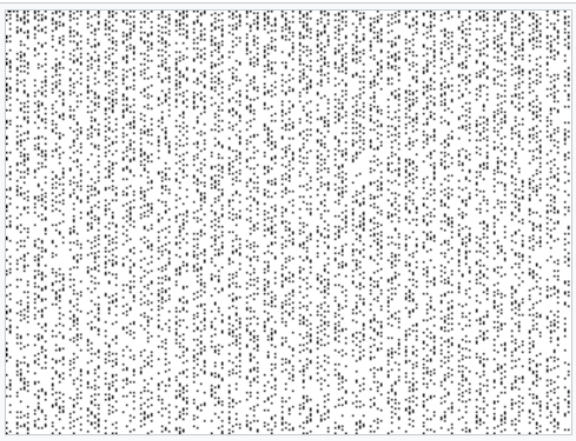
Arithmétique

MPSI Prytanée National Militaire

Pascal Delahaye

12 décembre 2017



La distribution des nombres premiers de 1 à 76 800, de gauche à droite et de haut en bas. Un pixel noir signifie que le nombre est premier alors qu'un blanc signifie qu'il ne l'est pas.

1 La division euclidienne.

THÉORÈME FONDAMENTAL 1 : **Division euclidienne**
Soient deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Alors : $\exists!\ (q,\ r) \in \mathbb{Z} \times \mathbb{N}$ tels que : $\boxed{a = qb + r \quad \text{ET} \quad 0 \leq r < b}$

L'entier q est appelé le *quotient* et r est appelé le *reste* de la division euclidienne de a par b.

Preuve 1 : On démontre que $a = bq + r$ avec $\begin{cases} q \in \mathbb{Z} \\ r \in [\![0, b-1]\!] \end{cases} \iff \begin{cases} q = \lfloor \frac{a}{b} \rfloor \\ r = a - bq \end{cases}$.

Dessin

Division euclidienne

Remarque 1.

1. Effectuer la division euclidienne de a par b signifie déterminer les entiers q et r tels que $\left\{\begin{array}{l} a=bq+r \\ 0\leq r<b \end{array}\right.$.
2. En Python : `a//b` donne le quotient et `a%b` donne le reste de la DE de a par b.

Décomposition d'un entier dans une base $b\in\mathbb{N}$ avec $b\geq 2$
Tout entier $n\in\mathbb{N}$ se décompose de façon unique sous la forme :

$$n=a_0b^0+a_1b^1+a_2b^2+\cdots+a_pb^p \quad \text{avec} \quad p\in\mathbb{N} \text{ et } \forall k\in[\![0,p]\!],\ a_k\in[\![0,b-1]\!]$$

Les valeurs $a_0,\ a_1,\ \ldots,\ a_p$ sont obtenues par des divisions euclidiennes successives par b.
Le nombre n est alors écrit :

$$n=\overline{a_pa_{p-1}\ldots a_1a_0} \quad \text{en base } b$$

`Exemple` 1. La division euclidienne permet de démontrer que les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m\in\mathbb{N}$

DÉFINITION 1 : **La relation "divise"**
Soit $(a,\ b)\in\mathbb{Z}\times\mathbb{Z}^*$.
Lorsque $\exists k\in\mathbb{Z}$ tel que $a=b.k$, on dira que : b *divise* a (noté $b\ /\ a$ ou $b\mid a$).

Remarque 2.

1. Dire que $b\mid a$ lorsque $b>0$ revient à dire que le reste de la division euclidienne de a par b est nul.
2. On note $b\mathbb{Z}$ l'ensemble des nombres divisibles par b. Ces nombres sont appelés les *multiples* de b.

$$\boxed{b \text{ divise } a \iff a \text{ multiple de } b}$$

3. La relation "divise" définit une relation d'ordre partielle sur $\mathbb{N}^*$.
4. Lorsque $a\neq 0$, on a enfin la propriété : $b\mid a\Rightarrow|b|\leq|a|$.

Méthode pour montrer que b divise a :
On pourra :

1. Rechercher une relation de la forme $a=bc$.
2. Effectuer la Division Euclidienne de a par b et prouver que le reste est nul.
3. Effectuer un calcul avec les congruences (voir ci-dessous).
4. Appliquer le théorème de Gauss (voir plus loin).

PROPOSITION 2 : **Propriétés de la divisibilité**
Soient a, b, c, d, λ et μ dans $\mathbb{Z}$.

1. Si $\left\{\begin{array}{l} a/b \\ c/d \end{array}\right.$ alors ac/bd
2. Si $\left\{\begin{array}{l} a/b \\ b/a \end{array}\right.$ alors $a=\pm b$ (antisymétrie)
3. $\boxed{\text{Si } \left\{\begin{array}{l} a/b \\ a/c \end{array}\right. \text{ alors } a/(\lambda b+\mu c)}$
4. Si $\left\{\begin{array}{l} a/b \\ b/c \end{array}\right.$ alors a/c (transitivité)

Preuve 2 : Aucune difficulté !

Remarque 3.

1. La proposition 2. (antisymétrie) est parfois utilisée pour démontrer des égalités.
2. La proposition 3. est souvent utilisée dans la recherche de diviseurs.

Remarque 4. Comme le montre les exemples suivants, les relations de divisibilité permettent en particulier de résoudre des équations d'entiers.

`Exemple` 2. $(*)$ Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $x-1 \mid x+3$
2. $xy = 2x+3y$

2 Les congruences

DÉFINITION 2 : **La notation "congruence"**
Soient trois entiers a, b et n.
Lorsqu'il existe $k \in \mathbb{Z}$ tels que $a = b+kn$, on écrit : $\boxed{a \equiv b\ [n]}$ ou parfois plus simplement : $a = b\ [n]$
On dit que "a est congru à b modulo n"

Remarque 5. Ainsi, si r est le reste de la division euclidienne de a par b, on a : $a \equiv r\ [b]$

PROPOSITION 3 : **Opérations sur les congruences**
Les nombres intervenant dans les propriétés suivantes sont tous des entiers.
Les différentes propriétés suivantes, permettent d'effectuer des "calculs de congruence" :

$\underline{P_1}$ Si $\begin{cases} a_1 \equiv b_1\ [n] \\ a_2 \equiv b_2\ [n] \end{cases}$ alors : $a_1a_2 \equiv b_1b_2\ [n]$ et $\lambda a_1 + \mu a_2 \equiv \lambda b_1 + \mu b_2\ [n]$ $\forall \lambda,\ \mu \in \mathbb{N}$.

$\underline{P_2}$ Si $a \equiv b\ [n]$ alors :
- pour tout $p \in \mathbb{N}$ on a : $a^p \equiv b^p\ [n]$
- pour tout $k \in \mathbb{Z}$, on a : $\begin{cases} k.a \equiv k.b\ [n] \\ k.a \equiv k.b\ [kn] \end{cases}$ et $k+a \equiv k+b\ [n]$
- $b \equiv a\ [n]$ (symétrie)
- $a-b \equiv 0\ [n]$

$\underline{P_3}$ Si $\begin{cases} a \equiv b\ [n] \\ b \equiv c\ [n] \end{cases}$ alors : $a \equiv c\ [n]$ (transitivité)

Preuve 3 : Pas de difficulté ...

Remarque 6. La relation $''\equiv''$ est une relation d'équivalence (réflexive, symétrique et transitive)

Méthodes
1. Pour montrer que b divise a on pourra donc calculer a modulo b et montrer que : $a \equiv 0[b]$.
2. Pour déterminer le reste de la division euclidienne de a par b, on pourra calculer a modulo b jusqu'à obtenir un entier compris entre 0 et $b-1$

`Exemple` 3. $(*)$ Soit $n \in \mathbb{N}$.
1. Montrer que : $3^{2n} - 2^n$ est un multiple de 7.
2. Montrer que : $11 \mid 2^{123} + 3^{121}$.
3. Montrer que : $6 \mid 5n^3 + n$
4. Déterminer le reste de la division euclidienne de 2^n par 3.

