L'arithmétique dans $\mathbb{Z}$.

1 Divise : Définition et propriétés.

Définition 1. Vocabulaire : Diviseur et Multiple

> Soit $a, b \in \mathbb{N}$ ou $\mathbb{Z}$.

On dit que a divise b, noté $a|b$ *ou* a divise b, Ssi

Il existe $k \in \mathbb{Z}$ tel que $b = a.k$

on dit alors que a est un diviseur de b et que b est un multiple de a.

> Soit $a \in \mathbb{Z}$.

Il est facile de voir que l'ensemble des multiples de a est égale à

$$\{0, a, -a, 2a, -2a, ...\} = \{ka \text{ avec } k \in \mathbb{Z}\}.$$

On note cet ensemble $a\mathbb{Z}$.

> Soit $a \in \mathbb{Z}$.

L'ensemble des diviseurs de a est un ensemble fini.

Je note $div(a)$ l'ensemble des diviseurs de a et $div_+(a)$ l'ensemble des diviseurs positifs de a, mais il n'y a pas de notation officielle.

`Remarque : ` n `divise` $a \iff |n|$ `divise` $|a|$.
`Donc on peut souvent supposer` $a, n \in \mathbb{N}$ `sans perte de généralité.`

Exemples

> $div_+(6) = \{1, 2, 3, \cancel{4}, \cancel{5}, 6\} = \{1, 2, 3, 6\}$ et $div(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$

> $div_+(41) = \{1, \cancel{2}, \cancel{3}, \cancel{4}, ..., \cancel{40}, 41\} = \{1, 41\}$ et $div(41) = \{\pm 1, \pm 41\}$

Théorème 2. Propriétés de la relation divise.

Soit $(a,b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}$.

> Bon sens.

a divise $b \implies |a| \leqslant |b|$.

> Transitivité.

$$\left.\begin{array}{c} a \text{ divise } b \\ \text{et} \\ b \text{ divise } c \end{array}\right\} \implies a \text{ divise } c$$

> Anti-Symétrie.

$$\left.\begin{array}{c} a \text{ divise } b \\ \text{et} \\ b \text{ divise } a \end{array}\right\} \implies a = b \text{ ou a=-b}$$

La propriété la plus importante de l'arithmétique.

$$\left.\begin{array}{c} p \text{ divise } a \\ \text{et} \\ p \text{ divise } b \end{array}\right\} \implies p \text{ divise les CL } ka + k'b$$

Démonstration : Anti-Symétrie se démontre facilement avec du bon sens.

Théorème 3. Propriétés de div_+, l'ensemble des diviseurs *positifs*.

Soit $n \in \mathbb{N}$. On sait que : $div_+(n) \overset{def}{=} \{$ L'ensemble des diviseurs *positifs* de $n \}$

Ainsi $n \in div(a) \iff n$ divise a.

On a

> $div_+(1) = \{1\}$ et $div_+(0) = \mathbb{N}$

Situation générale : $div_+(n) = \{ 1, \underbrace{\ldots\ldots\ldots}_{\text{intermédiaires}}, n \}$

> **Bonus** : Lorsque $n = ab$ alors on a $1 \leqslant \underbrace{a}_{\text{petit}} \leqslant \sqrt{n} \leqslant \underbrace{b}_{\text{Grand}} \leqslant n$

Ainsi Bonus : $div_+(n) = \{ 1, .., a, .., \sqrt{n}, .., b, .., n \}$

> **Bonusnus** : Le premier diviseur > 1 de n, est premier.

Ainsi Bonusnus : $div_+(n) = \{ 1, p, \ldots., n \}$

Application/Conséquence 1 : Lorsque $\div_+(n) = \{1, n\}$ alors .....

Application/Conséquence 2 : Tous les entiers $n \geqslant 2$ admette .....

Application/Conséquence 3 : Si n n'a pas de diviseur premier alors $n =$ ...

Démonstration : On va démontrer $div_+(1) = \{1\}$

Soit $n \in div_+(1)$

On va montrer que : $n = \pm 1$.

Comme $n \in div_+(1)$, on a n divise 1.

De plus on sait aussi que 1 divise n

Par anti-symétrie, on a $n = 1$ ou $n = -1$.

2 Congruence.

Définition 4.
Soit $a, a' \in \mathbb{Z}$ et $n \in \mathbb{N}$

On dit que $a \equiv a' \, mod[n]$ Ssi il existe $k \in \mathbb{Z}$ tel que $a = a' + kn$

Théorème 5. Formulaire, Division euclidienne

> **Formulaire.** Soit $a, a', b, b', c, c' \in \mathbb{Z}$, truc $\in \mathbb{N}$ et $n \in \mathbb{N}$. On a

$$\left.\begin{array}{c} a \equiv a' \, mod[n] \\ \text{et} \\ b \equiv b' \, mod[n] \end{array}\right\} \Longrightarrow \begin{array}{l} (a+b) \equiv \left(a'+b'\right) mod[n] \\ (ab) \equiv \left(a'b'\right) mod[n] \\ a^{truc} \equiv \left(a'\right)^{truc} mod[n] \end{array}$$

> **Utile.** Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$.

$\rightarrowtail a = b\,q + r \iff a \equiv r \; mod[b]$

$\rightarrowtail n$ divise $a \iff a \equiv 0 \; mod[n] \iff \underbrace{a \,\%\, n = 0}_{python}$

En python, on a $q = a//b$ et $r = a\,\%\,b$.

> **Division euclidienne.** Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$.

Il existe un unique couple d'entiers (q, r) tel que : $a = bq + r$ et $0 \leqslant r < b$

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

Théorème 6. le petit théorème de Fermat
Soit p un nombre premier et $a \in \{1, 2, ..., p-1\}$

On a alors $a^{p-1} \equiv 1 \; mod[b]$

Démonstration : La démonstration en sup se fait par récurrence sur a.
elle utilise des propriétés des nombres premiers (voir thm 18 page 11) ainsi que le théorème de Gauss sur la divisibilité (thm 12 page 7).
On la fera en fin de cours

3 PGCD et Algorithme d'Euclide.

3.1 PGCD.

Théorème 7. Définition et propriétés des pgcd-ppcm.

Définition Soit $a, b \in \mathbb{N}$.

$$pgcd(a,b) \overset{def}{=} \text{le Plus Grand Commun Diviseur,}$$
$$ppcm(a,b) \overset{def}{=} \text{le Plus Petit Commun Multiple}$$

Notation : $pgcd(a,b)$ est aussi noté $a \wedge b$
$ppcm(a,b)$ est aussi noté $a \vee b$.

Kulture : $pgcd(a,1) = 1$ et $pgcd(a,0) = a$.

> Propriétés de $d = pgcd(a,b)$.

> d est un entier $\geqslant 1$.

> d divise a et d divise b.

