Maths pour la Sécurité

Julien BERNARD

Le but de ce manuel est de fournir les bases mathématiques nécessaires à la compréhension du cours de Sécurité. Les notions abordées ici sont donc considérées comme acquises et n'ont pas à être justifiée dans les exercices. Les démonstrations des propriétés et des théorèmes ne sont pas données pour plus de concision.

Table des matières

1 Arithmétique dans $\mathbb{Z}$

1.1 Divisibilité

Définition 1 (Divisibilité) *Soient a et b deux entiers, on dit que a* divise *b, et on note $a|b$ si $\exists k \in \mathbb{Z}, b = k \times a$. On dit aussi que a est un* diviseur *de b, ou que b est un* multiple *de a.*

Propriété 1 *On a les propriétés suivantes :*

1. *Pour tout $a \in \mathbb{Z}$, 1 et -1 divisent a et a divise 0*
2. *Pour tout $a \in \mathbb{Z}$, a et $-a$ divisent a*
3. *Si $a|b$ et $b|c$, alors $a|c$ (transivité)*
4. *Si $q|a$ et $q|b$ alors $\forall m, n \in \mathbb{Z}, q|(ma + nb)$ (combinaison linéaire)*

1.2 Nombre premiers

Définition 2 (Nombre premier) *Un entier $n > 0$ est dit* premier *s'il admet exactement deux diviseurs positifs distincts, 1 et lui-même.*

Attention, 1 n'est pas premier ! Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13. En particulier, 2 est le seul nombre premier pair.

Théorème 1 (Théorème d'Euclide) *Il existe une infinité de nombres premiers.*

Propriété 2 *Tout entier naturel n plus grand que 1 admet au moins un diviseur premier.*

Propriété 3 *Si un entier naturel n n'est divisible par aucun nombre premier dont le carré est inférieur ou égal à n, alors n est premier.*

Cette propriété permet de tester si un nombre n est premier en regardant s'il est divisible par un premier inférieur à $\sqrt{n}$. Cette propriété s'appelle un *critère de primalité*, c'est-à-dire un test pour savoir si n est premier ou pas.

Théorème 2 (Théorème fondamental de l'arithmétique) *Tout entier n strictement positif s'écrit de manière unique sous la forme d'un produit de facteurs premiers. Autrement dit, il existe des nombres premiers deux à deux distincts p_1, ..., p_k et des entiers α_1, ..., α_k, uniques à l'ordre près, tels que :*

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$$

Attention, trouver cette décomposition est un problème très difficile !

1.3 Division euclidienne

Théorème 3 (Division euclidienne) *Soit b un entier non nul, tout entier a s'écrit de manière unique sous la forme $a = bq + r$ avec $0 \leq r < |b|$. Les entiers q et r sont appelés respectivement* quotient *et* reste *dans la division euclidienne de a par b.*

Ce théorème est très important parce qu'il établit à la fois l'existence et l'unicité de q et r, donc si on trouve un couple (q, r) qui satisfait les propriétés énoncées, on est certain d'avoir trouvé le quotient et le reste.

Propriété 4 $a|b \iff r = 0$

1.4 Plus grand commun diviseur

Définition 3 (Plus Grand Commun Diviseur) *Soit $D(a,b)$ l'ensemble des diviseurs commun à a et b. $D(a,b)$ est un ensemble fini et non vide donc a un plus grand élément appelé* plus grand commun diviseur*, ou* PGCD*, de a et b, noté $pgcd(a,b)$.*

On peut remarquer que les diviseurs communs à a et b sont les diviseurs de $\mathrm{pgcd}(a,b)$.

Propriété 5 *On a les propriétés suivantes :*
- $pgcd(a,b) = pgcd(b,a)$
- $pgcd(a,1) = 1$
- $b|a \iff pgcd(a,b) = b$
- $pgcd(ka,kb) = k \times pgcd(a,b)$
- *Si $d = pgcd(a,b)$, alors n divise a et b si et seulement si n divise d.*

Lemme 1 (Identité de Bezout) *Soient a et b deux entiers et $d = pgcd(a,b)$, alors il existe deux entiers $(u,v) \in \mathbb{Z}^2$ tels que :*

$$a \times u + b \times v = d$$

Attention, il n'y a pas d'unicité de u et v. En effet, si on considère $a = 150$ et $b = 24$, on a $d = \mathrm{pgcd}(a,b) = 6$ et :
- $6 = 150 \times 1 - 24 \times 6$ ($u = 1$ et $v = -6$)
- $6 = 150 \times 5 - 24 \times 31$ ($u = 5$ et $v = -31$)

Lemme 2 (Lemme d'Euclide) *Soient a et b deux entiers non-nuls et q et r, avec $r \neq 0$, tels que $a = b \times q + r$ alors $pgcd(a,b) = pgcd(b,r)$*

1.5 Nombres premiers entre eux

Définition 4 (Nombre premiers entre eux) *On dit que a et b sont* premiers entre eux *si $pgcd(a,b) = 1$.*

Attention, a et b premiers entre eux ne signifie pas que a ou b sont premiers. Par exemple, 21 et 8 sont premiers entre eux mais aucun des deux n'est premier.