Exercice : 1
$(*)$ Soit $n \in \mathbb{Z}$. Montrer que $\begin{cases} n^1 \equiv 0\ [4] \text{ ou } n^2 \equiv 4\ [8] & \text{si } n \text{ est pair} \\ n^2 \equiv 1\ [8] & \text{si } n \text{ est impair} \end{cases}$

3 PGCD et PPCM

DÉFINITION 3 : **PGCD et PPCM**
Soient a et b deux entiers naturels dont l'un au moins est non nuls.
1. L'ensemble des entiers de $\mathbb{N}^*$ diviseurs communs à a et b admet un plus grand élément δ noté $\delta = a \wedge b$. C'est le *plus grand commun diviseur* des entiers a et b.
2. L'ensemble des entiers de $\mathbb{N}^*$ multiples communs de a et b admet un plus petit élément μ noté $\mu = a \vee b$. C'est le *plus petit commun multiple* des entiers a et b.

Remarque 7.

1. Le PPCM de deux entiers permet en particulier :
   (a) de limiter les calculs lors de l'addition de deux fractions rationnelles.
   (b) de déterminer la plus petite période d'une fonction périodique
2. Le PGCD de deux entiers permet de transformer une fraction rationnelle en une fraction irréductible.

Remarque 8. On définit de même :

1. le PGCD d'un nombre fini d'entiers naturels comme le plus grand diviseur commun à tous les entiers.
2. le PPCM d'un nombre fini d'entiers naturels comme le plus petit multiple commun à tous les entiers.

Remarque 9. On peut étendre les notions de PGCD et de PPCM à deux entiers relatifs dont l'un au moins est non nul. On définit alors :

$$a \wedge b = |a| \wedge |b| \quad \text{et} \quad a \vee b = |a| \vee |b|$$

LEMME 4 : **Ensemble des multiples communs à deux entiers**
Les multiples communs à deux entiers a et b sont les multiples de leur PPCM.

Preuve 4 : Soit m un multiple commun à a et b.
On effectue la division euclidienne de m par μ le PPCM et on démontre que le reste est nul.

PROPOSITION 5 : **Les opérateurs "PGCD" et "PPCM" sont commutatifs et associatifs**
Pour tout entiers relatifs a, b et c non nuls, on a :

1. $a \wedge b = b \wedge a$ et $a \vee b = b \vee a$
2. $(a \wedge b) \wedge c = a \wedge (b \wedge c) \quad (= a \wedge b \wedge c)$ et $(a \vee b) \vee c = a \vee (b \vee c) \quad (= a \vee b \vee c)$

Preuve 5 : La démonstration de l'associativité est admise pour l'instant...

Remarque 10. On peut ainsi définir le PGCD et le PPCM de n entiers : $\begin{cases} \text{pgcd}(x_1, \dots, x_n) = x_1 \wedge \cdots \wedge x_n \\ \text{ppcm}(x_1, \dots, x_n) = x_1 \vee \cdots \vee x_n \end{cases}$

`Exemple` 4. $(*)$ Déterminer le PGCD des 4 nombres suivants : 34, 56, 45, 124.

PROPOSITION 6 : **Relation entre PGCD et PPCM**
Soient a et b deux entiers naturels dont l'un au moins est non nul.
Alors :

$$\boxed{(a \wedge b)(a \vee b) = ab}$$

Preuve 6 :

1. On pose $\begin{cases} \delta = a \wedge b \\ \mu = a \vee b \end{cases}$ et a', b' tels que $\begin{cases} a = \delta.a' \\ b = \delta.b' \end{cases}$ avec $a' \wedge b' = 1$.
2. Remarquons que $\delta.a'.b'$ est un multiple commun à a et b et donc à μ, donc : $\exists k \in \mathbb{N}$ tel que $\delta.a'.b' = k.\mu$
3. Comme μ est un multiple commun à a et b, on a d'autre part : $\begin{cases} \mu = \alpha.a \\ \mu = \beta.b \end{cases}$. Ainsi : $\begin{cases} b' = k\alpha \\ a' = k\beta \end{cases}$.
4. Or, comme $a' \wedge b' = 1$ alors $k = 1$. Et donc : $\delta.a'.b' = \mu$.
5. On conclut en multipliant par δ.

Remarque 11. Ainsi, pour $a,\ b \in \mathbb{N}$:

1. si $a \wedge b = 1$ alors $\boxed{a \vee b = ab}$
2. si $\begin{cases} a = a'\delta \\ b = b'\delta \end{cases}$ avec $a' \wedge b' = 1$ alors $\boxed{a \vee b = \delta a'b'}$

`Exemple` 5.

Exercice : 2
$(*)$ Résoudre dans $\mathbb{N}^2$ le système $\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases}$.

3.1 L'algorithme d'Euclide et ses conséquences

THÉORÈME FONDAMENTAL 7 : **Théorème d'Euclide**
Pour tout entiers relatifs a et b non nuls.
Si $a = bq + r$ est la division euclidienne de a par b, alors : $PGCD(a,\ b) = PGCD(b,\ r)$.

Preuve 7 : On montre sans difficulté que $\{a,\ b\}$ et $\{b,\ r\}$ ont même ensemble de diviseurs communs.

Pour prouver l'égalité de deux PGCD (cad $a \wedge b = e \wedge f$)
On pourra prouver que les deux couples $(a,\ b)$ et $(e,\ f)$ ont même ensemble de diviseurs commun.
Cela revient à raisonner de la façon suivante :

1. Soit d un diviseur commun à a et b, montrons que $\begin{cases} d \mid e \\ d \mid f \end{cases}$ ...
2. Soit d un diviseur commun à e et f, montrons que $\begin{cases} d \mid a \\ d \mid b \end{cases}$ ...

Exercice : 3
(∗) Démontrer l'associativité de l'opérateur $\wedge$.

Algorithme d'Euclide
Le théorème précédent permet de construire un algorithme permettant de déterminer le PGCD de deux entiers non nuls a et b.

1. On pose $r_0 = a$ et $r_1 = b$
2. On construit alors une suite (r_k) strictement décroissante de *restes* en effectuant, tant que $r_k \neq 0$, la division euclidienne de r_{k-1} par r_k et en appelant r_{k+1} le nouveau reste obtenu.
$$r_{k-1} = r_k.q_k + r_{k+1}$$
3. D'après le théorème d'Euclide, on a $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$.
Comme (r_k) est une suite d'entiers strictement décroissante, il existe un rang n tel que $r_n \neq 0$ et $r_{n+1} = 0$.
4. On a alors $\begin{cases} a \wedge b = r_n \wedge r_{n-1} \\ r_n / r_{n-1} \end{cases}$ et ainsi : $\boxed{r_n = a \wedge b}$

`Exemple` 6. (∗) Utiliser l'algorithme d'Euclide pour déterminer le PGCD de $a = 2004$ et $b = 835$.
En déduire la valeur du PPCM.

Dessin

Algorithme d'Euclide

Exercice : 4
(∗) Construire en langage Python une procédure mettant en oeuvre l'algorithme d'Euclide.

COROLLAIRE 8 : **Caractérisation des diviseurs et multiples communs à a et b**

Soient deux entiers a et b.

