Université des Antilles // Master MEEF // Année 2021/2022
Arithmétique

L'anneau des entiers $\mathbb{Z}$

1. Divisibilité dans $\mathbb{Z}$.

1.1. Divisibilité, diviseurs, multiples.

Définition 1.1. *Soient a et b deux entiers. On dit que a* **divise** *b quand il existe un entier q (le* **quotient de a par b***) tel que $\boxed{b = q \cdot a}$. On note $\boxed{a|b}$.*

On dit aussi "a **est un diviseur de** *b" ou b* **est un multiple de** *a.*

Exercice : 1. Montrer les propriétés suivantes

- si $a|b$ et $a|c$, alors pour tous entiers m, n, on a $a|mb+nc$;
  Solution : si $a|b$, alors il existe un entier q tel que $b = qa$.
  Si $a|c$, alors il existe un entier q' tel que $c = q'a$.
  On a donc $mb + nc = mqa + nq'a = (mq + nq')a$.
  Puisque m, n, q, q' sont entiers, $mq + nq'$ est un entier. Donc a divise $mb + nc$
- si $a|b$ et $c|d$, alors $ac|bd$;
  Solution : si $a|b$, alors il existe un entier q tel que $b = qa$.
  Si $c|d$, alors il existe un entier q' tel que $d = q'c$.
  Donc $bd = qaq'c = (qq')ac$. Puisque qq' est un entier, ac divise bd.
- si $a|b$ et m est un entier, alors $ma|mb$;
  Solution : si $a|b$, alors il existe un entier q tel que $b = qa$. On a donc $mb = mqa = q(ma)$ et ma divise mb.
- si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$.
  Solution : si $a|b$, alors il existe un entier q tel que $b = qa$.
  Si $b|a$, alors il existe un entier q' tel que $a = q'b$.
  Donc $a = q'b = q'(qa)$ et $qq' = 1$.
  Mais l'égalité $qq' = 1$ dans $\mathbb{Z}$ admet pour solutions $q = q' = 1$ et $q = q' = -1$.
  Donc $a = b$ ou $a = -b$.
- (transitivité) si $a|b$ et $b|c$ alors $a|c$.

2. Montrer que si m divise n, alors pour $a > 1$ entier, $a^m - 1$ divise $a^n - 1$.
Solution : Si $m|n$, alors il existe un entier q tel que $n = qm$.
On souhaite montrer que $a^m - 1$ divise $a^{qm} - 1$.
On considère la suite géométrique de premier terme 1 et de raison a^m.
La somme de ses q premiers termes est $\sum_{k=0}^{q-1} a^{mk}$ qui est un entier.
On calcule

$$(a^m-1)\sum_{k=0}^{q-1} a^{mk} = \sum_{k=0}^{q-1}(a^{m(k+1)}-a^{mk}) = \sum_{k=0}^{q-1} a^{m(k+1)} - \sum_{k=0}^{q-1} a^{mk} = \sum_{k=1}^{q} a^{mk} - \sum_{k=0}^{q-1} a^{mk}$$

$$= a^{mq} + \sum_{k=1}^{q-1} a^{mk} - \sum_{k=1}^{q-1} a^{mk} - 1 = a^{mq-1} = a^n - 1$$

Remarque : $2^{15} - 1$ n'est pas un nombre premier car $15 = 3 \times 5$ Donc $2^{15} - 1$ est divisible par $2^3 - 1$ et par $2^5 - 1$.

1.2. **Division Euclidienne.**

Définition 1.2. *Soient a et $b > 0$ deux entiers ; alors il existe un* **unique couple d'entiers** (q, r) *tel que* $\boxed{\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}}$

On appelle q **le quotient et** *r* **le reste** *de la* **division Euclidienne de** *a* **par** *b.*

Exercice : 1. Prouver cette "définition".

Preuve : on considère l'ensemble des entiers de la forme $a - bk$ avec k entier.

