frac{n}{1} = n$.

Definition 2.8 (Euler Totient function)**.**
Given a positive integer n, we consider the set:

$$\mathbf{E} = \{x \in \mathbb{N} \ : \ 1 \leq x \leq n-1, \ \gcd(x,n) = 1\}$$

The size of the aforementioned set $\mathbf{E}$ is denoted as Euler's Phi function of n (alternatively, Euler's Totient function):

$$\varphi(n) \ = |\ \{x \in \mathbb{N} \ : \ 1 \leq x \leq n-1, \ \gcd(x,n) = 1\}\ |$$

and provides the number of positive integers smaller than n coprime with n itself.

Lemma 2.1.
Let $n, m \in \mathbb{N} \setminus \{0\}$ with $n > m$, if $\gcd(n,m) = 1$ then $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Proof. Left as an exercise to the reader. □

Lemma 2.2. *Let p be a prime and $k \in \mathbb{N} \setminus \{0\}$*

$$\varphi(p^k) = p^k - p^{k-1}$$

Proof. $\varphi(p^k)$ provides the number of positive integers smaller than p^k, with no common factors with p^k. We now try to count all the integers smaller than p^k, which *have* a common factor with it. These integers must be multiples of p (i.e., $p, 2p, 3p, \dots p^2, 2p^2, \dots, p^{k-1}$). Therefore, the number of integers having a common factor with p^k is p^{k-1} and thus, by difference, $\varphi(p^k) = p^k - p^{k-1}$. □

Observation 2.2. *We can thus rephrase the last observation on cyclic groups saying that a finite cyclic group $(\mathbf{G}, \cdot)$ with order n has $\varphi(n)$ generators.*

Observation 2.3. *Every integer number $m \in \mathbb{N}^+$ has a unique prime factors decomposition $m = \prod_{i=1}^{s} p_i^{\alpha_i}$, where p_i are distinct primes and α_i are positive integer numbers.*
Knowing the prime factors decomposition it is easy to compute the Euler's Phi function as:

$$\varphi(m) = \varphi(\prod_{i=1}^{s} p_i^{\alpha_i}) = \prod_{i=1}^{s} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = m \prod_{i=1}^{s} (1 - \frac{1}{p_i})$$

Theorem 2.4 (Inverse of the Lagrange's Theorem for finite cyclic groups)**.**
A cyclic group $(\mathbf{G}, \cdot)$ with $|\mathbf{G}| = n$ has one and only one subgroup of order m for every possible divider of n.

Proof. Let g be the generator of $\mathbf{G}$ and $d = \frac{n}{m}$.
Consequently, $\langle g^d \rangle$ is a subgroup of $(\mathbf{G}, \cdot)$ of order m.
Let $\mathbf{K}$ be another subgroup of $\mathbf{G}$ with order m.
As a subgroup of the cyclic group $(\mathbf{G}, \cdot)$, $\mathbf{K} = \langle g^r \rangle$ for a certain value of r.
From this, we deduce $g^{r\,m} = 1 \Rightarrow n | rm \Leftrightarrow n \cdot l = r \cdot m$ for some integer l, which in turn implies that $r = l\frac{n}{m} = ld$ and thus $g^r = (g^d)^l$.
From this, we obtain $\mathbf{K} \subseteq \langle g^d \rangle$, but $|\mathbf{K}| = m$, thus $\mathbf{K} = \langle g^d \rangle$. □

3 Elements of Ring Theory

Definition 3.1 (Ring)**.** *A ring is an algebraic structure with two binary operations* $(\mathbf{R}, +, \cdot)$ *such that the following properties hold:*

- $(\mathbf{R}, +)$ *is an abelian group, and is commonly called additive group of the ring*
- $\cdot$ *is an internal, associative composition law on* $\mathbf{R}$*, i.e. for all* $a, b, c \in \mathbf{R}$*,* $(a \cdot b) \cdot c = a \cdot (b \cdot c) \in \mathbf{R}$
- $\cdot$ *is distributive with respect to* $+$*, that is* $\forall a, b, c \in \mathbf{R}$ *we have that* $a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c$

If there exists a neutral element with respect to $\cdot$ this is commonly called unity, notated with 1, and the ring is known as *ring with unity*. If $\cdot$ commutes, the ring is known as *commutative ring*.