> **Bézout.** d est une CL entre a et b
CàD il existe $u, v \in \mathbb{Z}$ tel que $a.u + b.v = d$
Les entiers u, v sont appelés des coefficients de Bézout.

> L'algorithme d'Euclide is great.

> Pour calculer le ppcm, on utilise la formule : $pgcd(a,b) \times ppcm(a,b) = ab$.

Démonstration :

Propriétés de $d = pgcd(a,b)$.

Les première propriétés sont une conséquence de la définition.
L'algorithme de d'Euclide justifie l'existence du pgcd, permet son calcul et démontre Bézout

Démonstration de $pgcd(a,1) = 1$ et $pgcd(a,0) = a$.

On sait que :

> $div_+(1) = \{1\}$ CàD le seul diviseur positif de 1, c'est 1.

> $div_+(0) = \{0, 1, 2, ..., 2020, ...\} = \mathbb{N}$, CàD tout le monde divise 0.

On va montrer $pgcd(a,1) = 1$

On note $d = pgcd(a,1)$.
Donc par définition du pgcd, d divise 1 et d est positif donc $d = 1$

On va montrer $pgcd(a,0) = 0$

On note $d = pgcd(a,0)$.
Par définition du pgcd, d divise a
donc le bon sens me dit que $d \leqslant a$
De plus a divise a et 0 donc a est un diviseur commun et d est le plus grand
donc on a $a \leqslant d$
Conclusion : $d = a$

3.2 L'algorithme d'Euclide.

L'algorithme d'Euclide permet

> de calculer le pgcd.
> de déterminer des coefficients de Bézout (et constitue une démonstration de Bézout)

Théorème 8. Lemme d'Euclide.

Soit a, b, q, r des entiers avec $a = b.q + r$

Alors on a $pgcd(a,b) = pgcd(b,r)$

Démonstration : On note $d = pgcd(a,b)$ et $d' = pgcd(b,r)$

On va montrer d divise d'

On sait que

$$\left.\begin{array}{l} d \text{ divise } a \\ d \text{ divise } b \end{array}\right\} \Longrightarrow d \text{ divise les CL de a et b}$$

Or r est une CL car $a = bq + r \Longrightarrow r = a - bq$ donc d divise r

$$\left.\begin{array}{l} d \text{ divise } b \\ d \text{ divise } r \end{array}\right\} \Longrightarrow d \text{ divise les CL b et de r } k\,a + k'\,b$$

Or $d' = pgcd(b,r)$ donc d'après Bezout est une CL de b et de r

Conclusion : d divise d'

On va montrer d' divise d C'est la même chose.

Remarque : La démonstration proposée est utilise "Bézout" qui se démontre avec l'algorithme d'Euclide qui utilise ce lemme. Bof, Bof, Bof!!!!

Voici maintenant l'algorithme d'Euclide théorique et donc bien plus abstrait que l'exemple fait en classe.

On suppose que $0 < b \leqslant a$.

> On fait la division euclidienne de a par b
ainsi on obtient $a = bq_1 + r_1$ et $0 \leqslant r_1 \leqslant b - 1$,

Avec le théorème précédent, on a $pgcd\,(a,b) = pgcd\,(b,r_1)$

Si $r_1 = 0$ *ou* 1, c'est fini car $pgcd(b,1) = 1$ et $pgcd(b,0) = b$

> Lorsque $r_1 \geqslant 2$, on recommence avec la division euclidienne de b par r_1
ainsi on obtient $b = r_1 q_2 + r_2$ et $0 \leqslant r_2 \leqslant r_1 - 1$,

on a alors $pgcd\,(b,r_1) = pgcd\,(r_1,r_2)$

Si $r_2 = 0$ *ou* 1 c'est fini

> lorsque $r_2 \geqslant 2$, on recommence avec la division euclidienne de r_1 par r_2

Comme la suite des restes $r_1, r_2, r_3, \ldots$ est une suite d'entier (positif) strictement décroissante,
donc elle termine à 0,

Conclusion : $r_N = 0$, $pgcd\,(a,b) = pgcd\,(r_1,r_2) = \ldots. = pgcd\,(r_{N-1},0) = r_{N-1}$
Donc $d = r_{N-1}$ le dernier reste non nul

De plus à l'aide de ces calcul, on peut calculer les coefficient de Bezout.

3.3 Factorisation du pgcd

Théorème 9. Factorisation du pgcd

Soit $a,b,k \in \mathbb{N}$, on a alors $pgcd(ka,kb) = k\,pgcd(a,b)$

Application : On note $d = a \wedge b = pgcd(a,b)$. Alors on peut factoriser le pgcd,
CàD on $a = d\,a'$, $b = d\,b'$ et $pgcd(a',b') = 1$.

Démonstration : La démonstration de $pgcd(ka,kb) = k\,pgcd(a,b)$ n'est pas évidente
car on a $k.div_+(a,b) \subset div_+(ka,kb)$ mais $\supset$ est fausse!!
Je note $D = pgcd(ka,kb)$ *et* $d = pgcd(a,b)$

On va démontrer que D divise $k.d$ et $k.d$ divise D.

$k.d$ divise D ?

Comme $D = pgcd(ka,kb)$, on sait avec Bézout que $D = (ka)... + (kb)...$ et

$$\left.\begin{array}{l} d = pgcd(a,b)\ divise\ a \Longrightarrow kd\ divise\ ka \\ d = pgcd(a,b)\ divise\ b \Longrightarrow kd\ divise\ kb \end{array}\right\} \Longrightarrow kd\ divise\ ...ka + ...kb = D$$

D divise $k.d$?

Comme $d = pgcd(a,b)$, on sait avec Bézout que $d = au + bv$ ainsi on a $kd = (ka)u + (kb)v$

$$\left.\begin{array}{l} D = pgcd(ka,kb)\ divise\ ka \\ D = pgcd(ka,kb)\ divise\ kb \end{array}\right\} \Longrightarrow D\ divise\ u(ka) + v(kb) = kd$$

Démon de l'application. Comme $d = pgcd(a,b)$, on sait (voir propriétés évidentes des pgcd) que d divise a et que d divise b, ainsi on peut écrire

$$a = d\,a' \quad et \quad b = d\,b'$$

Je note $pgcd(a',b') = d'$. Montrons que : $= d' = 1$.

En effet, si d' divise a' et b' alors le produit $(d\,d')$ divise a et b MAIS $d = pgcd(a,b)$ donc d est le plus grand diviseur commun $\Longrightarrow$ $d' = 1$.
Conclusion : le seul diviseur de a' et b', c'est 1 donc $pgcd(a',b') = 1$.

Théorème 10. Fraction irréductible.