On considère le plus petit entier positif ou nul de cet ensemble

$$r = \min\{a - bk,\ k \in \mathbb{Z}\}$$

On sait que $r \geq 0$ par hypothèse.

Pour montrer que $r < b$, on raisonne par l'absurde : si $r \geq b$, alors $r - b \geq 0$. Mais il existe un entier q tel que $r = a - qb$. Donc $r - b = a - (q + 1)b$ est un élément de l'ensemble, et il est strictement inférieur à r, et positif ou nul.

Ceci contredit la définition de r.

Donc $r < b$, et on a le résultat.

2. Soit r le reste de la division Euclidienne de a par b, r' le reste de le division Euclidienne de a' par b.

a. Montrer que $r = r'$ si, et seulement si b divise $a - a'$;

Solution : on a

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}, \begin{cases} a' = bq' + r' \\ 0 \leq r' < b \end{cases}$$

On écrit $a - a' = bq + r - (bq' + r') = b(q - q') + (r - r')$.

$$\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases} \Leftrightarrow \begin{cases} 0 \leq r < b \\ -b < -r' \leq 0 \end{cases} \Rightarrow -b < r - r' < b$$

Donc $a - a'$ est un multiple de b si, et seulement si $r - r'$ est un multiple de b, si et seulement si $r - r' = 0$.

b. montrer que les restes des divisions Euclidiennes de aa' et rr' par b sont égaux.

Solution. On écrit

$$aa' = (bq + r)(bq' + r') = bqbq' + bqr' + rbq' + rr' = b(qbq' + qr' + rq') + rr'$$

(Rappel) Si deux nombres diffèrent d'un multiple de b, alors ils ont le même reste dans la division euclidienne par b.

$$m = kb + n$$

On écrit les divisions euclidiennes

$$\begin{cases} m = bq + r \\ 0 \leq r < b \end{cases}, \begin{cases} n = bq' + r' \\ 0 \leq r' < b \end{cases}$$

Donc on a $bq + r = kb + bq' + r'$ et $b(q - q' - k) = r' - r$. Donc $r = r'$ par le même argument que précédemment.

Ici aa' et rr' diffèrent d'un multiple de b. Donc ils ont le même reste dans la division euclidienne par b.

3. Donner le reste de la division euclidienne de 2^{89975} par 13 ; celui de 25^{45678} par 11.

On calcule les restes des puissances de 2 par la division euclidienne par 13

$$2^0 -> 1,\ 2^1 -> 2, 2^2 -> 4, 2^3 -> 8, 2^4 = 16 -> 3, 2^5 -> 6, 2^6 -> 12$$

$$2^7 -> 11,\ 2^8 -> 9, 2^9 -> 5, 2^{10} -> 10, 2^{11} -> 7, 2^{12} -> 1$$

On effectue la division euclidienne de 89975 par 12: $89975 = 7497 \times 12 + 11$.

$$2^{89975} = 2^{7497\times 12+11} = (2^{12})^{7497} \times 2^{11}$$

Donc le reste est le même que celui de 2^{11}: c'est 7.

4. Soient m et n deux entiers naturels, et $m = qn + r$ la division euclidienne de m par n. Soit n un entier; montrer que le reste de la division euclidienne de $a^m - 1$ par $a^n - 1$ est $a^r - 1$.

On calcule la différence $a^m - 1 - (a^r - 1) = a^m - a^r = a^r(a^{m-r} - 1) = a^r(a^{qn} - 1)$.

Mais qn est un multiple de n. Donc $a^{qn} - 1$ est un multiple de $a^n - 1$.

On en déduit que les deux entiers $a^m - 1$ et $a^r - 1$ diffèrent d'un multiple de $a^n - 1$. Donc ils ont le même reste dans la division euclidienne par $a^n - 1$.

On sait que $0 \leq r < n$. Donc $1 \leq a^r < a^n$ et $0 \leq a^r - 1 < a^n - 1$.