Example 3.1 (Ring Examples)**.**

1. *The set of square matrices, with order* n *and elements in* $\mathbb{R}$ *is a ring with unity with respect to the usual matrix sum and product(the unity being the identity matrix of order* n*)*
2. *The set* $\mathbb{Z}$ *of signed integers is a commutative ring with unity with respect to the usual sum and product*
3. *The set of polynomials, with real coefficients, in the unknown* x *are a commutative ring with unity with respect to the usual sum and product of polynomials*
4. *Let* n *be an integer greater than* 1*,* $(\mathbb{Z}_n, +, \cdot)$ *(where* $+$ *is the sum modulo* n *and* $\cdot$ *the product modulo* n*) is a commutative ring with unity*

The following properties can be immediately verified: Given a ring $(\mathbf{R}, +, \cdot)$, let $\mathbf{0}$ and $-a$ be the neutral element and the inverse element of a, respectively, with respect to the $+$ operation. We have that:

- $\forall a \in \mathbf{R},\ a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$
- $\forall a, b \in \mathbf{R},\ a \cdot (-b) = (-a) \cdot b = -(ab)$

Definition 3.2 (Zero divisors)**.** *Let* $(\mathbf{R}, +, \cdot)$*,* $a, b \in \mathbf{R}$*. If* $a \neq \mathbf{0}$ *and* $b \neq \mathbf{0}$*, but* $a \cdot b = 0$*, then* a *and* b *are called* zero divisors *in* $\mathbf{R}$*.*

This definition is mutuated by the fact that in $\mathbf{R}$, a divides $\mathbf{0}$ (with quotient b).

Lemma 3.1 (Cancellation Law)**.** *A ring* $(\mathbf{R}, +, \cdot)$ *does not have any zero dividers if and only if the cancellation laws hold. This means that if* $a \cdot b = a \cdot c$ *and* $b \cdot a = c \cdot a$*, with* $a, b, c \in \mathbf{R}$ *and* $a \neq 0$*, then* $b = c$*.*

Definition 3.3 (Integral Domain)**.** *We define integral domain a commutative ring with unity and without any zero divisors.*

Example 3.2 (Sample integral domains)**.**

1. $(\mathbb{Z}, +, \cdot)$ *is an integral domain*
2. $(\mathbb{R}[X], +, \cdot)$ *is an integral domain*

Definition 3.4 (Division Ring (also known as Skew Field))**.** *We define Division Ring a ring* $(\mathbf{R}, +, \cdot)$ *where* $(\mathbf{R} \setminus \{0\}, \cdot)$ *is a group (i.e. there are multiplicative inverses for all non-zero elements of the support)*

Theorem 3.1. *Every finite integral domain is a division ring.*

Definition 3.5 (Commutative Field)**.** *A commutative field is defined as a division ring* $(\mathbf{R}, +, \cdot)$ *where the operation* $\cdot$ *is commutative.*

Theorem 3.2 (Wedderburn's little)**.** *Every finite division ring is a commutative field (called Galois Field).*

Example 3.3.

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *with the common addition and multiplication operations are commutative fields.*
2. *Let* p *be a prime number,* $(\mathbb{Z}_p, +, \cdot)$ *is a finite field.*
3. $(\mathbb{F}[X], +, \cdot)$ *is an integral domain for every possible commutative field* $(\mathbb{F}, \oplus, \odot)$*.*

1 Euclid's algorithm

On the integral domains $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{F}[X], +, \cdot)$ it is possible to define the common notion of order relation (between integer or polynomials) and the common notion of division between elements, for such a reason they are also called *Euclidean Domains.*

Definition 1.1 (Greatest Common divisor)**.** *Let* $\mathbf{D}$ *be either* $(\mathbb{Z}, +, \cdot)$ *or* $(\mathbb{F}[X], +, \cdot)$*. The* Greatest Common Divisor *between any two elements* $a, b \in D$*,* $\gcd(a, b)$*, is defined as the element* $d \in \mathbf{D}$ *such that* $d|a$*,* $d|b$ *and* $\forall y \in D$*,* $y|a \wedge y|b \Rightarrow y|d$*.*

Informally, we recall that, given $a, b \in \mathbf{D}$ if $d \in \mathbf{D}$ is their gcd, then d divides also every linear combination of them, that is: $d|(\xi \cdot a + \eta \cdot b)$ with $\xi, \eta \in \mathbf{D}$.