Soit $r \in \mathbb{Q}^*$.
Alors il existe un unique couple $a_0, b_0 \in \mathbb{N}^*$ tel que

$$r = \pm\frac{a_0}{b_0} \text{ avec } a_0 \wedge b_0 = 1$$

On dit que c'est la forme irréductible de r.

Démonstration : On fait l'existence et l'unicité.

> L'existence est "facile", il suffit de factoriser le pgcd
Comme $r \in \mathbb{Q}^*$, on peut écrire $r = \pm\frac{a}{b}$. Je note $d = pgcd(a,b)$,
on a alors $a = da'$, $b = db'$ et $pgcd(a',b') = 1$

$$\text{Ainsi on a } r = \pm\frac{a}{b} = \pm\frac{da'}{db'} = \pm\frac{a'}{b'} \ et \text{ on a } a' \wedge b' = 1$$

> L'unicité. On suppose que a,b et a',b' sont deux couples dans $\mathbb{N}^*$ qui vérifient les conditions de la forme irréductible
On a $r = \frac{a}{b} = \frac{a'}{b'} \Longrightarrow ab' = ba'$
Avec le théorème de Gauss, on obtient

$$\left.\begin{array}{l} [a \text{ divise } ba' \ et\ a \wedge b = 1] \overset{Gauss}{\Longrightarrow} a \text{ divise } a' \\ [a' \text{ divise } ab' \ et\ a' \wedge b' = 1] \overset{Gauss}{\Longrightarrow} a' \text{ divise } a \end{array}\right\} \Longrightarrow a = a'\ ou\ a = -a'$$

Comme a et a'sont dans $\mathbb{N}^*$ on a bien $a = a' \neq 0$ puis on a $b = b'$.

4 Premiers entre eux, Gauss, ...

Définition 11.

Soit $a, b \in \mathbb{N}$. On dit que : a et b sont premier entre eux

Ssi le seul diviseur commun positif, c'est 1.

On a donc

a et b sont premier entre eux

$$\text{Ssi } \underbrace{a \wedge b = pgcd(a,b) = 1}_{\text{Notation classique}} \text{ Ssi } \underbrace{div_+(a,b) = \{1, ..., \underbrace{1}_{pgcd}\} = \{1\}}_{\text{Signification}}$$

Théorème 12.

a et b sont premier entre eux ?

On suppose que n est un diviseur commun de a et b ainsi

$$\left.\begin{array}{l} n \text{ divise } a \\ n \text{ divise } b \end{array}\right\} \Longrightarrow \begin{array}{l} \text{alors } n \text{ divise les CL,....Ainsi } n = 1 \\ \text{Ainsi } n = 1 \text{ est le seul diviseur premier commun de } a \text{ et } b \end{array}$$

$$\text{Conclusion : } pgcd(a,b) = 1.$$

Bézout

a et b sont premier entre eux

$$\Longleftrightarrow pgcd(a,b) = 1 \Longleftrightarrow \text{Il existe } u, v \in \mathbb{Z} \text{ tel que } au + bv = 1$$

Théorème de Gauss.

$$\left.\begin{array}{l} a \text{ divise } bc \\ a, b \text{ sont premier entre eux} \end{array}\right\} \Longrightarrow a \text{ divise } c$$

Produit et pgcd.

$$\left.\begin{array}{l} a \text{ divise } n \\ b \text{ divise } n \\ a, b \text{ sont premier entre eux} \end{array}\right\} \Longrightarrow ab \text{ divise } n$$

Produit et premier.

Si a et b sont premiers avec n alors ab est premier avec n.

Démonstration :

Démonstration de Gauss

Comme a est premier avec b, on a $pgcd(a,b) = 1$ et avec Bezout on sait qu'il existe $u, v \in \mathbb{Z}$ tel que $a.u + b.v = 1$

On multiplie l'égalité par c ainsi $ca.u + cb.v = c$

$$\left.\begin{array}{l} a \text{ divise } bc \\ a \text{ divise } ac \end{array}\right\} \Longrightarrow a \text{ divise la CL } ac.u + bc.v = c$$

Démonstration de Produit et premier.

Comme a divise n, on a $n = an'$

De plus avec Gauss, on a

$$\left.\begin{array}{l} b \text{ divise } n = an' \\ a, b \text{ sont premier entre eux} \end{array}\right\} \Longrightarrow b \text{ divise } n'$$

Conclusion : on a $n = an' = abn''$.

5 ppcm.

5.1 La théorie du ppcm.

La théorie des pgcd, c'est la théorie des diviseurs.
La théorie des ppcm, c'est la théorie des multiples.

Définition 13. Multiple, Multiple commun

> Soit $a, b \in \mathbb{N}$. On dit que a divise b, aussi noté $a|b$ Ssi

Il existe $k \in \mathbb{Z}$ tel que $b = a.k$

On dit alors que b est un multiple de a.

> Soit $a \in \mathbb{N}$.

$$\begin{aligned} mul_+(a) &\overset{def}{=} \{\text{L'ensemble des multiples positifs de } a\} \\ &= \{0, a, 2a, 3a, ...\} \\ &= \{ka \text{ avec } k \in \mathbb{N}\}. \end{aligned}$$

On a donc $mul_+(a) = a\mathbb{N}$.

> Soit $a, b \in \mathbb{N}$.

$$\begin{aligned} mul_+(a,b) &\overset{def}{=} \{\text{L'ensemble des multiples positifs communs de } a \text{ et } b\} \\ &= \{0, ..., ab, ...\} \end{aligned}$$

Attention : ab est un multiple commun de a et de b donc $ab \in mul_+(a,b)$
mais à priori ce n'est le plus petit!!!
Par exemple lorsque $a = 4$ et $b = 6$,
on a $ab = 24$ et $mul_+(4,6) = \{0, 12, 24, 36, ...\}$.

Théorème 14. Définition et propriétés du ppcm

Soit $a, b \in \mathbb{Z}$.

$ppcm(a,b) \overset{def}{=}$ le Plus Petit Commun Multiple, CàD
Lorsque $mul_+(a,b) = \{0, m, ..., ab..., \}$, alors $ppcm(a,b) = m$.

Notation importante : $ppcm(a,b)$ est aussi noté $a \vee b$.

Propriétés de $m = ppcm(a,b)$.

> m est un entier et $1 \leqslant m \leqslant ab$.

> m est un multiple de a et m est un multiple de b.

> ~~Bézout~~. Bézout n'existe pas pour le ppcm.

> ~~Euclide~~. Il n'y a pas d'algorithme d'Euclide pour le ppcm.

5.2 Lien entre pgcd et ppcm.

Théorème 15. Lien entre ppcm et pgcd

Soit $a, b \in \mathbb{N}^*$.

> Lorsque $a \wedge b = 1$ alors $ppcm(a,b) = ab$.

> Plus généralement, on a $ppcm(a,b).pgcd(a,b) = ab$

Grâce à ce résultat, on peut calculer $ppcm(a,b)$.