Propriété 6 *Soient a et b deux entiers non nuls, et $d = pgcd(a,b)$, alors il existe a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.*

Théorème 4 (Théorème de Bezout) *a et b sont premiers entre eux si et seulement s'il existe $(u,v) \in \mathbb{Z}^2$ tels que :*

$$a \times u + b \times v = 1$$

Contrairement à l'identité de Bezout qui est une simple implication, le théorème de Bezout est une équivalence. Donc, si on trouve u et v qui satisfont la propriété, alors, on sait que a et b sont premiers entre eux.

Lemme 3 (Lemme de Gauss) *Si $a|bc$ et si a est premier avec b, alors $a|c$.*

Définition 5 (Indicatrice d'Euler) *Soit $n > 0$, on définit l'*indicatrice d'Euler*, notée $\varphi(n)$, par le nombre d'entiers strictement positifs inférieurs ou égaux à n et premiers avec n.*

2 Congruence

2.1 Congruence modulo n

Définition 6 (Congruence modulo n) *Soient a et b deux entiers, pour $n \neq 0$, on dit que a est* congru *à b* modulo *n si et seulement si $n|a-b$. On note :*
- $a \equiv b \mod n$
- $a \equiv b[n]$.

Propriété 7 *Soient a et b deux entiers, a est congru à b modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.*

Cette propriété donne en fait une définition équivalente de la congruence modulo n.

Propriété 8 *On a les propriétés suivantes :*
1. $a \equiv a \mod n$ *(réflexivité)*
2. $a \equiv b \mod n \iff b \equiv a \mod n$ *(symétrie)*
3. *Si* $a \equiv b \mod n$ *et* $b \equiv c \mod n$*, alors* $a \equiv c \mod n$ *(transivité)*

Ces trois premières propriétés démontrent que la relation de congruence modulo n est une relation d'équivalence.

Propriété 9 *La relation de congruence est compatible avec l'addition, la soustraction, la multiplication et l'exponentiation. Autrement dit, si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors :*
- $a + c \equiv b + d \mod n$
- $a - c \equiv b - d \mod n$
- $a \times c \equiv b \times d \mod n$
- $\forall p \in \mathbb{N}, a^p \equiv b^p \mod n$

Théorème 5 (Inverse modulaire) *Soit $n > 0$ et a un entier premier avec n, alors il existe b tel que $a \times b \equiv 1 \mod n$. b est appelé l'*inverse *de a modulo n.*

Ce théorème résulte directement du théorème de Bezout. On pourra également noter que le nombre d'éléments inversibles strictement inférieurs à n est égal à $\varphi(n)$.

Définition 7 (Ordre d'un élément) *Soit $n > 0$ et a un entier premier avec n. On appelle* ordre *de a modulo n le plus petit entier $k > 0$ tel que $a^k \equiv 1 \mod n$.*

On remarque qu'alors, l'inverse de a est a^{k-1}.

Propriété 10 *Soit $n > 0$ et a d'ordre k. S'il existe b tel que $a^b \equiv 1 \mod n$, alors $k|b$.*

Théorème 6 (Théorème d'Euler) *Soit n un entier et a un entier premier avec n alors :*

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

Cela signifie, entre autre, que $\varphi(n)$ divise l'ordre de a.

Théorème 7 (Théorème des restes chinois) *Soient $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux (ce qui veut dire pgcd$(n_i, n_j) = 1$ lorsque $i \neq j$). Alors pour tous entiers $a_1, \ldots, a_k$, il existe un entier x, unique modulo $n = \prod_{i=1}^{k} n_i$ et tel que :*

$$\begin{gathered} x \equiv a_1 \mod n_1 \\ \cdots \\ x \equiv a_k \mod n_k \end{gathered}$$

2.2 Congruence modulo p premier

Ce cas particulier est très important car, si p est premier, cela signifie que tout entier non multiple de p est inversible modulo p.

Théorème 8 (Petit théorème de Fermat) *Soit p premier et a non divisible par p alors on a :*

$$a^{p-1} \equiv 1 \mod p$$

Autrement dit, l'ordre de a divise $p - 1$.

Le petit théorème de Fermat est un cas particulier du théorème d'Euler. En effet, pour p premier, $\varphi(p) = p - 1$.

Corollaire 1 *Soit p premier, alors pour tout entier a, on a :*

$$a^p \equiv a \mod p$$

Attention, la réciproque n'est pas vraie !