Considering any two elements $a, b \in \mathbf{D}$, it is possible to prove, together with the existence of a gcd d also the existence of at least a pair of elements $x_a, x_b \in \mathbf{D}$ such that

$$d = x_a a + x_b b$$

This result will allow us to compute the multiplicative inverse in a finite field.

Lemma 1.1. *Given two elements* $a, b \in \mathbf{D}$*, with* $a \geq b > 0$*; if* $\mathbf{D}$ *is either* $(\mathbb{Z}, +, \cdot)$ *or* $(\mathbb{F}[X], +, \cdot)$ *we can define the concept of quotient, that is* $q = \lfloor a/b \rfloor$*. Once the definition of quotient is given, we define as remainder* $r = a \bmod b = a - qb \in \{0, 1, 2 \ldots, b-1\}$*. Assumed these premises, the following equality holds:*

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

In case one of the operands is zero we assume that $\gcd(a, 0) = a$*,* $\forall\, a \in \mathbf{D}$

Employing the previous lemma, it is possible to write down the following relations:

$a > b > 0$	$d = \gcd(a, b)$
$r_0 = a$	
$r_1 = b$	$d = \gcd(r_0, r_1)$
$r_2 = r_0 \bmod r_1 = r_0 - \lfloor r_0/r_1 \rfloor r_1;\ \ 0 \leq r_2 < r_1$	$d = \gcd(r_1, r_2)$
$r_3 = r_1 \bmod r_2 = r_1 - \lfloor r_1/r_2 \rfloor r_2;\ \ 0 \leq r_3 < r_2$	$d = \gcd(r_2, r_3)$
$r_4 = r_2 \bmod r_3 = r_2 - \lfloor r_2/r_3 \rfloor r_3;\ \ 0 \leq r_4 < r_3$	$d = \gcd(r_3, r_4)$
$\ldots$	$\ldots$
$r_n = r_{n-2} \bmod r_{n-1} = r_{n-2} - \lfloor r_{n-1}/r_{n-2} \rfloor r_{n-2};\ \ r_n = 0$	$d = \gcd(r_{n-1}, 0)$

for a given integer n the following hold:

$$d = \gcd(a, b) = r_{n-1}$$

Rewrite now all the steps as a linear combination of a, b only:

$$
\begin{aligned}
&a > b > 0 \\
&r_0 = 1 \cdot a + 0 \cdot b \\
&r_1 = 0 \cdot a + 1 \cdot b \\
&r_2 = r_0 \bmod r_1 = (1a + 0b) - \lfloor \tfrac{r_0}{r_1} \rfloor (0a + 1b) = (\xi_2 a + \eta_2 b);\ 0 \leq r_2 < r_1 \\
&r_3 = r_1 \bmod r_2 = (0a + 1b) - \lfloor \tfrac{r_1}{r_2} \rfloor (\xi_2 a + \eta_2 b) = (\xi_3 a + \eta_3 b);\ 0 \leq r_3 < r_2 \\
&r_4 = r_2 \bmod r_3 = (\xi_2 a + \eta_2 b) - \lfloor \tfrac{r_2}{r_3} \rfloor (\xi_2 a + \eta_2 b) = (\xi_4 a + \eta_4 b);\ 0 \leq r_4 < r_3 \\
&\dots \\
&r_{n-1} = r_{n-3} \bmod r_{n-2} = (\xi_{n-3} a + \eta_{n-3} b) - \lfloor \tfrac{r_{n-3}}{r_{n-2}} \rfloor (\xi_{n-2} a + \eta_{n-2} b) = \\
&\qquad = (\xi_{n-1} a + \eta_{n-1} b);\ 0 \leq r_{n-1} < r_{r-2} \\
&r_n = r_{n-2} \bmod r_{n-1} = (\xi_{n-2} a + \eta_{n-2} b) - \lfloor \tfrac{r_{n-3}}{r_{n-2}} \rfloor (\xi_{n-1} a + \eta_{n-1} b) = \\
&\quad = (\xi_n a + \eta_n b);\ r_n = 0
\end{aligned}
$$

thus,

$$d = r_{n-1} = \xi_{n-1} a + \eta_{n-1} b;\ \ \xi, \eta \in D$$

Formalizing properly the previous derivations, we obtain the Euclid's algorithm for the computation of the greatest common divisor.