Démonstration : On suppose que $a \wedge b = 1$ et je note $m = ppcm(a,b)$. On va montrer que $m = ab$

$\Longrightarrow$ On sait que $mul_+(a,b) = \{0, m, ..., ab, ...\}$
Donc $m \leqslant ab$.

$\Longrightarrow$ Comme $m = ppcm(a,b)$ donc m est un multiple a ET m est un multiple b
On utilise le théorème classique de l'arithmétique "produit et pgcd", ainsi on a

$$[a \text{ et } b \text{ divisent } m \text{ et } a \wedge b = 1] \Longrightarrow \begin{array}{l} ab \text{ divise } m \\ \text{Donc } ab \leqslant m \end{array}$$

Conclusion : $m = ab$.

Démonstration : La situation générale.

On utilise la factorisation du pgcd et les formules autour de pgcd et ppcm

$$\begin{aligned} ppcm(a,b).pgcd(a,b) &= ppcm(da', db').pgcd(da', db') \\ &= d^2\, ppcm(a', b').pgcd(a', b') \\ &\text{Comme } a' \wedge b' = 1 \text{ on a } pgcd(a', b') = 1 \text{ et } ppcm(a', b') = a'b' \\ &= d^2 (a'.b').1 = (da')(db') = ab \text{ Fini.} \end{aligned}$$

6 Premiers et premier entre eux.

6.1 Les nombres premiers.

Définition 16. Nombre premier et nombre composée.

> On dit que p est entier premier

Ssi $p \geqslant 2$ et $div_+(p) = \{1, \cancel{2}, \cancel{3}, \cancel{4}, ..., \cancel{p-1}, p\} = \{1, p\}$

L'ensemble des nombres premiers est noté $\mathscr{P}$.

et on a $\mathscr{P} = \{2,3,5,7,11,13,17,19,....,41,....,641,...,2017,....\}$.

> On dit que $n \geqslant 2$ est un entier composé Ssi n n'est pas premier.

n est composé $\iff$ *n admet des diviseurs intermédiaires*
$\iff$ *On peut écrire* $n = a.b$ avec $2 \leqslant a \leqslant b \leqslant n-1$

Théorème 17.

> Lorsque n n'a aucun petit diviseur entre 2 et $\sqrt{n}$

alors n est premier.

> Il y a une infinité de nombre premier,

CàD le cardinal de $\mathscr{P}$ est infini.

Démonstration : On fait un RA. On suppose que l'ensemble $\mathscr{P}$ contint exactement N éléments, ainsi on a

$$\mathscr{P} = \{2,3,5,7,..,41,...641,...,2017,....,p_N\}$$

Je considère le nombre $A = (\textit{Le produit de tous les nombres premier}) + 1$

> D'une part : Comme $A \in \mathbb{N}$ et $A \geqslant 2$ donc A admet une factorisation. Je note p un de ses facteurs.
Donc : Comme p divise $A \implies A \equiv 0 \mod [p]$

> D'autre part : $A = 2.3.5.7...41...p...641...2017...p_N + 1 = p.K + 1$
Donc $A \equiv 1 \mod [p]$ OUPS!!!

Le crible d'Eratosthène.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

6.2 Propriétés des nombres premiers

Théorème 18. Propriétés spécifiques des nombres premiers.

$$\left.\begin{array}{c} a \in \mathbb{N} \\ p \text{ premier} \end{array}\right\} \Longrightarrow \text{Soit } p \text{ divise } a, \quad \text{Soit } p \text{ est premier avec } a.$$

$$\left.\begin{array}{c} p \text{ divise } ab \\ p \text{ premier} \end{array}\right\} \Longrightarrow p \text{ divise } a \quad \text{ou} \quad p \text{ divise } b.$$

$$\left.\begin{array}{c} p \text{ ne divise pas } a \\ p \text{ ne divise pas } b \\ p \text{ premier} \end{array}\right\} \Longrightarrow p \text{ ne divise pas } ab.$$

Attention *: Si on remplace p premier par n un nombre les implications sont fausses.*

Démonstration : La démonstration est "visuelle".

Comme p divise ab donc p est dans la factorisation de ab.

De plus la factorisation de ab est obtenue à partir de celle de a et de celle de b

Donc p est dans la factorisation de a ou dans celle de b.

Théorème 19. Factorisation des entiers.

Soit $n \in \mathbb{Z}$

L'entier n se factorise en produit de nombre premier

et cette factorisation est unique.

Application. Combien $n = 84 = 2^2.3.7$ admet de diviseurs positifs ?

a divise $n = 84 = 2^2.3.7$ alors a est de la forme $a = 2^{\alpha}.3^{\beta}.7^{\gamma}$

On peut avoir $\underbrace{\alpha = 0,1 \, ou \, 2}_{\text{3 possibilités}}$ et $\underbrace{\beta = 0 \, ou \, 1}_{\text{2 possibilités}}$ et $\underbrace{\gamma = 0 \, ou \, 1}_{\text{2 possibilités}}$

Conclusion :

l'entier $n = 84 = 2^2.3.7$ admet $(3)(2)(2) = 12$ diviseurs positifs distincts

Démonstration : **Existence d'une factorisation.**. On démontre l'existence d'une factorisation *avec une récurrence forte.*

On va démontrer $H_{<n>}$: l'entier n admet une factorisation en produit de facteur premier.

Initialisation.

$H_{<2>}$ est vraie

Hérédité. On suppose que $H_{<2>}, H_{<3>}, ..., H_{<n>}$ sont vraies

On va montrer $H_{<n+1>}$

- Soit $n+1$ est un nombre premier et c'est fini.

- Soit $n+1$ est composée et on peu écrire $n+1 = ab$ avec $2 \leqslant a \leqslant \sqrt{n} \leqslant b \leqslant n-1$.

On applique $H_{<a>}$ et $H_{<b>}$, ainsi $a = p_1...p_k$ et $b = q_1...q_l$

ainsi $n+1 = p_1...p_k \, q_1...q_l$ Fini.

Démonstration : **Unicité de la factorisation.**

6.3 Valuation.

Définition 20. Valuation

On considère $n = \prod_{p\in\mathscr{P}} p^{\alpha_p}$ un entier écrit sous forme factorisé.

L'entier $\alpha_p \in \mathbb{N}$ s'appelle la valuation de p dans le nombre n, il est noté $v_p(n)$.

Conclusion : on peut écrire $n = \prod_{p\in\mathscr{P}} p^{v_p(n)}$.

Remarque : Cette écriture est faussement infini, CàD $v_p(n) = 0$ pour presque tput les p.

Théorème 21.