1. d est un diviseur commun de a et b ssi d divise $a \wedge b$
2. m est un multiple commun de a et b ssi m est un multiple de $a \vee b$

Preuve 8 :

1. $\Rightarrow$ C'est une conséquence de l'algorithme précédent.
   $\Leftarrow$ Evident !
2. Déjà démontré !

Remarque 12. En d'autres termes :

1. $a \wedge b$ est le plus grand des diviseurs communs à a et b également pour la relation d'ordre partielle "divise".
2. Si a et b divise un entier c alors $a \vee b$ divise aussi c.

COROLLAIRE 9 : **Caractérisation du PGCD**
Si a et b sont 2 entiers relatifs non nuls, vérifiant $\begin{cases} a = a'\delta \\ b = b'\delta \end{cases}$ alors : $\boxed{\delta = a \wedge b \Longleftrightarrow a' \wedge b' = 1}$.

Preuve 9 : Par double contraposée.

Méthodes pour déterminer un PGCD

1. On pourra utiliser l'algorithme d'Euclide (lorsque les entiers a et b sont connus)
2. On pourra utiliser la caractérisation précédente, c'est à dire, montrer que :
   $$\text{il existe deux entiers } a' \text{ et } b' \text{ et un entier } \delta \text{ tels que } a' \wedge b' = 1 \text{ et } \begin{cases} a = \delta a' \\ b = \delta b' \end{cases}$$
3. On pourra enfin effectuer un raisonnement direct de type Analyse/Synthèse :
   "soit d un diviseur commun à a et b alors..."
   on utilisera en particulier le fait que d divise toute combinaison linéaire entière de a et b

PROPOSITION 10 : **2 formules de calcul**

Si a, b et c sont 3 entiers naturels non nuls alors :

$\underline{F_1}$: $\begin{cases} (ca) \wedge (cb) = c(a \wedge b) \\ (ca) \vee (cb) = c(a \vee b) \end{cases}$ $\quad$ $\underline{F_2}$: $a^k \wedge b^k = (a \wedge b)^k$ pour tout $k \in \mathbb{N}^*$

Preuve 10 :

1. Distributivité :
   (a) Pour la première :
   On écrit que $\begin{cases} a = \delta a' \\ b = \delta b' \end{cases}$ avec $a' \wedge b' = 1$. On a alors $\begin{cases} ac = c\delta a' \\ bc = c\delta b' \end{cases}$ avec $a' \wedge b' = 1$.
   On a donc $c\delta = (ac) \wedge (bc)$ d'après la caractérisation du PGCD.
   (b) On déduit la deuxième de la première à l'aide de la relation $ab = (a \wedge b)(a \vee b)$.

2. Puissance :
   On note $\delta = a \wedge b$ et $d = a^k \wedge b^k$ et on montre que $d = \delta^k$.
   Pour cela, on calcule $d = a^k \wedge b^k = ...$ en exprimant $\begin{cases} a = a'.\delta \\ b = b'.\delta \end{cases}$ avec $a' \wedge b' = 1$.
   On démontrera plus loin que $a'^k \wedge b'^k = 1$.

`Exemple` 7. $(*)$ Prouver que si $x \wedge y \wedge z = 1$ alors $x^2 \wedge y^2 \wedge z^2 = 1$

Exercice : 5
$(*)$ Soit a et b deux entiers relatifs tels que a^2/b^2. Montrer que a/b.

On pourra penser dans les raisonnements à utiliser l'équivalence : $b \mid a \Longleftrightarrow b = a \wedge b$.

3.2 Le théorème de Bezout

THÉORÈME FONDAMENTAL 11 : **Théorème de Bezout**
Soient a et b deux entiers relatifs non nuls.
On a :
$$a \wedge b = \delta \quad \Rightarrow \quad \exists (u,\ v) \in \mathbb{Z}^2 \quad \text{tels que} \quad au + bv = \delta$$

`Exemple` 8. **Méthode simple pour trouver u et v :**
Lorsque a et b sont simples, en comparant les multiples on peut trouver rapidement un couple de bezout.
Faites-le pour $(a,\ b) \in \{(5,\ 3),\ (11,\ 13),\ (4,\ 9)\}$.

Preuve 11 : La démonstration est donnée par l'algorithme suivant.

Remarque 13.

1. On dira que $(u,\ v)$ tel que $au + bv = \delta$ est un *couple de Bezout* associé à a et b.
2. On retrouve ainsi le fait qu'un diviseur commun à a et b divise aussi $a \wedge b$.
3. Comme on le verra plus tard, il existe une infinité de couples de Bezout.
4. ⚠ : la réciproque de ce théorème n'est vraie que si δ est un diviseur commun à a et b.
5. Le théorème de Bezout est très souvent utilisé dans les exercices ou les démonstrations.

Algorithme pour trouver un couple de Bezout
Soient a et b deux entiers relatifs non nuls tels que $a \wedge b = \delta$.
On pourra trouver un couple de Bezout associé à a et b en procédant de la façon suivante :

1. On applique l'algorithme d'Euclide à a et b.
   On construit les suites $\begin{cases} (r_n) \\ (q_n) \end{cases}$ telles que $\begin{cases} r_0 = a \\ r_1 = b \end{cases}$ et : $\boxed{r_n = q_{n+1}.r_{n+1} + r_{n+2}}$ avec $0 < r_{n+1} < r_n$.
   Notons $r_{n_0} = \delta$ le dernier terme non nul de la suite (r_n).
2. On recherche des suites (u_n) et (v_n) telles que $r_n = u_n a + v_n b$ pour tout $n \in [\![1, n_0]\!]$.
   On constate que $\begin{cases} (u_n) \\ (v_n) \end{cases}$ définies par $\begin{cases} (u_0,\ v_0) = (1,\ 0) \\ (u_1,\ v_1) = (0,\ 1) \end{cases}$ et $\begin{cases} u_{n+2} = u_n - q_{n+1}u_{n+1} \\ v_{n+2} = v_n - q_{n+1}v_{n+1} \end{cases}$ conviennent.
3. Comme d'autre part $\delta = u_{n_0} a + v_{n_0} b$, alors les coefficients de Bezout sont u_{n_0} et v_{n_0}.
4. Lors de l'application manuelle de cet algorithme, on pourra présenter les calculs intermédiaires dans un tableau de la forme :

	$r_0 = a$	$r_1 = b$	r_2	$\dots$	r_n	$\dots$	δ
q_k		q_1	q_2	$\dots$	q_n	$\dots$	
u_k	1	0	u_2	$\dots$	u_n	$\dots$	$u_{n_0} = u$
v_k	0	1	v_2	$\dots$	v_n	$\dots$	$v_{n_0} = v$

`Exemple` 9. $(*)$ Appliquer l'algorithme précédent pour déterminer :

1. un couple de Bezout pour $a = 22$ et $b = 17$.
2. un couple de bezout pour $a = 127$ et $b = 35$.

`Exemple` 10. $(**)$ Sauriez-vous construire un programme déterminant un couple de Bezout pour un couple $(a,\ b)$ donné ?

PROPOSITION 12 : **Généralisation de Bezout**
Soient $a_1,\ \dots,\ a_n$ et $n \in \mathbb{N}^*$ entiers naturels non nuls.
On a :
$$a_1 \wedge \dots \wedge a_n = \delta \quad \Rightarrow \quad \exists (u_1,\ \dots,\ u_n) \in \mathbb{Z}^n \quad \text{tels que} \quad a_1u_1 + \dots + a_nu_n = \delta$$

Preuve 12 : Par récurrence sur n.

4 Les nombres premiers entre eux

DÉFINITION 4 : **Nombres premiers entre eux**
Soient a et b deux entiers relatifs non nuls.
On dit que a et b sont *premiers entre eux* ssi $a \wedge b = 1$

`Exemple` 11. (∗) Démontrer que deux entiers naturels consécutifs sont premiers entre eux.