Algorithm 1.1: Extended Euclid Algorithm

Input: $a, b \in D$
Output: $d = \xi \cdot a + \eta \cdot b,\ \xi, \eta \in \mathbf{D}$

1 **begin**
2 $\underline{u} \leftarrow (a, 1, 0)$ `// array with three elements:` $u[0], u[1], u[2]$
3 $\underline{v} \leftarrow (b, 0, 1)$
4 **repeat**
5 $\underline{w} \leftarrow \underline{u} - \lfloor \frac{\underline{u}[0]}{\underline{v}[0]} \rfloor \cdot \underline{v}$
6 $\underline{u} \leftarrow \underline{v}$
7 $\underline{v} \leftarrow \underline{w}$
8 **until** $(w[0] = 0)$
9 $d \leftarrow \underline{u}[0],\ \xi \leftarrow \underline{u}[1],\ \eta \leftarrow \underline{u}[2]$
10 **return** (d, ξ, η)

The algorithm can be re-written to make use of only subtraction operations with a computational complexity linear in the bit-length of the input operands and equal to $\mathcal{O}\big(2 \log(\max\{a, b\})\big)$ addition/subtraction operations (Refer to Chap. 14, Menezes et al. *Handbook of Applied Cryptography*, CRC Press)

Example 1.1. *Let* $D =< Z, +, \cdot >$

$d = \gcd(11, 5) = 11\xi + 5\eta$*;*

$\underline{u} \leftarrow (11, 1, 0)$*;*
$\underline{v} \leftarrow (5, 0, 1)$*;*

$q = \lfloor \frac{11}{5} \rfloor = 2$*,* $\underline{w} \leftarrow (11 - 2 \cdot 5, 1 - 0 \cdot 2, 0 - 1 \cdot 2) = (1, 1, -2)$*;*
$\underline{u} \leftarrow (5, 0, 1)$*;*
$\underline{v} \leftarrow (1, 1, -2)$*;*

$q = \lfloor \frac{5}{1} \rfloor = 5$*,* $\underline{w} \leftarrow (5 - 1 \cdot 5, 0 - 1 \cdot 5, 1 - (-2) \cdot 5) = (0, -5, 11)$*;*
$\underline{u} \leftarrow (1, 1, -2)$*;*
$\underline{v} \leftarrow (0, -5, 11)$*;*

$d = 1$*;* $\xi = 1$*;* $\eta = -2$*.*

in fact: $1 = 1 \cdot 11 + (-2) \cdot 5$*.*

2 The Groups $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \cdot)$

These groups are particularly useful in cryptography.

We have seen that $(\mathbb{Z}_n, +)$ has cardinality $|(\mathbb{Z}_n, +)| = n$, and the inverse of any element a is computed as its opposite $-a \equiv |\mathbb{Z}_n| - a$.
It can be easily shown to be a cyclic group (indeed, the element 1 – identified with the equivalence class [1] – is a generator), while the number of generators is $\varphi(n)$.

Considering $(\mathbb{Z}_n^*, \cdot)$, the support $\mathbb{Z}_n^*$ must include the representatives of the equivalence classes modulo n with a multiplicative inverse (the symbol $*$ in $(\mathbb{Z}_n^*, \cdot)$ denotes that not every positive number smaller than n has such a property). Indeed, let us consider an integer $0 \leq x \leq n-1$ as a possible representative of equivalence classes in $\mathbb{Z}_n^*$ and the following two situations:

- $\texttt{gcd}(x, n) = 1$ – the number of values x satisfying this condition are $\varphi(n)$.
- $\texttt{gcd}(x, n) = d > 1$

In the former case, lifting the value of x in the integral domain $(\mathbb{Z}, +, \cdot)$, we can apply the extended Euclid algorithm to find the coefficients ξ, η in the following equality:

$$1 = x \cdot \xi + n \cdot \eta$$

Computing mod$n$ at both members, we can derive that

$$1 \bmod n = (x \cdot \xi) \bmod n = ((x \bmod n) \cdot (\xi \bmod n)) \bmod n$$