Comme la factorisation est unique, on a

$$2016 = 2^5.3^2.7 = 2^5.3^2.5^0.7^1.11^0.... = \prod_{p\in\mathscr{P}} p^{v_p(2016)} \Longrightarrow \begin{cases} v_2(2016) = 5 \\ v_3(2016) = 2 \\ v_5(2016) = 0 \\ v_7(2016) = 1 \\ \\ Si\ p \neq 2,3,7\ alors\ v_p(2016) = 0 \end{cases}$$

Exemples : Comme $12 = 2^2.3$, on a $v_2(12) = 2,\ v_3(12) = 1$ et $v_5(12) = 0$

Comme $360 = 2^3 3^2 5$, on a $v_2(360) = 3,\ v_3(360) = 2$ et $v_5(360) = 1$

Théorème 22. Propriétés de la valuation

Soit $a, b \in \mathbb{N}$ et $p \in \mathscr{P}$ un nombre premier.

> On a : p divise $a \iff v_p(a) \geqslant 1$

p ne divise pas $a \iff v_p(a) = 0$

> On a : a divise $b \iff \forall p \in \mathscr{P},\ v_p(a) \leqslant v_p(b)$

> On a $a^2 = \left(\prod_{p\in\mathscr{P}} p^{v_p(a)}\right)^2 = \left(\prod_{p\in\mathscr{P}} p^{2v_p(a)}\right)$

Donc à cause de l'unicité : $\forall p \in \mathscr{P},\ v_p\left(a^2\right) = 2v_p(a) = pair$

Avec la même démarche, on obtient $v_p(ab) = v_p(a) + v_p(b)$

> a et b sont premiers entre eux

Ssi a et b n'ont pas de facteur commun (en dehors de 1)

Ssi a et b n'ont pas de facteur *premier* commun

Ssi pour tout $p \in \mathscr{P}$: Soit $v_p(a) \geqslant 1$ et $v_p(b) = 0$ CàD p est facteur de a et pas de b

Soit $v_p(a) = 0$ et $v_p(b) \geqslant 1$ CàD p est facteur de b et pas de a

Soit $v_p(a) = 0$ et $v_p(b) = 0$ CàD p n' est ni facteur de a et ni facteur de b

Applications : `Avec la valuation, on peut montrer les résultats classiques suivants`

> Si a^2 divise b^2, Alors a divise b.

Comme a^2 divise b^2, alors pour tout $p \in \mathscr{P}$, $2v_p(a) = v_p(a^2) \leqslant v_p(b^2) = 2v_p(b)$

Conclusion : pour tout $p \in \mathscr{P}$, $v_p(a) \leqslant v_p(b)$, ainsi a divise b.

> Si $ab = c^2$ et a et b sont premiers entre eux, Alors a est un carré et b est un carré

Si $v_p(a) \geqslant 1$ alors $v_p(b) = 0$ et $v_p(a) = v_p(c^2) = 2v_p(c)$ est pair

ainsi pour tout $p \in \mathscr{P}$, $v_p(a) = 0$ ou $v_p(a) = 2v_p(c)$

Conclusion : pour tout $p \in \mathscr{P}$, $v_p(a)$ est pair donc a est un carré.

7 Exercices

Autour de Divise.

Exercice 1. [Correction] Soit $n \in \mathbb{N}^*$. Déterminer les diviseur commun positif

> entre n et $n+1$

> entre n et $2n+1$

> entre n^2+n et $2n+1$

> entre $3n^2+2n$ et $n+1$

Exercice 2. [Correction]

1. Déterminer les entiers relatifs n tels que $n-4$ divise $3n-17$.
2. Montrer par récurrence que, pour tout $n \in \mathbb{N}$, 11 divise $\left(9^{5n+2}-4\right)$

Exercice 3. [Correction] En utilisant le binôme, montrer que n^2 divise dans $(1+n)^n-1$.

Exercice 4. Résoudre l'équation $n^2-3n+6 \equiv 0 \ mod[5]$

Exercice 5. En utilisant le petit théorème de Fermat, déterminer

le reste de la division euclidienne de 1234^{4321} par 7

puis le reste de la division euclidienne de $1234^{4321}+4321^{1234}$ par 7

Exercice 6. [Correction]

1. Déterminer les diviseurs de 127.
2. Montrer que $(x-y)$ se factorise dans x^3-y^3 et finir la factorisation.
3. Déterminer tous les couples $(x,y) \in \mathbb{N}^2$ tel que $x^3-y^3=127$.

PGCD, Bézout, Gauss et Équation diophantienne.

Exercice 7. Déterminer le pgcd et un couple de Bézout des couples d'entiers (a,b) suivants :

$a=33$ et $b=24$ $\qquad$ $a=37$ et $b=27$ $\qquad$ $a=270$ et $b=105$

Exercice 8. Résoudre, dans $\mathbb{Z}$, les équations suivantes

$$2x+5y=1 \text{ puis } 2x+5y=3$$

Exercice 9. On va résoudre dans $\mathbb{Z}$ l'équation : $-156x+276y=48 \quad (E)$

Soit (x,y) une solution.

1. Calculer $pgcd(156,276)$.

   En déduire que l'équation (E) est équivalent à $-13x+23y=4 \quad (E')$.

2. Avec Bézout, déterminer une solution particulière (x_0,y_0) de l'équation E'.
3. Démontrer que 23 divise $(x-x_0)$.
4. Résoudre l'équation (E).
5. Parmi les solutions lesquelles sont dans $\mathbb{N}$

Exercice 10. Exo oral CCP

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux et $c \in \mathbb{N}$.
   Prouver que : $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.
3. On considère le système (S) : $\left\{ \begin{array}{rcll} x & \equiv & 6 & [17] \\ x & \equiv & 4 & [15] \end{array} \right.$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.
   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Exercice 11. Théorème des restes chinois.

1. Soient n, m, c trois entiers tels que $pgcd(n,m) = 1$.
   Résoudre l'équation $nx \equiv c\,[m]$.
2. Soient n, m, a, b quatre entiers tels que $pgcd(n,m) = 1$.
   Résoudre les systèmes $\left\{ \begin{array}{l} x \equiv 1\,[n] \\ x \equiv 0\,[m] \end{array} \right.$, puis $\left\{ \begin{array}{l} x \equiv 0\,[n] \\ x \equiv 1\,[m] \end{array} \right.$ et enfin $\left\{ \begin{array}{l} x \equiv a\,[n] \\ x \equiv b\,[m] \end{array} \right.$
3. Application 1.
   Un phare émet un signal jaune toutes les 15 secondes et un signal rouge toutes les 28 secondes. On aperçoit le signal jaune 2 secondes après minuit et le rouge 8 secondes après minuit.
   À quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ’
4. Application 2.
   Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur.
   Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors quatre pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés et le partage laisserait cinq pièces d'or à ce dernier.
   Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ’

Nombre premier entre eux, gauss et application.