Remarque 14. On dira qu'une fraction a/b est *irréductible* lorsque $a \wedge b = 1$.

Exercice : 6

(∗) Prouver que la fraction $\frac{21n+4}{14n+3}$ est irréductible pour tout $n \in \mathbb{N}$.

THÉORÈME FONDAMENTAL 13 : **Théorème de Bezout (bis)**
Soient a et b deux entiers relatifs non nuls.
On a :

$$a \wedge b = 1 \iff \exists (u,\ v) \in \mathbb{Z}^2 \quad \text{tels que} \quad au + bv = 1$$

Preuve 13 :

$\Rightarrow$ Conséquence immédiate du théorème de Bezout.

$\Leftarrow$ Comme $a \wedge b$ divise a et b, alors il divise $au + bv$, c'est à dire 1.

Pour prouver que deux entiers sont premiers entre eux
On peut :

1. Soit montrer que leur PGCD est égal à 1 avec l'algorithme d'Euclide
2. Soit montrer qu'un diviseur commun divise nécessairement 1
3. Soit utiliser le théorème de Bezout(bis)

`Exemple` 12. (∗) Soit $n \in \mathbb{N}^*$ avec $n \geq 2$. Déterminer les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z},\ \times)$.
Dans quel cas tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont-ils inversibles ?

COROLLAIRE 14 :
Si a, b et c sont 3 entiers relatifs non nuls alors : $\begin{cases} c \text{ divise } a \\ a \wedge b = 1 \end{cases} \Rightarrow c \wedge b = 1.$

En d'autres termes : "Si $a \wedge b = 1$ alors les diviseurs de a sont également premiers avec b."

Preuve 14 :

M1 : On utilise l'égalité de Bezout pour traduire $a \wedge b = 1$.

M2 : On peut aussi effectuer une démonstration directe.

COROLLAIRE 15 :

— Si a, b_1 et b_2 sont 3 entiers relatifs non nuls, alors : $\begin{cases} a \wedge b_1 = 1 \\ a \wedge b_2 = 1 \end{cases} \Rightarrow a \wedge b_1 b_2 = 1.$

— De façon plus générale :

1. si a est premier avec b_1, ...et b_k alors $a \wedge b_1 \dots b_k = 1$.
2. $a \wedge b = 1 \Longleftrightarrow a^p \wedge b^q = 1$ pour tout $(p,\ q) \in \mathbb{N}^{*2}$

Preuve 15 : Immédiat avec le théorème de Bezout, puis on généralise par récurrence.

`Exemple` 13. (∗) Si a et b sont premiers entre eux, montrer que $ab \wedge (a + b) = 1$.

THÉORÈME FONDAMENTAL 16 : **Théorème de Gauss**
Soient a, b et c trois entiers naturels non nuls.
On a :

$$\text{Si} \quad \begin{cases} a \text{ divise } bc \\ a \wedge b = 1 \end{cases} \quad \text{alors} \quad a \text{ divise } c$$

Preuve 16 : Conséquence immédiate du théorème de Bezout.

Exercice : 7

(∗∗) L'armée de Sun Zi.
Pour compter l'effectif de son armée, Sun zi procède ainsi :

1. En regroupant les soldats par 3, il en reste 2
2. En les regroupant par 5 il en reste 3
3. En les regroupant par 7 il en reste 2

Quel est l'effectif minimum de l'armée de Sun Zi ?

Il existe une méthode plus générale (vue en TD) de résolution de ce type de problème dit "problème des restes chinois".

Formes à reconnaître en arithmétique :

1.	$ab = c$	permet d'affirmer que a et(ou) b divise c
2.	$ab = cd$	permet éventuellement d'appliquer le théorème de Gauss pour montrer que a divise c
3.	$ab + cd = 1$	permet d'en déduire que $a \wedge c = 1$

`Exemple` 14. Prouver d'une fraction irréductible a un nombre de décimales fini si et seulement si son dénominateur est de la forme $2^i.5^j$ avec $(i,\ j) \in \mathbb{N}^2$.

Equations diophantiennes
Soient A, B et C trois entiers relatifs non nuls et on considère l'équation :

$$(E)\ :\ Ax + By = C \quad \text{avec } (x,\ y) \in \mathbb{Z}^2$$

Voici une méthode permettant de résoudre cette équation.

1. Soit $\delta = A \wedge B$.
   (a) Si δ ne divise pas C alors on montre facilement que $\mathcal{S} = \emptyset$.
   (b) Sinon, en divisant par δ, l'équation (E) on se ramène à $(E')\ :\ A'x + B'y = C'$ avec $A' \wedge B' = 1$.
2. On détermine une solution particulière de (E') en recherchant un couple de Bezout associé à A' et B'.
3. On en déduit alors l'ensemble $\mathcal{S}$ de toutes les solutions par une Analyse/Synthèse à l'aide du théorème de Gauss.

`Exemple` 15. $(*)$ Résoudre dans $\mathbb{Z}$ les équations : $13x + 5y = 4$ et $24x + 20y = 36$

Corollaire 17 : Soient a, b et c trois entiers relatifs non nuls. $\begin{cases} a \text{ divise } c \\ b \text{ divise } c \\ a \wedge b = 1 \end{cases} \Rightarrow ab$ divise c

Preuve 17 : Immédiat avec le théorème de Gauss.

`Exemple` 16. $(*)$ Soit $p > 3$ un nombre premier. Montrer que $24 \mid p^2 - 1$.

Définition 5 : **N nombres premiers entre eux**
Soient $a_1,\ \ldots,\ a_n,\ n \in \mathbb{N}^*$ entiers naturels non nuls.

1. On dit que $a_1,\ \ldots,\ a_n$ sont *premiers entre eux dans leur ensemble* ssi $a_1 \wedge \cdots \wedge a_n = 1$
2. On dit que $a_1,\ \ldots,\ a_n$ sont *premiers entre eux 2 à 2* ssi $\forall i,\ j \in [\![1, n]\!]$ tels que $i \neq j$, $a_i \wedge a_j = 1$

Remarque 15.

1. n entiers peuvent être premiers entre eux dans leur ensemble sans être premiers entre eux deux à deux. Montrer que les entiers 10, 6 et 15 sont premiers entre eux. Le sont-ils deux à deux ?
2. Prouver que si parmi n entiers, deux sont premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. En deduire une implication entre les deux notions.

Proposition 18 : Le théorème précédent se généralise au cas a est divisible par $b_1, \ldots, b_k$ avec les b_i premiers entre eux deux à deux.

5 Les nombres premiers

DÉFINITION 6 : **Nombre premier**

Dans $\mathbb{N}^*$, on dira qu'un nombre est premier ssi : $\left\{ \begin{array}{l} \text{il est différent de 1} \\ \text{il n'admet pas d'autre diviseur que 1 et lui-même} \end{array} \right.$.

On pourra noter $\mathcal{P}$ l'ensemble des nombres premiers.

Remarque 16. Les nombres premiers sont les *atomes* de l'arithmétique. Comme les atomes permettent en chimie de construire toutes les molécules, nous verrons en effet que les nombres premiers engendrent l'ensemble des nombres entiers.

Exercice : 8

(∗) Soit $p,\ q \in \mathbb{N}^*$ tels que $\frac{p}{q} > 1$. Déterminer les valeurs $n \in \mathbb{N}^*$ telles que $n\frac{p}{q}$ est premier.

Remarque 17. Le crible d'érathostène permet de déterminer les premiers nombres premiers.
Proposer une programmation de cet algorithme en Python.

Exercice : 9

(∗∗) Soit a et p deux entiers supérieurs à 2.