Donc la division euclidienne de $a^r - 1$ par $a^n - 1$ est $a^r - 1 = 0 \times (a^n - 1) + a^r - 1$. Le reste est $a^r - 1$.

5. On note $n\mathbb{Z}$ l'ensemble des multiples de n. Montrer que c'est un sous-groupe additif de $\mathbb{Z}$.

6. Soit G un sous-groupe de $(\mathbb{Z}, +)$.

a/ Montrer que si G contient un élément non nul, alors G contient un entier strictement positif.

b/ On note n le plus petit entier naturel non nul de G. Montrer que G contient le sous-groupe $n\mathbb{Z}$.

c/ Soit a un élément de G; montrer que le reste de la division euclidienne de a par n est un élément de G.

d/ En déduire que $G = n\mathbb{Z}$, puis tous les sous-groupes additifs de $\mathbb{Z}$.

1.3. **Congruences.**

Définition 1.3. *Soit n un entier ; si a et b sont deux entiers, on dit que a* **est congru à** *b* **modulo** *n, et on note* $\boxed{a \equiv b \mod n}$ *quand* $\boxed{n \textbf{ divise } b - a}$.

Exercice : 1. Montrer que la relation $\equiv \mod n$ est une relation d'équivalence sur $\mathbb{Z}$, et que les classes d'équivalence sont les $a + n\mathbb{Z} = \{a + kn,\ k \in \mathbb{Z}\}$, pour $0 \leq a \leq n - 1$.

Solution : On montre que $\equiv \mod n$ est

- réflexive : pour tout entier a, on a $a \equiv a \mod n$ car $a - a = 0$ est multiple de n.
- symétrique : si a et b sont deux entiers tels que $a \equiv b \mod n$, alors n divise $b - a$. Donc n divise $a - b$ donc $b \equiv a \mod n$.
- transitive : si a, b et c sont trois entiers tels que $a \equiv b \mod n$ et $b \equiv c \mod n$, alors n divise $b-a$ et n divise $c-b$. Donc n divise $c-b+b-a = c-a$. Donc $a \equiv c \mod n$.

Donc $\equiv \mod n$ est une relation d'équivalence.

Si a est un entier, la classe d'équivalence de a pour la relation $\equiv \mod n$ est

$$\{b \in \mathbb{Z},\ a \equiv b \mod n\} = \{b \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ b - a = kn\} = \{a + kn,\ k \in \mathbb{Z}\}$$

On a vu que tous les entiers d'une classe d'équivalence ont le même reste dans la division euclidienne par n. Donc la classe d'équivalence de a est la même que la classe d'équivalence de r, où r est le reste de la division euclidienne de a par n.

En particulier il y a exactement n classes d'équivalence pour la relation $\equiv \mod n$, qui sont les classes d'équivalence de 0, 1, ..., $n-1$.

2. Montrer que

- si $a \equiv b \mod n$ et m est un entier, alors $ma \equiv mb \mod mn$;
- si a, b, c, d sont quatre entiers tels que $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $a + b \equiv c + d \mod n$ et $ac \equiv bd \mod n$ (on dit que la congruence est *compatible aux opérations* de $\mathbb{Z}$);
- si $a = ma'$, $b = mb'$ et $n = mn'$, et si $a \equiv b \mod n$, alors $a' \equiv b' \mod n'$.

2. Diviseurs et multiples communs

2.1. Plus grand commun diviseur.

Définition 2.1. *Soient a et b deux entiers; leur* **plus grand commun diviseur**, *noté* $\boxed{\text{pgcd}(a,b)}$, *est l'unique entier positif divisant a et b, et tel que ($d|a$ et $d|b \Rightarrow d|\text{pgcd}(a,b)$).*

Exercice : montrer les propriétés suivantes

- si $n \geq 1$ est un entier, alors $\text{pgcd}(na, nb) = n\text{pgcd}(a, b)$;
  Solution : on a
  - $n\text{pgcd}(a, b)$ divise na et nb. C'est facile : on sait que $\text{pgcd}(a, b)$ divise a et b, il suffit de multiplier par n. Donc $n\text{pgcd}(a, b)$ divise $\text{pgcd}(na, nb)$.
  - d'autre part l'entier $\text{pgcd}(na, nb)$ est un multiple de n, on l'écrit nk. Alors nk divise na et nb; donc k divise a et b, et k divise $\text{pgcd}(a, b)$. Donc $\text{pgcd}(na, nb)$ divise $n\text{pgcd}(a, b)$.