Exercice 12. [Correction]

1. Montrer que pour tout $n \in \mathbb{N}$, les nombres $n+1$ et $2n+1$ sont premiers entre eux.
2. Exprimer $\binom{2n+1}{n+1}$ en fonction $\binom{2n}{n}$.
3. En déduire que ; $(n+1)$ divise $\binom{2n}{n}$.

Exercice 13. [Correction] On va démontrer un résultat sur le triangle de Pascal.

1. Écrire le triangle de Pascal jusqu'à la ligne n°7.
   Je vous donne la ligne 11 : 1, 11, 55, 165, 330, 462, 462, 330, 165, 55, 11, 1.
   On constate que lorsque p est premier,
   alors "tous" les coefficients de la ligne p du triangle sont divisibles par p.
2. On va démontrer ce résultat.
   (a) Exprimer $\binom{p}{k}$ en fonction $\binom{p-1}{k-1}$.
   (b) Classique En déduire, avec Gauss, que : lorsque p est premier alors $\forall\ k \in \{1,2,..,(p-1)\}$, p *divise* $\binom{p}{k}$.

Exercice 14. On considère le polynôme $P(X) = 3X^3 + 5x^2 + 8x + 2$.
On suppose que $r = p/q$ est une racine rationnelle de P écrite sous forme irréductible.

1. Que signifie que la fraction p/q est irréductible.
2. Comme r est une racine, on sait que $P(r) = 0$. En déduire que p divise 2.
3. Déterminer les valeurs possibles de q puis de r.
4. Est ce que le polynôme $P(X)$ a des racines rationnelles.

Autour des nombres premiers.

Exercice 15. [Correction] **Les nombres de Mersenne.**
Soit $\in \mathbb{N}$. On considère le nombre $M_n = 2^n - 1$

1. On suppose que n est composée, ainsi on peut écrire $n = ab$ avec $2 \leqslant a \leqslant \sqrt{n} \leqslant b$.

   Montrer que : $M_n \equiv 0 \mod [M_a]$

   Indication : $2^a - 1 = M_a \equiv 0 \mod [M_a] \Longrightarrow 2^a \equiv 1 \mod [M_a]$

   `Interprétation : le nombre` M_a `divise` M_n `donc le nombre` M_n `est composée.`

   Conclusion : Lorsque le nombre n est composée,
   Alors le nombre M_n est composée

2. En déduire que : Si M_n est premier alors n est premier.

   `Remarque : la réciproque est fausse car` $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$. `est un nombre composé.`

Exercice 16. [Correction] **Les nombres de Fermat.**
Soit $\in \mathbb{N}$. On considère le nombre $f_n = 2^n + 1$

1. On suppose que $n = a\,b$ avec b un nombre impair

   Montrer que : $f_n \equiv 0 \mod [f_a]$

   En déduire que : Si f_n est un nombre premier alors n n'a pas de diviseur impair donc $n = 2^\alpha$

   Les nombres $F_n = 2^{2^n} + 1$ sont appelés les nombres de Fermat.

2. la réciproque est fausse. On va montrer que $F_5 = 2^{2^5} + 1 = 2^{32} + 1 \equiv 0 \mod [641]$

   En remarquant que $641 = 2^7.5 + 1$, montrer que : $F_5 \equiv 0 \mod [641]$.

   `On a la factorisation :` $F_5 = 4294967297 = 641 \times 6700417$.

Exercice 17. [Correction] Forcément plus dur **Deux résultats sur les nombres premiers.**
Les deux questions sont indépendantes.

1. On sait qu'il y a une infinité de nombre premier, donc il y a une infinité de nombre premier impair,
   CàD dire de la forme $4k+1$ ou $4k+3$.

   Relire la démonstration de "il existe une infinité de nombre premier".
   En suivant la même démarche, monter qu'il existe une infinité de nombre premier de la forme $4k+3$.

2. Soit $n \in \mathbb{N}$. On note p_n le n-ième nombre premier (ainsi $p_1 = 2$, $p_2 = 3$, $p_5 = 11$).
   (a) Relire la démonstration de "il existe une infinité de nombre premier".
   En déduire que $p_{n+1} \leqslant p_1.p_2...p_n + 1$.
   (b) En déduire que $p_n \leqslant 2^{2^n}$.

Divers.

Exercice 18. Difficile **Un résultat dû à Lagrange.**

1. On considère $n!$. Réfléchir et voir que la multiplicité de 2 dans $n!$ est toujours $>$ que celle de 5.
   En déduire que le nombre de zéro à la fin de $n!$ est égale à la multiplicité de 5 dans $n!$.
2. Montrer que le nombre de zéro à la fin de $n!$ est égale à $\left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \left\lfloor \frac{n}{5^3} \right\rfloor + \cdots$

Exercice 19. Soit a, b des nombres premiers entre eux.

1. Pour tout $k \in \mathbb{N}^*$, on note r_k le reste de la division euclidienne de a^k par b.
   Justifier qu'il existe deux entiers distincts k, k' tel que $r_k = r_{k'}$
2. En déduire qu'il existe $n \in \mathbb{N}^*$ tel que $a^n \equiv 1 \mod [b]$.

Exercice 20. Un résultat original Pour $n \in \mathbb{N}$, on note $u_n = \underbrace{11...1}_{n \text{ chiffres}}$

1. Pour tout $k \in \mathbb{N}$, on note r_k le reste de la division euclidienne de u_k par 23.
   Justifier qu'il existe deux entiers distincts $k > k'$ tel que $r_k = r_{k'}$
2. Simplifier $u_k - u'_k$. En déduire que $u_{k-k'} \equiv 0 \mod [23]$
   Conclusion : On a trouver un nombre de la forme 11...1 divisible par 23.
3. Peut-on remplacer 23 par un autre entier '

Exercice 21. Un exercice qui utilise le petit théorème de Fermat.

Soit $n \in \mathbb{N}$ et $A_n = n^2 + n + 1$.

1. On suppose que p est un diviseur premier de p et que $p > 3$
   (a) Montrer que : $n \not\equiv 1 \mod [p]$ puis que $n^2 \not\equiv 1 \mod [p]$.
   (b) Montrer que : $n^3 \equiv 1 \mod [p]$.
   (c) En utilisant le petit théorème de Fermat, montrer que $p \equiv 1 \mod [3]$.
2. Montrer qu'il existe une infinité de nombre premier congrus à 1 modulo 3.

Correction.