1. Montrer que si $a^p - 1$ est premier alors $a = 2$ et p est premier.
2. Etudier la réciproque de la proposition précédente.

Lorsque $2^p - 1$ est premier alors ce nombre est appelé un "nombre premier de Mersenne".

Pour prouver qu'un nombre n'est pas premier, on pourra montrer :

$$\text{qu'il s'écrit sous la forme } n = ab \text{ avec } a,\ b \in \mathbb{Z} \text{ et } \left\{ \begin{array}{l} a \geq 2 \\ b \geq 2 \end{array} \right.$$

Un tel nombre est dit *composé*.

Remarque 18. Un nombre $n \in \mathbb{N}$ est composé s'il s'écrit sous la forme $n = ab$ avec $a,\ b \in [\![2, n-1]\!]$

`Exemple` 17. (∗∗) Montrer que $\forall n \in \mathbb{N}^*,\ 4n^3 + 6n^2 + 4n + 1$ est un nombre composé. (Utilisez votre calculatrice...)

5.1 Propriétés des nombres premiers

PROPOSITION 19 : **Propriétés des nombres premiers**

1. Soit $p \in \mathbb{N}$ un nombre premier et $n \in \mathbb{Z}$. Alors, soit p divise n, soit $p \wedge n = 1$.
   En particulier, un nombre premier p est premier avec tous les éléments de $[\![1, p-1]\!]$.
2. Deux nombres premiers distincts sont premiers entre eux.
3. Si un nombre premier divise un produit d'entiers, alors il divise l'un d'entre eux.

Preuve 19 :

1. Pas de difficulté.
2. Pas de difficulté.
3. On applique le théorème de Gauss et la propriété 1.

Remarque 19. Ainsi, si un nombre premier p divise m^k alors p divise m.

`Exemple` 18. (∗∗)

1. Soit p un nombre premier. Prouver que $\sqrt{p}$ est un irrationnel.
2. Démontrer par l'absurde que pour tout $n \in \mathbb{N}$, et p premier avec $p \geq 3$, $p^n + 1$ est un nombre pair.

THÉORÈME 20 : **Le petit théorème de Fermat**
Soit p un nombre premier et $n \in \mathbb{Z}$.
On a :
- $n^p \equiv n[p]$.
- $n^{p-1} - 1 \equiv 0[p]$ si p ne divise par n.

Preuve 20 : On montre que $\forall k \in [\![1, p-1]\!]$, on a $\binom{p}{k} \equiv 0\ [p]$.
Puis on en déduit que :
1. $\forall (a,\ b) \in \mathbb{Z}^2$, on a $(a+b)^p \equiv a^p + b^p\ [p]$.
2. $\forall n \in \mathbb{Z}$ on a $n^p \equiv n[p]$. *récurrence pour $n \in \mathbb{N}$ - cas particulier $p = 2$ pour $n \in \mathbb{Z}\backslash\mathbb{N}$*
3. si p ne divise par n alors $n^{p-1} - 1 \equiv 0[p]$. *Gauss*

Remarque 20.
1. Ce théorème est entre autre utilisé dans la méthode de codage RSA.
2. Comme le montre l'exemple suivant, il permet de simplifier rapidement des calculs modulo un nombre premier p.

`Exemple` 19. $(*)$ Calculer une valeur simple de 2016^{2017} modulo 11.

THÉORÈME 21 : Tout entier naturel $n \geq 2$ admet un diviseur premier.

Preuve 21 :
1. Méthode 1 : Par récurrence (forte) ...
2. Méthode 2 : On note $\mathcal{D}(n)$ l'ensemble des entiers naturels différents de 1 qui divisent n.
   $\mathcal{D}(n)$ est une partie de $\mathbb{N}$ non vide, donc il admet un plus petit élément.
   On montre alors que cet élément est un nombre premier.

THÉORÈME 22 :
Tout entier composé n admet un diviseur premier $p \leq \sqrt{n}$.

Preuve 22 : On note $n = ab$ avec $\begin{cases} a \geq 2 \\ b \geq 2 \end{cases}$. On montre que $\begin{cases} a > \sqrt{n} \\ b > \sqrt{n} \end{cases}$ est impossible...
Puis, on suppose par exemple que $a \leq \sqrt{n}$ et comme a admet un diviseur premier ...

Remarque 21. **Applications :**

1. Pour tester si un nombre est premier :
   Un entier n qui n'admet pas de diviseur premier inférieur à $\sqrt{n}$ est un nombre premier.

2. Dans le crible d'érathostène, il suffit d'éliminer tous les multiples des nombres premiers inférieurs à $\sqrt{N}$ pour déterminer tous les nombres premiers inférieurs à N.

`Exemple` 20. $(*)$ Prouver que 2011 est un nombre premier.

Exercice : 10
$(*)$ Soit m un entier strictement plus grand que 1.
Montrer que si m divise $(m-1)! + 1$ alors m est premier.

THÉORÈME FONDAMENTAL 23 : **Infinité des nombres premiers**
Il existe une infinité de nombres premiers.

Preuve 23 : Il existe un grand nombre de démonstrations possibles.
Procédons ici par l'absurde en supposant que $\mathcal{P} = \{p_1,\ \ldots,\ p_k\}$.
On considère alors l'entier $a = p_1.p_2 \ldots p_k + 1$.
Comme a est un nombre composé (puisque strictement supérieur à tous les p_i), il est divisible par l'un des p_i.
Et comme a et $p_1.p_2 \ldots p_k$ sont divisibles par ce p_i alors 1 l'est aussi ... ce qui est impossible !

Remarque 22. Il a été prouvé que le nombre de nombres premiers inférieurs ou égal à n était équivalent à $\frac{n}{\ln n}$.

5.2 Décomposition d'un entier en produit de facteurs premiers

THÉORÈME FONDAMENTAL 24 : **Décomposition d'un entier en produit de facteurs premiers**
Tout entier naturel $n \in \mathbb{N}^*$ se décompose de façon unique en produit de facteurs premiers.

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

où :

1. $\mathcal{P}$ est l'ensemble des nombres premiers
2. $(\alpha_p)_{p\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ une suite presque nulle
3. $v_p(n) = \alpha_p$ est appelée la *valuation p-adique* de l'entier n.

Preuve 24 : On peut démontrer l'existence par une récurrence forte et l'unicité de façon classique.

Exercice : 11
(∗∗) Pendant la guerre de 1914-1918, des travaux de fortification mirent au jour une pertuisane enterrée lors d'un très ancien combat. Si l'on multiplie la longueur de la pertuisane, évaluée en pieds, par la moitié de l'âge du capitaine qui se distingua au cours de cette bataille, puis par le nombre de jours que comporte le mois où la pertuisane fut trouvée, enfin par le quart du nombre des années écoulées entre sa disparition et sa découverte, on obtient le nombre : 225 533.

1. Comment s'appelait le capitaine ?
2. Au cours de quelle bataille la pertuisane fut-elle enterrée ?

Remarque 23. Pour deux entiers naturels non nuls a et b, on a : $v_p(a \times b) = v_p(a) + v_p(b)$

`Exemple` 21. (∗)

1. Prouver que $\log 2$ est irrationnel.
2. Montrer que : $v_2(1000!) = 994$

PROPOSITION 25 : **Une caractérisation des nombres premiers entre eux**
Soient x, y deux entiers plus grands que 2 et X et Y les ensembles de nombres premiers intervenant dans leurs décompositions en facteurs premiers respectives. On a alors :

$$x \wedge y = 1 \iff X \cap Y = \emptyset$$

Preuve 25 : Facile par double contraposée.