Thus, we can conclude that, the inverse of x in $(\mathbb{Z}_n^*, \cdot)$ is given by:

$$x^{-1} = (\xi \bmod n).$$

In the latter case, when $\texttt{gcd}(x, n) = d > 1$, we can easily prove that the considered value, x, does not belong to $(\mathbb{Z}_n^*, \cdot)$.
Indeed, assuming $x \in (\mathbb{Z}_n^*, \cdot)$ means that there should exist another element, say it z, such that $x \cdot z = 1 \bmod n \Rightarrow x \cdot z - 1 = 0 \bmod n \Rightarrow x \cdot z - 1 = n \cdot q$ for a proper integer q.
Dividing both members of the last equality by d, we can derive that
$\frac{x}{d} \cdot z - \frac{n}{d} \cdot q = \frac{1}{d}$, which is clearly false (...the difference of two integer numbers cannot be equal to $\frac{1}{d}$). Therefore, we can conclude that also the assumption that $x \in (\mathbb{Z}_n^*, \cdot)$ is false.

Overall, we can conclude that $(\mathbb{Z}_n^*, \cdot)$ has a cardinality $|(\mathbb{Z}_n^*, \cdot)| = \varphi(n)$.
It is important to establish with which values of n, the group $(\mathbb{Z}_n^*, \cdot)$ is cyclic and, in such a case, how many generators it has.

Theorem 2.1. *The group $(\mathbb{Z}_n^*, \cdot)$ is cyclic if and only if n=1, 2, 4, n=p^k, n=2p^k where $k \geq 1$ and $p \geq 3$ is a prime integer.*

It is worth noting that $(\mathbb{Z}_p^*, \cdot)$ is a cyclic multiplicative group with cardinality $|(\mathbb{Z}_p^*, \cdot)| = \varphi(p) = p - 1$ thus, $\mathbb{Z}_p^* = \mathbb{Z} \backslash \{0\}$, and has a number of generators equal to $\varphi(|(\mathbb{Z}_p^*, \cdot)|) = \varphi(\varphi(p)) = \varphi(p-1) = |\{1 \leq h < p-1 : \gcd(p-1, h) = 1\}|$.

Proposition 2.1 (Numerical Finite fields)**.** *The finite group $(\mathbb{Z}_p^*, \cdot)$ is cyclic and also the finite group $(\mathbb{Z}_p, +)$ is cyclic therefore, the structure $(\mathbb{Z}_p, +, \cdot)$ is a* ***finite field****. The field $(\mathbb{Z}_p, +, \cdot)$ is also denoted as $\mathbb{Z}/(p)$ or $\mathbb{Z}/p\mathbb{Z}$.*

2.1 Computing inverses in $(\mathbb{Z}_n^*, \cdot)$

The inverses in $(\mathbb{Z}_n^*, \cdot)$ with any $n \geq 2$ can be computed in two distinct ways:

- either through the extended Euclid algorithm
- or via the properties of the groups

In particular, since $(\mathbb{Z}_n^*, \cdot)$ is a finite group with order $|\mathbb{Z}_n^*| = \varphi(n)$, each one of its elements will have an order dividing $\varphi(n)$ (... indeed, the set of powers of an element x is a subgroup of $\mathbb{Z}_n^*$ and the Lagranges' Th. guarantees that its order is a factor of $\varphi(n)$). Consequently, it is true that:

$$x \in \mathbb{Z}_n^*,\ x^{\varphi(n)} \equiv 1 \mod n, \quad \text{(relation known as Euler's theorem)}$$

Therefore

$$x \in \mathbb{Z}_n^*,\ x^{\varphi(n)} \equiv 1 \mod n \ \Rightarrow\ x^{-1} \equiv x^{\varphi(n)-1} \mod n$$

An efficient method for computing a modular exponentiation is essential. The most naive way to compute a^n is to do $n - 1$ multiplications of the element a with itself. In practical applications most choices of n are large enough that it would be infeasible to compute a^n using $n - 1$ successive multiplications by a. There are two ways to reduce the time required to do an exponentiation. One way is to decrease the time to multiply two elements in the group; the other is

to reduce the number of multiplications used to compute a^n. Ideally, one would do both. We now consider the general techniques for exponentiation.