Solution de l'exercice 1 (Énoncé) On utilise le théorème le plus important de l'arithmétique

> Déterminer les diviseur commun positif entre n et $(n+1)$

Soit a un diviseur positif de n et $n+1$

$$\left.\begin{array}{r} a \text{ divise } n \\ a \text{ divise } n+1 \end{array}\right\} \Longrightarrow a \text{ divise } (-1)\times n+(1)(n+1)=1$$

Conclusion a divise 1 donc $a=1$

> Déterminer les diviseur commun positif entre (n^2+n) et $(2n+1)$

Soit a un diviseur positif de (n^2+n) et $(2n+1)$

$$\left.\begin{array}{r} a \text{ divise } n^2+n \\ a \text{ divise } 2n+1 \end{array}\right\} \Longrightarrow a \text{ divise } (2)\times(n^2+n)+(-1)(2n+1)=2n-1$$

On re-commence

$$\left.\begin{array}{r} a \text{ divise } 2n+1 \\ a \text{ divise } 2n-1 \end{array}\right\} \Longrightarrow a \text{ divise } (1)\times(2n+1)+(-1)(2n-1)=2$$

On re-re-commence

$$\left.\begin{array}{r} a \text{ divise } 2 \\ a \text{ divise } 2n21 \end{array}\right\} \Longrightarrow a \text{ divise } (-n)\times(2)+(1)(2n+1)=1$$

Conclusion a divise 1 donc $a=1$

Solution de l'exercice 2 (Énoncé)

1. Déterminer les entiers relatifs n tels que $n-4$ divise $3n-17$.

On a

$$\left.\begin{array}{r} n-4 \text{ divise } n-4 \\ n-4 \text{ divise } 3n-17 \end{array}\right\} \Longrightarrow n-4 \text{ divise } (1)\times(3n-14)+(-3)(n-4)=-2$$

Donc $n-4$ est un diviseur de -2

De plus on sait que : $div(-2)=div(2)=\{\pm1,\pm2\}=\{1,2,-1,-2\}$

Conclusion il y a 4 possibilités : $n-4=1$, $n-4=2$, $n-4=-1$, $n-4=-2$

2. Montrer par récurrence que, pour tout $n\in\mathbb{N}$, 11 divise $\left(9^{5n+2}-4\right)$

On fait par récurrence $H_{<n>}$: 11 divise $\left(9^{5n+2}-4\right)$

> Initialisation $n=0$

Comme $9^{5.0+2}-4=9^2-4=81-4=77$, $H_{<0>}$ est vrai

> Hérédité. On suppose $H_{<n>}$

On va montrer $H_{<n+1>}$, CàD 11 divise $\left(9^{5(n+1)+2}-4\right)$

On cherche le lien entre $9^{5(n+1)+2}-4$ et $9^{5n+2}-4$ puis on applique $H_{<n>}$

$$\begin{aligned} 9^{5(n+1)+2}-4 &= 9^5.9^{5n+2}-4 \\ &= 9^5.\left(9^{5n+2}-4\right)+4.9^5-4 \\ &= 9^5.\left(9^{5n+2}-4\right)+4.\left(9^5-1\right) \\ &= 9^5.\left(9^{5n+2}-4\right)+4.59048 \\ &= 9^5.\left(9^{5n+2}-4\right)+4.11.5368 \end{aligned}$$

On applique $H_{<n>}$

$$= 9^5.11\times k+4.11.5368=11\times\left(9^5.k+4.5368\right)$$

Donc $H_{<n+1>}$ est vraie.

Autre solution avec le congruence

On sait que : $9^{5n+2}-4=\left(9^5\right)^n.9^2-4$

De plus $9^2=81=4+77\equiv 4 \mod[11]$ et $9^5=9^2.9^2.9\equiv 4.4.(-2) \mod[11]$

$$\equiv 16.(-2) \mod[11]$$
$$\equiv 5.(-2) \mod[11]$$
$$\equiv (-10) \mod[11]$$
$$\equiv 1 \mod[11]$$

Ainsi $9^{5n+2}-4\equiv\left[(1)^n.4-4\right] \mod[11]$

$$\equiv 0 \mod[11]$$

Conclusion : 11 divise $\left(9^{5n+2}-4\right)$

Solution de l'exercice 3 (Énoncé) En utilisant le binôme, montrer que n^2 divise dans $(1+n)^n-1$.

On a

$$\begin{aligned}(1+n)^n-1 &= \left[\sum_{k=0}^{n}\binom{n}{k}n^k\right]-1\\ &= \sum_{k=1}^{n}\binom{n}{k}n^k \qquad \text{car } \underbrace{1}_{k=0}\\ &= \underbrace{\binom{n}{1}\times n}_{k=1}+\underbrace{\sum_{k=2}^{n}\binom{n}{k}n^k}_{\text{Ici } k\geqslant 2 \text{ donc } n^2 \text{ se factorise.}}\\ &= n^2+n^2\left(\sum_{k=2}^{n}\binom{n}{k}n^{k-2}\right)\\ &= n^2\times Entier\end{aligned}$$

Conclusion : n^2 divise dans $(1+n)^n-1$.

Solution de l'exercice 6 (Énoncé)

1. Déterminer les diviseurs de 127.

   Les petits diviseurs sont à chercher parmi : $1,2,3,4,5,6,7,8,9,10,11$ car $11<\sqrt{127}<12$

   On obtient que $div_+(127)=\{1,127\}$ CàD 127 est premier et $div(127)=\{1,127,-1,-127\}$

2. Montrer que $(x-y)$ se factorise dans x^3-y^3 et finir la factorisation.

   On a : $x^3-y^3=(x-y)\left[x^2+xy+y^2\right]$

3. Déterminer tous les couples $(x,y)\in\mathbb{N}^2$ tel que $x^3-y^3=127$.

   On a : $x^3-y^3=127 \iff (x-y)\left[x^2+xy+y^2\right]=127$

   ainsi $(x-y)$ est un diviseur de 127

   Il y a 4 situations à examiner

   $$\begin{aligned}&x-y=1 \text{ et } x^2+xy+y^2=127\\ &x-y=127 \text{ et } x^2+xy+y^2=1\\ &x-y=-1 \text{ et } x^2+xy+y^2=-127\\ &x-y=-127 \text{ et } x^2+xy+y^2=-1\end{aligned}$$

   > Comme $x^2+xy+y^2=X^2+Xy+y^2$ est toujours positifs (Car $\Delta\leqslant 0$),
   les situations $x^2+xy+y^2=-127$ et $x^2+xy+y^2=-1$ n'ont pas de solution.

   > La situation $x-y=1$ et $x^2+xy+y^2=127$ se fait par substitution, CàD $x=y+1$ puis

   $$\begin{aligned}x^2+xy+y^2=127 \text{ devient } (y+1)^2+(y+1)y+y^2=127 &\iff 3y^2+3y+1=127\\ &\iff y^2+y=42\\ &\iff y=6 \text{ ou } y=-7\end{aligned}$$

   Ainsi $y=6$ car $y\in\mathbb{N}$ puis $x=y+1=7$.