Remarque 24. **Méthode :** a et b sont donc premiers entre eux si et seulement si, ils n'ont pas de nombre premier en commun dans leur décomposition en facteur premier. Cela continue une 4ème méthode pour prouver que deux nombres sont premiers entre eux. Vous souvenez-vous des 3 autres ?

`Exemple` 22. Prouver que les deux entiers suivants sont premiers entre eux : $\begin{cases} a = 5377456 = 2^4.7^2.19^3 \\ b = 5671875 = 3.5^6.11^2 \end{cases}$.

PROPOSITION 26 : **Caractérisation de la divisibilité**
Soit $n,\ d \in \mathbb{N}^*$ de décomposition en facteurs premiers : $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$ et $d = \prod_{p\in\mathcal{P}} p^{v_p(d)}$.
On a alors :

$$d \mid n \iff \forall p \in \mathcal{P},\quad v_p(d) \leq v_p(n)$$

L'ensemble des diviseurs positifs de n est alors :

$$\mathcal{D}_n = \{\prod_{p\in\mathcal{P}} p^{\alpha_p} \mid \forall p \in \mathcal{P},\ 0 \leq \alpha_p \leq v_p(n)\}$$

Preuve 26 : Pas de réelle difficulté.

`Exemple` 23. (∗) La décomposition en facteurs premiers reste un problème très difficile pour les grands nombres. En revanche, elle ne pose pas de difficulté pour les *petits* nombres.

1. Décomposer 2004 en facteurs premiers.
2. Déterminer l'ensemble de ses diviseurs

Exercice : 12
(∗∗) Résoudre dans $\mathbb{N}^2$ l'équation $11(a \wedge b) + (a \vee b) = 203$ avec $a \leq b$.

Exercice : 13
(∗∗) Soit $n \in \mathbb{N}\backslash\{0;1\}$ dont la décomposition en nombre premier est $n = \prod_{i=1}^{N} p_i^{\alpha_i}$.
On note $d(n)$ le nombre de diviseurs positifs de n, $\pi(n)$ et $\sigma(n)$ le produit et la somme de ceux-ci.
Montrer que :

1. $d(n) = \prod_{i=1}^{N}(\alpha_1 + 1)$
2. $\pi(n) = \prod_{i=1}^{N} p^{\alpha_i(\alpha_i+1)/2}$
3. $\sigma(n) = \prod_{i=1}^{N} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$

COROLLAIRE 27 : **Expression du PGCD et du PPCM**
Soient a et b deux entiers naturels non nuls de décompositions en facteurs premiers suivantes :

$$a = \prod_{p\in\mathcal{P}} p^{v_p(a)} \quad \text{et} \quad b = \prod_{p\in\mathcal{P}} p^{v_p(b)}$$

On a alors :

$$\boxed{a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),\ v_p(b))}} \quad \text{et} \quad \boxed{a \vee b = \prod_{p\in\mathcal{P}} p^{\max(v_p(a),\ v_p(b))}}$$

Preuve 27 :

1. Tous les diviseurs communs à a et b divisent $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),\ v_p(b))}$ qui divise aussi a et b.
2. Il suffit d'utiliser la relation $(a \wedge b)(a \vee b) = ab$.

Remarque 25. **Méthode :** Le théorème précédent nous donne une 4ème méthode de recherche du PGCD de deux entiers.

`Exemple` 24. (∗) Déterminer le PGCD et le PPCM de $a = 6513$ et $b = 2004$.

Exercice : 14
(∗) Reprendre les questions suivantes en utilisant le théorème précédent :

1. Montrer que si $b^2 \mid a^2$ alors $b \mid a$.
2. Montrer que si $a \wedge b = 1$ alors $a^p \wedge b^q = 1$.
3. Justifier la distributivité de $\times$ sur $\wedge$ et $\vee$.

COROLLAIRE 28 :
Les lois $\wedge$ et $\vee$ sont distributives l'une sur l'autre : $\begin{cases} a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \end{cases}$

Preuve 28 : Démonstration admise. Elle utilise les formules démontrées dans le corollaire précédent.

6 Exercice : Les nombres parfaits pairs (Euler 1849)

Le but de cet exercice est de déterminer une expression pour les nombres parfaits pairs.

1. Soit $p \in \mathbb{N}^*$ tel que $2^p - 1$ soit premier.
   (a) Montrer que p est premier.
   (b) Montrer que le nombre $N = 2^{p-1}(2^p - 1)$ est un nombre parfait.

2. On souhaite maintenant prouver que tout nombre parfait pair est de la forme $2^{p-1}(2^p-1)$ avec (2^p-1) premier et donc p est premier. Effectuons pour cela une analyse.
   Soit N un nombre parfait pair.

   (a) Forme adaptée pour N :
   Prouver qu'il existe $n \in \mathbb{N}$ $(n \geq 1)$ et $a \in \mathbb{N}$ impair tel que : $N = 2^n.a$.
   Dans la suite, on note $\sigma(N)$ la somme des diviseurs de N.

   (b) Exploitation des hypothèses :
   i. Prouver que $\sigma(N) = (2^{n+1}-1)\sigma(a)$, puis que $2^{n+1}a = (2^{n+1}-1)\sigma(a)$.
   ii. Justifier que $\begin{cases} \sigma(a) = 2^{n+1}b \\ a = (2^{n+1}-1)b \end{cases}$ avec b un nombre impair.

   (c) Fin du raisonnement :
   i. Par l'absurde : Supposons que a n'est pas un nombre premier.
   En traitant séparément les cas où $b = 1$ et $b > 1$ et en minorant $\sigma(a)$ (on trouvera 3 diviseurs), montrer que l'on arrive à une contradiction.

3. Conclure.

7 Connaissez-vous votre cours ?

Vous devez impérativement savoir répondre aux différentes questions suivantes :

	Questions	Réponses attendues
1.	Résoudre dans $\mathbb{N}^2$ l'équation $xy + x = 4$	$(1,\ 3)$, $(2,\ 1)$ et $(4,\ 0)$
2.	Trouver les couples $(x,\ y) \in \mathbb{Z}^2$ tels que $x - y \mid x$	$\{(2p,\ p) \mid p \in \mathbb{Z}\}$
3.	Connaissez-vous toutes les relations opératoires sur la relation de congruence ? Sauriez-vous prouver qu'il s'agit d'une relation d'équivalence ?	cf cours
4.	Savez-vous définir $\mathbb{Z}/n\mathbb{Z}$ et prouver que c'est un anneau ?	cf cours
5.	Quels sont les théorèmes à utiliser pour prouver l'existence du PPCM et du PGCD ?	cf cours
6.	Comment déterminer le PGCD de deux nombres ?	- euclide - decomp. fact. prem.
7.	Quel est le lien entre PGCD et diviseurs communs ? Quel est le lien entre PPCM et multiples communs ?	cf cours cf cours
8.	Quel est le lien entre les notions de "P1 : premiers entre eux dans leur ensemble" et "P2 : premiers entre eux deux à deux" ?	P2 $\Rightarrow$ P1
9.	Quel est la propriété fondamentale qui permet de justifier l'algorithme d'euclide ?	cf cours

10.	Quelle méthode permet de prouver que $a \wedge b = c \wedge d$? Et que $a \vee b = c \vee d$?	Mêmes div. communs Mêmes mult. communs
11.	Citez les deux théorèmes de Bezout !	cf cours
12.	Savez-vous déterminer un couple de Bezout ? Faites-le pour $11u + 13v = 1$.	$(6,\ -4)$
13.	Comment prouver que deux nombres sont premiers entre eux ?	- relation de Bezout - les div. communs - decomp. fact. prem.
14.	Savez-vous démontrer que le PGCD et le PPCM sont liés par : $(a \wedge b)(a \vee b) = ab$	cf cours
15.	Que dit le théorème de Gauss ? Que permet-il de démontrer ?	cf cours
16.	Rappelez en détail la méthode permettant de résoudre des équations diophantiennes.	cf cours
17.	Rappeler le théorème permettant de prouver que si $p > 3$ est premier alors $24 \mid p^2 - 1$	cf cours
18.	Comment prouver qu'un nombre est composé (non premier) ?	cf cours
19.	Sauriez-vous prouver que si p est premier alors $\sqrt{p}$ est un irrationnel ?	cf cours
20.	Donner un algorithme rapide permettant de vérifier si un nombre est premier ou pas.	cf cours
21.	Comment déterminer tous les diviseurs d'un entier ?	decomp. fact. prem.

