Les entiers – Théorie

Définition 1 (Division)**.** *Soient a, $b \in \mathbb{Z}$ avec $a \neq 0$. On dit que a* ***divise*** *b, noté $a|b$ si et seulement si*

$$\exists c \in \mathbb{Z}\ b = ac.$$

On dit également que b est un ***multiple*** *de a.*

Exercice 1. *Montrez que (a) $2|4$, (b) $3 \nmid 7$, (c) $1|13$, et (d) $17|17$.*

Exercice 2. *Soient a, b, $c \in \mathbb{Z}$ avec $a \neq 0$. Prouvez les affirmations ci-dessous.*

1. *Si $a|b$ et $a|c$, alors $a|(b+c)$.*
2. *Si $a|b$, alors quel que soit $d \in \mathbb{Z}$ $a|bd$.*
3. *Si $a|b$ et $b|c$, alors $a|c$.*

Théorème 2 (Algorithme de division d'Euclide)**.** *Soient $a \in \mathbb{Z}$ et $d \in \mathbb{N}_0$. Il existe deux uniques entiers q et r tels que $0 \leq r < d$ et $a = dq + r$.*

Définition 3. *Dans le théorème ci-dessus, a est appelé le* ***dividende****, d est appelé le* ***diviseur****, q (noté $a \div d$ ou a div d) est appelé le* ***quotient*** *et r (noté $a \mod d$) est appelé le* ***reste****.*

Exercice 3. *Dans chacun des cas suivants, trouvez le quotient et le reste. (1) $a = 17$ et $d = 4$; (2) $a = 17$ et $d = 19$; (3) $a = 121$ et $d = 11$; (4) $a = 8121$ et $d = 7$.*

Définition 4 (Congruence)**.** *Soient a, $b \in \mathbb{Z}$ et $n \in \mathbb{N}_0$. On dit que a est* ***congru*** *à b* ***modulo*** *n si et seulement si n divise $(a-b)$. On note alors $a \equiv_n b$.*

Exercice 4. *Vrai ou Faux. (a) $1 \equiv_2 3$, (b) $5 \equiv_3 9$, (c) $7 \equiv_7 12$, (d) $13 \equiv_5 23$.*

Exercice 5. *Soient a, $b \in \mathbb{Z}$ et $n \in \mathbb{N}_0$. Montrez que $a \equiv_n b \;\Leftrightarrow\; a \mod n = b \mod n$.*

Définition 5 (Nombre premier)**.** *Un nombre $p \in \mathbb{N}$ est dit* ***premier*** *si il admet exactement deux diviseurs naturels distincts (qui sont 1 et p).*

Exercice 6. *Donnez tous les nombres premiers inférieurs à* 20.

Théorème 6 (Théorème fondamental de l'arithmétique)**.** *Tout naturel $n \geq 2$ peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.*

Exercice 7. *Donnez un algorithme qui prend en entrée un naturel n et répond **oui**, si n est premier et **non**, sinon. Quelle est la complexité de votre algorithme (en fonction de la **taille** de l'entrée).*

Exercice 8. *Montrez que si n n'est pas premier, alors n est divisible par un nombre premier inférieur ou égal à $\sqrt{n}$. En quoi cette propriété est-elle intéressante ?*

Exercice 9. *Prouvez que* 101 *est un nombre premier.*

Exercice* 10. *Prouvez qu'il y a une infinité de nombres premiers.*

Définition 7 (PGCD)**.** *Soient a, $b \in \mathbb{Z}$ tels que $a \neq 0$ ou $b \neq 0$. Le plus grand naturel d tel que $d|a$ et $d|b$ est appelé**le plus grand commun diviseur de** a **et** b et est noté $pgcd(a, b)$.*

Exercice 11. *Calculez (a) $pgcd(24, 36)$, (b) $pgcd(15, 100)$, (c) $pgcd(1, 317)$.*

Définition 8 (PPCM)**.** *Soient a, $b \in \mathbb{N}_0$. **Le plus petit commun multiple de** a **et** b est le plus petit naturel d tel que $a|d$ et $b|d$. Il est noté $ppcm(a, b)$.*

Exercice 12. *Calculez (a) $ppcm(2, 3)$, (b) $ppcm(15, 12)$, (c) $ppcm(1, 317)$.*

Exercice 13. *Quel que soient a, $b \in \mathbb{N}_0$, montrez que $ab = pgcd(a, b) \cdot ppcm(a, b)$*

Exercice 14. *Quel que soient a, $b \in \mathbb{N}_0$, montrez que $pgcd(a, b) = pgcd(b, a \mod b)$. En déduire un algorithme qui calcule le pgcd de deux naturels.*

Théorème 9 (Représentation des naturels en base b)**.** *Soient $b \in \mathbb{N}$ tel que $b \geq 2$ et $n \in \mathbb{N}$, on peut écrire n de façon unique sous la forme*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 b^0,$$

où $0 \leq a_k, a_{k-1}, \ldots, a_1, a_0 \leq b - 1$. On dit que $(a_k a_{k-1} ... a_1 a_0)_b$ est la représentation de n en base b.

Par exemple la représentation de 11 en base 3 est $(102)_3$ car $11 = \mathbf{1}.3^2 + \mathbf{0}.3^1 + \mathbf{2}.3^0$.

Exercice* 15. *Donnez un algorithme qui construit la représentation d'un nombre en base b.*

Théorème 10 (Petit théorème de Fermat)**.** *Soient p un nombre premier et a un nombre entier non divisible par p, on a*

$$a^p \equiv_p a.$$