  On en déduit que $n\text{pgcd}(a, b)$ et $\text{pgcd}(na, nb)$ sont deux entiers naturels qui se divisent l'un l'autre: ils sont égaux.
- si $a = bq + r$ est la DE de a par b, alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$;
  Solution : Soit d un diviseur commun à a et b. Alors d divise r car $r = a - bq$. Donc d est un diviseur commun à b et r.

  Soit d un diviseur commun à r et b. Alors d divise a car $a = bq + r$. Donc d est un diviseur commun à a et b.

  Donc les diviseurs communs à a et b sont les mêmes que les diviseurs communs à b et r. En particulier, ces deux couples d'entiers ont le même pgcd.

On a le résultat fondamental suivant, qui donne un algorithme de calcul du pgcd

Théorème 2.1 (Algorithme d'Euclide)**.** *Soient a et b des entiers, $a > b > 0$. L'algorithme*

- `la division euclidienne de` a `par` b `a pour quotient` q_1 `et pour reste` r_1 `;`

- `la division euclidienne de` b `par` r_1 `a pour quotient` q_2 `et pour reste` r_2 ;
- `la division euclidienne de` r_1 `par` r_2 `a pour quotient` q_3 `et pour reste` r_3`...`

s'arrête: après un nombre fini de pas, on a $r_k = 0$. *Le* **pgcd** *de* a *et* b *est le* **dernier reste non nul**.

Démonstration :
On sait que r_1 est le reste de la DE de a par b. Donc $0 \leq r_1 < b$.
On sait que r_2 est le reste de la DE de b par r_1. Donc $0 \leq r_2 < r_1$.
Donc les entiers $r_1, r_2, \ldots$ forment une suite strictement décroissante **d'entiers naturels**. Il existe donc un entier naturel k tel que $r_n = 0$ pour tout $n \geq k$.
On a vu que

$$\text{pgcd}(a,b) = \text{pgcd}(b,r_1) = \text{pgcd}(r_1,r_2) = \ldots = \text{pgcd}(r_{k-1},r_k) = r_{k-1}$$

car $r_k = 0$. Donc le dernier reste non nul est égal au pgcd de a et b.

Exercice : 1. Calculer de cette façon les pgcd suivants:

$$\text{pgcd}(6n+4, 2n+1),\ \text{pgcd}(4n+5, 16n^2-23),\ \text{pgcd}(6n+4, 18n^2+18n+8)$$

2. Soient m et n deux entiers naturels. Montrer que $\text{pgcd}(a^m-1, a^n-1) = a^{\text{pgcd}(m,n)} - 1$.
3. Montrer qu'on a toujours $r_{n+2} < \frac{r_n}{2}$ tant que ces restes sont non nuls (on raisonnera par disjonction des cas, suivant que $r_{n+1} \leq \frac{r_n}{2}$ ou non).
En déduire qu'on a $r_{2k+1} < \frac{r_1}{2^k}$ pour tout $k \geq 1$, puis donner une majoration du nombre de boucles à effectuer dans l'algorithme d'Euclide en fonction de b.
4. Ecrire l'algorithme d'Euclide dans votre langage de programmation préféré.

Des résultats précédents, on déduit

Théorème 2.2 (Bezout)**.** *Il existe deux entiers* u *et* v *tels que* $au + bv = \text{pgcd}(a,b)$.