8 Exercices de TD

Codage :

1. Les exercices avec des coeurs ♡ sont à traiter en priorité.
2. Le nombre d'étoiles $*$ ou de coeurs ♡ correspond à la difficulté des exercices.

I] Divisibilité - Congruences

1. Bien connaître le théorème de la division euclidienne.
2. Bien connaître les règles de calcul sur les congruences.
3. Les relations de divisibilité s'expriment comme des relations de congruence (et inversement).
4. Les équations de nombres entiers se résolvent par analyse\synthèse en faisant apparaître des divisibilités.

Exercice de TD : 1

(♡) Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ et q le quotient de la division euclidienne de $a-1$ par b.
Déterminer $\forall n \in \mathbb{N}$, le quotient de la division euclidienne de $ab^n - 1$ par b^{n+1}.

Exercice de TD : 2

(♡) Quel est le reste de la division euclidienne de $1234^{4321} + 4321^{1234}$ par 7 ?

Exercice de TD : 3

(♡) Trouver les entiers $n \in \mathbb{Z}$ tel que $10 \mid n^2 + (n+1)^2 + (n+3)^2$.
On pensera à exprimer n modulo 10.

Exercice de TD : 4

(∗∗) Montrer que pour tout $n \in \mathbb{N}$:

1. $6 \mid 5n^3 + n$
2. $7 \mid 3^{2n+1} + 2^{n+2}$
3. $5 \mid 2^{2n+1} + 3^{2n+1}$
4. $11 \mid 3^{8n}.5^4 + 5^{6n}.7^3$
5. $9 \mid 4^n - 1 - 3n$
6. $15^2 \mid 16^n - 1 - 15n$

Exercice de TD : 5

(∗∗) Soient $a \in \mathbb{Z}$ impair et $n \in \mathbb{N}$ tel que $n \geq 3$.
Montrer que $a^{2^{n-2}} \equiv 1\ [2^n]$.

Exercice de TD : 6

(∗∗) Montrer que dans la suite (u_n) de terme général $u_n = 2^n - 3$, il y a :

1. une infinité de termes divisibles par 5,
2. une infinité de termes divisibles par 13,
3. aucun terme divisible par 65.

Exercice de TD : 7

(∗) Soit $k \in \mathbb{N}^*$. Montrer que le produit de k entiers consécutifs est divisible par $k!$.
On pensera à utiliser les coefficients binomiaux.

Exercice de TD : 8

(∗∗) Montrer que pour tout entier n tel que $n \geq 5$, on a : $9 \mid \sum_{k=1}^{n} k^2 k!$.

Exercice de TD : 9

(∗) L'équation $x^3 + x^2 + 2x + 1 = 0$ admet-elle des solutions rationnelles ?

II] PGCD et PPCM

1. On détermine le PGCD de deux nombres à l'aide de
   (a) l'algorithme d'Euclide
   (b) la décomposition en facteurs premiers de ces nombres
2. On détermine le PPCM
   (a) en recherchant le PGCD
   (b) en appliquant la formule qui relie les deux
3. On montre que $\delta = a \wedge b$ en prouvant que δ divise a et b et que tout diviseur de a et b divise aussi δ
4. On montre que $a \wedge b = c \wedge d$ en montrant que a, b et c, d admettent le même ensemble de diviseurs communs.
5. Savoir déterminer un couple de Bezout (avec la liste des multiples ou avec le tableau).
6. $a \wedge b = |a| \wedge |b|$ et $a \vee b = |a| \vee |b|$
   (a) L'ensemble des diviseurs communs à deux nombres est l'ensemble des diviseurs du PGCD
   (b) L'ensemble des multiples communs à deux nombres est l'ensemble des multiples du PPCM
7. Bien connaître le théorème de Bezout.

Exercice de TD : 10

(∗) Résoudre dans $\mathbb{N}^2$: $\begin{cases} x+y=56 \\ x \vee y = 105 \end{cases}$ puis $\begin{cases} x+y=56 \\ x \wedge y = 7 \end{cases}$.

Exercice de TD : 11

(∗) Résoudre dans $\mathbb{N}^2$: $x \wedge y + x \vee y = x + y$.

Exercice de TD : 12

(♡) Un agriculteur achète au marché 100 volailles : des poussins, des poules et des coqs.
Il débourse pour cela 100 euros sachant qu'un poussin vaut 0,1 euros, une poule 3 euros et un coq 6 euros.
Combien a-t-il acheté de poussins, de poules et de coqs ?

Exercice de TD : 13

(♡♡)

1. Résoudre dans $\mathbb{Z}^2$ l'équation : $11x + 5y = 8$
2. Montrer que si l'on remplace 8 par $n \geq 55$ alors il existe une solution dans $\mathbb{N}^2$.
3. Que dire si $n = 37$?

Exercice de TD : 14

(♡) Soit $a,\ b \in \mathbb{N}^*$ tels que $a \wedge b = 1$ et $c \in \mathbb{N}^*$.
Montrer que $a \wedge bc = a \wedge c$.

III] Nombres premiers entre eux

1. Pour démontrer que deux nombres sont premiers entre eux, on peut :
   (a) Prouver que leur PGCD est égal à 1
   (b) Utiliser le théorème de Bezout.
   (c) Utiliser la caractérisation à l'aide des décompositions en facteurs premiers.
2. Bien retenir les théorèmes suivants sur les nombres premiers :
   (a) Si a et b divisent x avec $a \wedge b = 1$ alors ab divise x.
   (b) Si $a \wedge b_1 = 1$ et $a \wedge b_2 = 1$ alors $a \wedge b_1 b_2 = 1$. Bien connaître les généralisations...
   (c) Le lemme de Gauss.
   On pensera en particulier à l'utiliser lorsque l'on obtient une relation de la forme $ab = cd$.
   (d) Si $d \mid a$ et que $a \wedge b = 1$ alors $d \wedge b = 1$.
3. Savoir résoudre les équations diophantiennes.

Exercice de TD : 15

(∗) Montrer que pour tout $n \in \mathbb{N}$, on a :

1. $(n^2 + n) \wedge (2n + 1) = 1$
2. $(3n^2 + 2n) \wedge (n + 1) = 1$

Exercice de TD : 16

(♡) **Restes chinois**.

Cet exercice propose une méthode pour résoudre le système : (S) $\begin{cases} x \equiv 3[25] \\ x \equiv 10[17] \end{cases}$ où $x \in \mathbb{Z}$.

On introduit pour cela les deux systèmes : $(S1)$ $\begin{cases} x \equiv 1[25] \\ x \equiv 0[17] \end{cases}$ et $(S2)$ $\begin{cases} x \equiv 0[25] \\ x \equiv 1[17] \end{cases}$.

1. Démontrer que 25 et 17 sont premiers entre eux. Déterminer une relation de Bezout entre 25 et 17.
2. En déduire une solution x_1 de $(S1)$ puis une solution x_2 de $(S2)$.
3. En déduire une solution particulière x_0 de (S) puis résoudre (S).