The problem can be re-formulated as follows: Given $a, n \in \mathbb{N}$, we want to compute the integer $c = a^n$ through employing a number of multiplications much smaller than n.
Let t be the number of binary digits necessary to encode the value n, that is:

$$t = \lceil \lg_2 n \rceil,\ n = (n_{t-1}, \ldots, n_1, n_0) \text{ with } n_i \in \{0, 1\},\ i \in \{0, 1, \ldots, t-1\}$$

we can write that:

$$c = a^n = a^{\sum_{j=0}^{t-1} n_j 2^j} = a^{n_{t-1}2^{t-1} + n_{t-2}2^{t-2} + \ldots + n_1 2^1 + n_0} \tag{1}$$

Depending on the way we read (interpret) the last member of the above equality chain, two different exponentiation algorithms (known as *Square and Multiply(S&M) algorithms*) can be formulated.

2.1.1 Square and Multiply - Left to Right

Assuming to scan the bits of the exponent n in the equation (1) from left to right, the following equality holds:

$$c = a^n = ((\cdots((a^{n_{t-1}})^2 \cdot a^{n_{t-2}})^2 \cdots)^2 \cdot a^{n_1})^2 \cdot a^{n_0}$$

Example 2.1. *Given the following operation $c = 5^6$; we have that $a = 5$, $t = 3$, $n = 6_{\text{decimal}} = \langle 110 \rangle_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, then:*

$$c = 5^{\langle 110 \rangle_2} = ((5^1)^2 \cdot 5^1)^2 \cdot 5^0 = (5^2 \cdot 5)^2 = 15625.$$

The computational cost of this method, expressed in terms of squarings and multiplications needed to compute the final result, is (on average): $t-1$ squarings, plus $\frac{1}{2}(t-1)$ multiplications, with $t = \lceil \lg_2 n \rceil$.

Algorithm 2.1: S&M Left to Right

Input: a, n, $t = \lceil \lg_2 n \rceil$, $n = (n_{t-1}, \ldots, n_1, n_0), n \geq 0$
Output: $c = a^n$

```
1 begin
2     if n = 0 then
3         return 1
4     c ← a
5     for i ← t − 2 down-to 0 do
6         c ← c^2
7         if n_i = 1 then
8             c ← c · a
9     return c
```

2.1.2 Square and Multiply - Right to Left

Assuming to scan the bits of the exponent n in the equation (1) from right to left, the following equality holds:

$$c = a^n = (a^{2^0})^{n_0} \cdot (a^{2^1})^{n_1} \cdot (a^{2^2})^{n_2} \cdots (a^{2^{t-1}})^{n_{t-1}}$$

Example 2.2. *Given the following operation $c = 5^6$; we have that $a = 5$, $t = 3$, $n = 6 = \langle 110 \rangle_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, then:*

$$c = 5^{110_2} = (5^{2^0})^0 \cdot (5^{2^1})^1 \cdot (5^{2^2})^1 = (5 \cdot 5^2 \cdot 5^4) = 15625.$$

Note that the factor a^{2^j} can be computed re-using the previous factor and employing only one squaring operation: $\left(a^{2^{j-1}}\right)^2$

Analogously to the previous method, the computational cost of this technique, expressed in terms of squarings and multiplications needed to compute the final result, is (on average): $t-1$ squarings, plus $\frac{1}{2}(t-1)$ multiplications, with $t = \lceil \lg_2 n \rceil$.

Algorithm 2.2: S&M Right to Left

Input: a, n, $t = \lceil \lg_2 n \rceil$, $n = (n_{t-1}, \ldots, n_1, n_0), n \geq 0$
Output: $c = a^n$

```
1  begin
2      if n = 0 then
3          return 1
4      b ← a
5      if n_0 = 1 then
6          c ← a
7      else
8          c ← 1
9      for i ← 1 to t − 1 do
10         b ← b^2
11         if n_i = 1 then
12             c ← c · b
13     return c
```

A generalization of the S&M algorithms consists of processing more than one exponent bit at time (which is equivalent to encode the exponent in a numerical base $b = 2^k$ for some k), to trade-off the storage needed for some pre-computation with the efficiency of the squaring and multiplication operations. For example:

Algorithm 2.3: Window method

Input: a, n, $t = \lceil \lg_b n \rceil$, $n = (n_{t-1}, \ldots, n_1, n_0)$, $n \geq 0$, $b = 2^k$
Output: $c = a^n$

```
1  begin
2      if n = 0 then
3          return 1
4      g_0 ← 1
5      for i ← 1 to 2^k − 1 do
6          g_i ← g_{i−1} · a
7      c ← g_{n_{t−1}}
8      for i ← t − 2 down-to 0 do
9          c ← c^{2^k}
10         if n_i ≠ 0 then
11             c ← c · g_{n_i}
12     return c
```

3 Chinese remainder theorem (CRT)

Due to its usefulness in implementing efficient cryptosystems, we recall the following very old piece of mathematics, which dates back at least 2000 years. We shall use the CRT in a few places, for example to improve the performance of the decryption operation of RSA and in a number of other protocols.

Theorem 3.1 (Chinese Remainder Theorem)**.**
Let $n_1, \ldots, n_k$ be k positive integers pairwise coprime, and let $x_1, \ldots, x_k$ be k elements of $\mathbb{Z}$. The following system of modular congruences

$$\begin{cases} X \equiv x_1 \pmod{n_1} \\ X \equiv x_2 \pmod{n_2} \\ X \equiv x_3 \pmod{n_3} \\ \cdots \\ X \equiv x_k \pmod{n_k} \end{cases}$$

has a unique solution $\overline{X}$ such that $0 \leq \overline{X} < N$, with $N = \prod_{i=1}^{k} n_i$.

Theorem 3.2 (Chinese Remainder Theorem - alternate definition)**.**
Let X, n be positive integers, such that:

$$N = \prod_{i=1}^{k} n_i = n_1 \cdot n_2 \cdot n_3 \cdot \cdots \cdot n_k$$
$$\forall i, j \in \{1, \ldots, k\}, i \neq j \quad gcd(n_i, n_j) = 1$$

The relation

$$X \mapsto (x_1, x_2, \ldots, x_n)$$
$$\text{with} \quad X \equiv x_i \bmod n_i \quad (0 \leq x_i < n_i)$$

is bijective.

Proof. (Sketch)

- Given X and a k-uple of integers, $(n_1, n_2, \ldots, n_k)$ pairwise coprime, proving that there is only one k-uple $\{x_1, x_2, \ldots, x_k\}$, with $0 \leq x_i < n_i$, fitting the relation is trivial: it is sufficient to consider the k-uple ($X \bmod n_1, X \bmod n_2, \ldots, X \bmod n_k$) for the relation to hold.
- We now prove that given a k-uple $(x_1, x_2, \ldots, x_k)$, $0 \leq x_i < n_i$, such that $\forall i \neq j$ $\gcd(n_i, n_j) = 1$, it is possible to associate only one positive integer $X \bmod N$ with $N = \prod_{i=1}^{k} n_i$.

  In order to do so, let M_i and M_i' be: $M_i = \frac{N}{n_i}$ and $M_i' = M_i^{-1} \bmod n_i$, respectively. Note that it is always possible to compute M_i' since all the n_i values are coprime by construction with M_i.
  We note that:

  $$M_i \cdot M_i' \equiv 1 \bmod n_i \qquad \forall i \in \{1, 2, \ldots, k\}$$
  $$M_i \cdot M_i' \equiv 0 \bmod n_j \qquad \forall i \in \{1, 2, \ldots, k\}, j \neq i$$

  The first observation is rather trivial as M_i e M_i' are one the inverse of the other by construction.

The second observation employs the fact that, by construction, M_i is a multiple of all the values n_j except for n_i.

It is thus easy to verify that the positive integer number X, $0 \leq X < N$ defined as:

$$X \triangleq \left(\sum_{i=1}^{k} M_i \cdot M_i' \cdot x_i \right) \bmod N \tag{2}$$

is the smallest positive integer bound to the tuple $(x_1, x_2, \ldots, x_k)$, where $\forall i \, X \equiv_{n_i} x_i$. In fact, all the elements of the sum are equal to zero mod n_i except for the i-th one.

□