C'est facile à voir : en écrivant $r_1 = a - q_1 b$, $r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 + q_1 q_2)$ et les égalités suivantes, on montre par récurrence que pour tout $1 \leq i \leq n$, r_i s'écrit sous la forme $r_i = u_i a + v_i b$. Si r_n est le dernier reste non nul, alors on a $r_n = \text{pgcd}(a,b)$, donc on peut choisir $u = u_n$ et $v = v_n$.
L'algorithme d'Euclide autorise le calcul des "coefficients de Bezout": en effet les suites u_i et v_i satisfont les relations

$$u_{i+2} = u_i - q_{i+2} u_{i+1},\ v_{i+2} = v_i - q_{i+2} v_{i+1}$$

Exercice : 1. Montrer que l'ensemble des entiers de la forme $am + bn$ avec m et n entiers est égal à l'ensemble des multiples de $\text{pgcd}(a,b)$.
2. En déduire que l'équation diophantienne $ax + by = c$ admet des solutions entières si, et seulement si c est un multiple de $\text{pgcd}(a,b)$.
3. Ecrire l'algorithme d'Euclide étendu (qui donne les entiers u et v) à l'aide d'un tableur, puis en Python.

2.2. **Plus petit commun multiple.**

Définition 2.2. *Soient a et b deux entiers non nuls; leur* **plus petit commun multiple**, *noté* $\boxed{\text{ppcm}(a,b)}$, *est l'(unique) entier positif qui est à la fois multiple de a et b, et tel que ($a|m$ et $b|m \Rightarrow \text{ppcm}(a,b)|m$).*

2.3. **Entiers premiers entre eux.**

Définition 2.3. *Deux entiers a et b sont* **premiers entre eux** *quand* $\boxed{\text{pgcd}(a,b) = 1}$.

Dans ce cas, le **théorème de Bezout** s'écrit

Théorème 2.3. *Deux entiers a et b sont premiers entre eux si, et seulement si il existe des entiers u et v tels que $au + bv = 1$.*

Exercice : 1. Montrer que si deux entiers a et b sont premiers entre eux, il en est de même de a^n et b^m, pour m et n deux entiers naturels.

2. Montrer que si a et b sont tous les deux premiers à n, alors ab est encore premier à n.

3. Montrer que si a et n sont deux entiers premiers entre eux, alors il existe un entier u tel que $au \equiv 1 \mod n$. En déduire l'ensemble des solutions de la congruence $ax \equiv b \mod n$ dans $\mathbb{Z}$.

4. Résoudre la congruence $2x \equiv 0 \mod 6$ dans $\mathbb{Z}$.

Un autre résultat fondamental est le **lemme de Gauss**

$\boxed{\text{Si } a \text{ et } b \text{ sont deux entiers premiers entre eux, et si } a|bc, \text{ alors } a|c.}$

Exercices : 1. Montrer le lemme de Gauss.

2. Si a et b sont deux entiers premiers entre eux, déterminer tous les couples (m,n) d'entiers tels que $am + bn = 0$. Exprimer toutes les solutions de l'équation diophantienne $ax + by = 1$ à l'aide d'une solution particulière (u,v).

3. On suppose maintenant que a et b sont deux entiers non nuls. Donner l'ensemble des solutions de l'équation diophantienne $ax + by = 0$.

Théorème 2.4 (des restes chinois)**.** *Soient m et n des entiers* premiers entre eux*, et $0 \leq a \leq m-1$, $0 \leq b \leq n-1$ des entiers. Il existe un unique entier $0 \leq l \leq mn-1$ satisfaisant les congruences*

$$\begin{cases} l \equiv a \mod m \\ l \equiv b \mod n \end{cases}$$

Exercices 1. Montrer ce résultat (pour l'existence, on utilisera une écriture de Bezout de la forme $um + vn = 1$, puis on s'intéressera à l'entier $x = bum + avn$).

2. Un équipage est composé de 27 pirates, et d'un cuisinier. Suite à une fortune de mer, ils s'emparent d'un trésor constitué de lingots d'or.

Les pirates décident de prendre chacun le même nombre de lingots, et de donner le reste au cuisinier; le cuisinier en obtient alors 7.