Une généralisation de cette méthode est proposée dans l'exercice suivant...

Exercice de TD : 17

(∗∗) **Restes Chinois : méthode générale**

Cet exercice est une généralisation de l'exercice précédent.

1. Soient a_1, a_2, ..., $a_n \in \mathbb{N}^*$, premiers entre eux 2 à 2. Soient y_1, y_2, ..., $y_n \in \mathbb{Z}$.
   (a) Démontrer que $\forall k \in [\![1, n]\!]$, les entiers a_k et $b_k = \prod_{i \neq k} a_i$ sont premiers entre eux.
   (b) Soit $k \in [\![1, n]\!]$. Démontrer que le système (S_k) $\{x \equiv \delta_{i,k}\ [ai],\ 1 \leq i \leq n$ admet une solution entière x_k.
   (c) Démontrer que le système (S) $\{x \equiv y_i[a_i],\ 1 \leq i \leq n$ admet une solution entière x_0. Résoudre (S).
2. Application :
   Jack Sparrow partage un butin de N pesos à parts égales entre ses 25 hommes d'équipages et il ne garde que le reste de 3 pesos. Il perd 8 pirates suite à une dysentrie sévère et le butin N est de nouveau partagé et il lui reste alors 10 pesos. Suite à une attaque des sbires de Davy Jones, il ne lui reste que 13 hommes et ce dernier partage le gratifie de 7 pesos. Finalement, il part seul avec tout le butin. Quel est sa fortune minimale ?

Exercice de TD : 18

(♡♡) Montrer que pour tout entier $n \in \mathbb{N}^*$, $n+1$ et $2n+1$ sont premiers entre eux.
En déduire que $(n+1) \mid \binom{2n}{n}$.

Exercice de TD : 19

(♡♡) Soient a et b deux entiers non nuls premiers entre eux et un couple de Bezout $(u_0,\ v_0) \in \mathbb{Z}^2$ tel que $au_0 + bv_0 = 1$.

1. Déterminer tous les couples d'entiers $(u,\ v) \in \mathbb{Z}^2$ tels que : $\quad au + bv = 1$.
2. Si $a,\ b \in \mathbb{N}^*$, montrer qu'il existe deux entiers $(u,\ v) \in \mathbb{Z}^2$ tels que : $\quad au + bv = 1 \quad$ et $\quad \begin{cases} |u| < b \\ |v| \leq a \end{cases}$

Exercice de TD : 20

(∗∗) Pour $n \in \mathbb{N}$, montrer qu'il existe un couple unique $(a_n,\ b_n) \in \mathbb{N}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$ avec $a_n \wedge b_n = 1$.

Exercice de TD : 21

(∗∗) Pour $n \in \mathbb{N}$, on définit $M_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n$.

1. Montrer que M_n est pair.
2. Déterminer une relation de la forme $M_{n+2} = aM_{n+1} + bM_n$.
3. En déduire que 2^n divise M_n.

Exercice de TD : 22

(∗ ∗ ∗) Soit a et b deux entiers relatifs premiers entre eux et $d \in \mathbb{N}$ un diviseur de ab.
On souhaite montrer que $\exists!(d_1,\ d_2) \in \mathbb{N}^2$ tel que $d = d_1d_2$, $d_1 \mid a$ et $d_2 \mid b$.

1. Prouver le résultat précédent à l'aide du théorème de décomposition de facteurs premiers.
2. Autre méthode :
   (a) Analyse : Prouver que si d_1 et d_2 conviennent, alors $d_1 = d \wedge a$ et $d_2 = d \wedge b$
   (b) Synthèse : Prouver que les deux valeurs trouvées précédemment conviennent.
   Aide : Pour prouver que $d_1d_2 = d$, on pourra procéder par double divisibilité.

IV] Les nombres premiers

1. Bien connaître le théorème de décomposition en produit de facteurs premiers (existence ET unicité).
2. Savoir exprimer les valeurs du PGCD et du PPCM à l'aide des décompositions en facteurs premiers.
3. Savoir exprimer les diviseurs d'un nombre à l'aide de la décomposition en facteurs premiers du nombre.
4. Savoir retrouver les formules donnant le nombre, la somme et le produit des diviseurs d'un nombre.
5. Savoir caractériser le fait que deux nombres sont premiers entre eux à l'aide de leur décomposition en facteurs premiers.
6. Bien connaître le petit théorème de Fermat.
7. Savoir prouver qu'un nombre est premier.
8. Se souvenir qu'il existe une infinité de nombres premiers.

Exercice de TD : 23

(∗) Montrer que pour tout $n \in \mathbb{Z}$, $N(n) = n^4 - n^2 + 16$ n'est pas premier.
Vous tenterez d'identifier dans $N(n)$ des termes provenant du développement d'un produit remarquable

Exercice de TD : 24

(∗) Déterminer les nombres premiers p tels que $p^2 + 2$ soit lui-même premier.
On pourra chercher p modulo 3.

Exercice de TD : 25

(∗) Soit $s,\ d,\ x \in \mathbb{N}$. Prouver que si $sd = x^2$ alors $s = S^2$ et $d = D^2$ avec $S,\ D \in \mathbb{N}$.
On pourra utiliser les décompositions en facteurs premiers de s, d et x.

Exercice de TD : 26

(♡) Soit $n \in \mathbb{N}$. Montrer que $\sqrt{n} \in \mathbb{Q} \Longleftrightarrow \exists m \in \mathbb{N}$ tel que $n = m^2$.
En déduire que $\sqrt{2} \notin \mathbb{Q}$ et $\sqrt{3} \notin \mathbb{Q}$.

Exercice de TD : 27

(∗∗) **Les nombres de Fermat**

1. Soit $k \in \mathbb{N}^*$.
   Montrer que si $2^k + 1$ est premier, alors k est une puissance de 2.
   Aide : on pourra exprimer k sous la forme $k = 2^n(2a + 1)$ et prouver que $a = 0$.
   Les nombres $F_n = 2^{2^n} + 1$ sont appelés les nombres de Fermat. Il ne sont pas tous premiers ... (C/ex : F_5)
2. Soient $n,\ p \in \mathbb{N}$ tels que $p < n$.
   Montrer que $F_n \equiv 2\ [F_p]$ puis en déduire que deux nombres de Fermat distincts sont premiers entre eux

Exercice de TD : 28

(♡♡♡) Pour tout entier $n \geq 2$, montrer que $v_p(n!) = \sum_{k=1}^{q} \lfloor \frac{n}{p^k} \rfloor$ avec $q = \lfloor \frac{\ln n}{\ln p} \rfloor$.

Aide : On pourra commencer par vérifier la formule $\lfloor \frac{\lfloor px \rfloor}{p} \rfloor = \lfloor x \rfloor$ pour tout $x \in \mathbb{R}$ et $p \in \mathbb{N}^*$

Exercice de TD : 29

(∗ ∗ ∗) **Olympiades iranniennes de mathématique**
Trouver les entiers naturels tous non nuls n, a, b et c tels que : $2^n = a! + b! + c!$

Exercice de TD : 30

(∗) **Un crible géométrique.**
Soit $\mathcal{P}$ la parabole d'équation $y = x^2$.
Pour $n \geq 2$ on note $M_n(n,\ n^2)$ et $M'_n(-n,\ n^2)$ les points de la paraboles d'abscisse entière différentes de 0 et ± 1.
En étudiant les points d'intersection de O_y avec les segments de la forme $[M'_m M_n]$, déterminer une méthode géométrique pour déterminer l'ensemble des 100 premiers nombres premiers.

Cette méthode a été proposée par Yuri Matiyasevich.