Suite à une nouvelle fortune de mer, il ne reste plus que 13 pirates, et le cuisinier. Avec le même mode de partage, le cuisinier aura 11 lingots.

Sachant qu'il y a moins de 400 lingots, combien le cuisinier aura-t-il de lingots quand il aura empoisonné le reste de l'équipage ?

3. Nombres premiers

3.1. **Définition et factorisation des entiers.**

Définition 3.1. *Un entier p est* **premier** *quand ses seuls diviseurs sont* 1 *et lui même.*

Exercices : 1. Montrer qu'un entier non divisible par p premier est nécessairement premier à p.

2. Montrer le lemme d'Euclide : *si p est un entier premier qui divise ab, alors p divise a ou p divise b*

Une des principales applications des nombres premiers est la **factorisation des entiers**:

Théorème 3.1. *Soit n un entier; alors n s'écrit de* manière unique *sous la forme*

$$n = p_1^{m_1} \dots p_k^{m_k}$$

où $p_1 < \dots < p_k$ sont des nombres premiers, et $m_1, \dots, m_k$ sont des entiers strictement positifs.

Exercices : 1. Soit n un entier non premier; montrer qu'il existe un diviseur premier p de n tel que $p \leq \sqrt{n}$.

2. Montrer que les diviseurs de $n = p_1^{m_1} \dots p_k^{m_k}$ sont les $d = p_1^{a_1} \dots p_k^{a_k}$, avec $0 \leq a_i \leq m_i$, puis exprimer le nombre de diviseurs de n en fonction des m_k.

3. Montrer que l'entier n a un nombre impair de diviseurs si, et seulement si c'est un carré.

4. Montrer que deux entiers n et n' sont premiers entre eux si, et seulement si l'ensemble des facteurs premiers de n et l'ensemble des facteurs premiers de n' sont disjoints.

On appelle l'exposant m_i la **valuation p_i-adique de n**, et on la note $v_{p_i}(n)$. Pour tous les premiers p n'apparaissant pas dans la décomposition ci-dessus, on pose $v_p(n) = 0$.

Application : Une fois qu'on connaît les factorisations de a et b, il est facile de déterminer $\mathrm{pgcd}(a, b)$ et $\mathrm{ppcm}(a, b)$:

- pour tout premier p on a $\boxed{v_p(\mathrm{pgcd}(a,b)) = \min(v_p(a), v_p(b))}$;
- pour tout premier p on a $\boxed{v_p(\mathrm{ppcm}(a,b)) = \max(v_p(a), v_p(b))}$.

Exercice : 1. Montrer que pour tous entiers a et b, on a $\mathrm{ppcm}(a, b)\mathrm{pgcd}(a, b) = ab$;

On donne maintenant le petit théorème de Fermat

Théorème 3.2 (Fermat)**.** $\boxed{\textit{Soient } n \textit{ et } p \textit{ deux entiers, avec } p \textit{ premier. Alors } p \textit{ divise } n^p - n.}$

Exercice : 1. Montrer que pour $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k}$ est un multiple de p.

2. En déduire une démonstration par récurrence du petit théorème de Fermat.

3.2. **Déterminer les premiers nombres premiers.** On fixe un entier n, et on recherche la liste des nombres premiers inférieurs ou égaux à n.

On dispose pour cela du **crible d'Eratosthène**:

- on écrit la liste de entiers de 2 à n;
- on garde l'entier 2, puis on ôte de la liste tous ses multiples stricts $(4, 6, 8, \ldots)$
- on passe à l'entier suivant de la liste (ici c'est 3), et on barre tous ses multiples stricts (donc 9, 15,... puisqu'on a déjà barré 6, 12,...)
- on recommence l'étape précédente, jusqu'à arriver à un entier $> \sqrt{n}$, alors on s'arrête.

À la fin de cet algorithme, la liste contient tous les nombres premiers inférieurs ou égaux à n.

Exercice : montrer l'affirmation précédente (no pourra montrer qu'un nombre qui n'a pas été oté de la liste est premier, puis que tous les nombres non premiers ont été otés de la liste).

3.3. **L'ensemble des nombres premiers.** Un premier résultat:

Il existe une infinité de nombres premiers

Mais **on ne sait pas construire explicitement une infinité de nombres premiers**: on ne connaît aucune suite d'entiers explicites dont tous les termes soient premiers. On connaît seulement quelques suites (très peu denses) dont les éléments ont de bonnes raisons d'être premiers : par exemple

- la suite des **nombres de Mersenne** 2^p-1, p premier est la plus efficace; par exemple le plus grand premier connu est $2^{82589933} - 1$ (environ 24 millions de chiffres en base 10) ;
- $2^{2^n} + 1$, le suite des **nombres de Fermat** (Fermat a conjecturé qu'ils sont tous premiers, mais c'est faux pour $5 \leq n \leq 32$, et on ne le sait pas pour n plus grand).

Exercice : Soient m et n deux entiers.

1. Montrer que si $m^n - 1$ est premier, alors $m = 2$ et n est premier.
2. Montrer que si $m^n + 1$ est premier, alors n n'a aucun facteur premier impair.

La densité asymptotique de l'ensemble de l'ensemble des nombres premiers est connue d'après le **théorème d'Hadamard et de la Vallée Poussin** : si pour tout réel $x > 0$ on note $\pi(x)$ le nombre de premiers $p \leq x$, alors

On a l'équivalence de fonctions $\pi(x) \sim_{x\to\infty} \frac{x}{\ln x}$.

On connaît aussi de nombreux résultats sur la répartition des nombres premiers; en voici quelques-uns.

- (Dirichlet) si a et b sont premiers entre eux, il existe une infinité de premiers congrus à b modulo a (c'est à dire dans la *progression arithmétique* $\{an + b,\ n \in \mathbb{Z}\}$). Plus précisément, si on fixe a, les premiers sont (asymptotiquement) équirépartis dans les progressions ci-dessus quand b parcourt les entiers de $[0, a - 1]$ premiers à a ;

- récemment Green et Tao ont montré qu'il existe des progressions arithmétiques arbitrairement longues constituées uniquement de nombres premiers ;
- les premiers jumeaux sont des couples de nombres premiers $p, p+2$; on ne sait pas s'il en existe une infinité;
- en revanche, on sait depuis 2014 et un résultat de Zhang que si (p_n) désigne la suite croissante de tous les nombres premiers, alors on a

$$\liminf_{n\to\infty} p_{n+1} - p_n < \infty$$

- Les premiers de Sophie Germain sont les premiers p tels que $2p+1$ est encore un nombre premier; on ne sait pas s'il en existe une infinité.

4. Ecriture en base n

Nous sommes habitués à l'écriture décimale des nombres, c'est à dire en base 10. Mais on peut les écrire de bien d'autres manières, selon le même principe (dit de *numération de position*) qu'on va détailler ci-dessous.

Il y a de nombreux exemples d'utilisations d'autres bases de numération dans l'histoire de l'humanité, ou dans la vie de tous les jours

- on donne l'heure en base 60, c'est une écriture *sexagésimale*. Elle a aussi été utilisée par certaines civilisations (en Mésopotamie par exemple)
- les ordinateurs calculent en base 2, c'est l'écriture *binaire* des nombres.
- une clé WIFI est souvent composée des symboles $0, \dots, 9, A, B, C, D, E, F$, c'est un nombre écrit en base 16.
- certaines civilisations ont compté en base 5, 20.

Définition 4.1. *Soit $n > 0$ un entier. Tout entier m s'écrit de façon unique sous la forme*

$$m = m_0 + nm_1 + m_2 n^2 + \cdots + m_k n^k,\ 0 \leq m_0, \dots, m_k \leq n-1,$$

c'est **l'écriture en base n de m.** *On dit que $m_0, \dots, m_k$ sont les chiffres en base n de m, et on écrit $(m)_n = \underline{m_k \cdots m_0}$.*

La division euclidienne donne encore un algorithme, pour trouver l'écriture en base n d'un entier:

Théorème 4.1. *Soit m un entier. On note q_0 et r_0 le quotient et le reste de la DE de m par n, puis q_1 et r_1 le quotient et le reste de la DE de q_0 par n, etc... L'algorithme s'arrête et on a $m = r_k n^k + \cdots + n_2 r^2 + nr_1 + r_0$: c'est l'écriture en base n de m.*

Exemple 4.1. *On a $(63)_2 = \underline{111111}_2$; $(678)_7 = \underline{1656}_7$; $(242)_3 = \underline{22222}_3$.*

Exercice : 1. Soit n un entier naturel: on l'écrit en base 10 sous le forme

$$n = 10^k a_k + \cdots + 100a_2 + 10a_1 + a_0,\ 0 \leq a_i \leq 9$$

c'est à dire que ses chiffres en base 10 sont les a_i (a_0 est son chiffre des unités, a_1 celui des dizaines, etc...

- quel est le reste de la division euclidienne de n par 10 ? En déduire un critère de divisibilité de n par 10 ?

- montrer que le reste de la division euclidienne de n par 2 est le même que celui de la division euclidienne de a_0 par 2. En déduire un critère de divisibilité de n par 2. Que se passe-t-il si on remplace 2 par 5 ?
- montrer que le reste de la division euclidienne de n par 3 est le même que celui de la division euclidienne de la somme de ses chiffres $a_0 + \ldots + a_k$ par 3. En déduire un critère de divisibilité de n par 3. Que se passe-t-il si on remplace 3 par 9 ?
- montrer que le reste de la division euclidienne de n par 4 est le même que celui de la division euclidienne de $10a_1 + a_0$ par 4. En déduire un critère de divisibilité de n par 4.

2. Montrer les propriétés suivantes

- on a $(n^d - 1)_n = \overbrace{\underline{n-1n-1\ldots n-1}_n}^{d \text{ fois}}$;
- le nombre de chiffres de l'écriture en base n de m est $[\log_n(m)] + 1 = \mathrm{E}[\frac{\ln m}{\ln n}] + 1$;
- un entier est divisible par n si, et seulement si son écriture en base n se termine par un zéro 0 ;
- un entier est divisible par $n-1$ si, et seulement si la **somme de ses chiffres en base** n l'est ;
- un entier est divisible par $n+1$ si, et seulement si la **somme alternée de ses chiffres en base** n l'est.

3. En déduire un critère de divisibilité d'un entier par 11 à l'aide des chiffres de son écriture décimale.

Application : calcul rapide de puissances. On va montrer le résultat suivant

On peut calculer a^n en effectuant au plus $2[\log_2(n)] + 2$ multiplications.

Soit $n = \underline{n_k \ldots n_0}_2$, $n_0, \ldots, n_k \in \{0, 1\}$ l'écriture en base 2 de n. En d'autres termes, on a $n = n_0 + 2n_1 + \cdots + 2^k n_k$, et $k = [\log_2(n)]$; donc

$$a^n = a^{n_0}(a^2)^{n_1} \ldots (a^{2^k})^{n_k}.$$

On propose l'algorithme suivant, avec en entrée a et les chiffres de l'écriture de n en base 2

`On pose` $A = 1$, $B = a$, $i = 0$
`Tant que` $i \leq k - 1$, `faire:`
`i/ si` $n_i = 0$ `aller en iii/ ;`
`ii/ si` $n_i = 1$, `on remplace` A `par` AB `;`
`iii/ on remplace` B `par` B^2, `on remplace` i `par` $i + 1$.

Montrer qu'on a $A = a^n$ quand l'algorithme se termine.
Justifier le résultat sur le nombre d'opérations.
Donner un algorithme qui, étant donnés a et n, donne a^n rapidement.