   > La situation $x-y=127$ et $x^2+xy+y^2=1$ se fait aussi substitution
   Et on trouve qu'il n'y a pas de solution dans $\mathbb{N}$

   Conclusion : l'unique solution est $x=7$ et $y=6$. Pour info : $7^3-6^3=343-216=127$

Solution de l'exercice 12 (Énoncé)

1. Voir exo 18
2. On a $\binom{2n+1}{n+1}=\frac{(2n+1)!}{n!(n+1)!}=\frac{2n+1}{n+1}\binom{2n}{n}$.

3. On a $(n+1)\binom{2n+1}{n+1} = (2n+1)\binom{2n}{n}$

$$\left.\begin{array}{l}(n+1) \text{ divise } (2n+1)\binom{2n}{n} \\ n \text{ est premier avec } (2n+1)\end{array}\right\} \overset{Thm\ Gauss}{\Longrightarrow\Longrightarrow\Longrightarrow} (n+1) \text{ divise } \binom{2n}{n}$$

Solution de l'exercice 13 (Énoncé)

1. Facile
2. Classique.
   (a) On a $\binom{p}{k} = \cdots = \frac{p}{k}\binom{p-1}{k-1}$.
   (b) On a $k\binom{p}{k} = p\binom{n-1}{k-1}$
   Comme $k \in \{1,2,..,(p-1)\}$ et que p est premier DONC p est premier avec k, ainsi

$$\left.\begin{array}{l}p \text{ divise } k\binom{p}{k} \\ p \text{ est premier avec } k\end{array}\right\} \overset{Thm\ Gauss}{\Longrightarrow\Longrightarrow\Longrightarrow} p \text{ divise } \binom{p}{k}$$

3. Démonstration du petit théorème de Fermat. : Soit p un nombre premier.
   (a) pour tout $a, b \in \mathbb{N}$, on a

$$\begin{aligned}(a+b)^p &= \text{Binôme} \\ &= \sum_{k=0}^{p}\binom{n}{k}a^k b^{p-k} \\ &= \underbrace{b^p}_{k=0} + \underbrace{\binom{p}{1}a\,b^{p-1}}_{k=1} + \cdots + \underbrace{\binom{p}{p-1}a^{p-1}\,b}_{k=p-1} + \underbrace{a^p}_{k=p} \\ &\quad Or\ \binom{p}{1} = \binom{p}{2} \cdots = \binom{p}{p-1} \equiv 0 \mod [p] \\ &\equiv (a^p + 0 + 0 \cdots + 0 + b^p) \mod [p]\end{aligned}$$

   (b) Facile par récurrence.

Solution de l'exercice 15 (Énoncé)

1. On sait que : $2^a - 1 = M_a \equiv 0 \mod [M_a]$ ainsi $2^a \equiv 1 \mod [M_a]$, d'où le calcul

$$\begin{aligned}2^a &\equiv 1 \mod [M_a] \\ &\Longrightarrow \left(2^a\right)^b \equiv 1^b \mod [M_a] \\ &\Longrightarrow 2^{ab} \equiv 1 \mod [M_a] \\ &\Longrightarrow \underbrace{2^{ab} - 1}_{=M_n} \equiv 0 \mod [M_a] \\ &\quad \textit{Conclusion : } M_n \equiv 0 \mod [M_a]\end{aligned}$$

   Comme n est composée, on a $2 \leqslant a \leqslant \sqrt{n} \leqslant b$
   Ainsi $M_a = 2^a - 1 \geqslant 2^2 - 1 = 3$ Donc M_a est bien un diviseur "intermédiaire" de M_n,
   Donc M_n est composée.
2. Par contraposée, Si M_n est premier alors n est premier.

Solution de l'exercice 16 (Énoncé)

1. On sait que : $2^a+1=f_a\equiv 0 \mod [f_a]$ ainsi $2^a\equiv(-1) \mod [f_a]$, d'où le calcul

$$\begin{aligned}
&2^a\equiv(-1) \mod [f_a]\\
&\Longrightarrow \left(2^a\right)^b\equiv(-1)^b \mod [f_a]\\
&\quad \textit{Or } b \textit{ est impair et } (-1)^{impair}=(-1)\\
&\Longrightarrow 2^{ab}\equiv(-1) \mod [f_a]\\
&\Longrightarrow \underbrace{2^{ab}+1}_{=f_n}\equiv 0 \mod [f_a]\\
&\quad \textit{Conclusion : } f_n\equiv 0 \mod [f_a]
\end{aligned}$$

   Si $b\neq 1$ alors $3\leqslant f_a<f_n$, donc f_a est bien un diviseur "intermédiaire" de f_n,
   alors f_n est composée.

   Par contraposée : Si f_n est premier alors n n'a pas de diviseur impair
   Ainsi dans sa factorisation en facteur premier, il n'y a pas de facteur premier impair
   Ainsi $n=2^\alpha$.

2. Comme $641=2^7.5+1$, on a

$$\begin{aligned}
&5.2^7\equiv -1 \mod [641]\\
&\Longrightarrow \left(5.2^7\right)^4\equiv(-1)^4 \mod [641]\\
&\Longrightarrow \underbrace{625}_{\equiv -16 \mod [641]}.2^{28}\equiv 1 \mod [641]\\
&\Longrightarrow -\underbrace{16}_{=2^4}.2^{28}\equiv 1 \mod [641]\\
&\Longrightarrow -2^{32}\equiv 1 \mod [641]\\
&\Longrightarrow \underbrace{2^{32}+1}_{=F_5}\equiv 0 \mod [641]
\end{aligned}$$

   Conclusion : 641 divise F_5 Donc F_5 n'est pas premier ! ! ! !

Solution de l'exercice 17 (Énoncé)

1. On fait un RA.
   On suppose qu'il y a un nombre fini, noté $p_1,\ldots,p_N$ de nombre premier de la forme $4k+3$ et on considère $A=4(p_1....p_N)+3$.
   On va calculer $A \mod [4]$.

   $>$ D'une part : $A=4(p_1....p_N)+3\equiv 3 \mod [4]$.

   $>$ D'autre part : A admet une factorisation en produit de nombre premier MAIS aucun de p_i de la forme $4k+3$ ne divise A

   Donc $A=q_1...q_\alpha$ avec q_i de la forme $4k+1$

   On a donc $A=q_1...q_\alpha=\overline{q_1}\cdots\overline{q_\alpha} \mod [4]=1.1...1 \mod [4]=1$

2. Soit $n\in\mathbb{N}$. On note p_n le n-ième nombre premier (ainsi $p_1=2,\ p_2=3,\ p_5=11$).
   (a) RA
   On suppose que $p_{n+1}>p_1.p_2...p_n+1$.

   On cherche OUPS

   Le nombre $A=p_1.p_2...p_n+1$ conduit a une absurdité.

   $>$ Comme $A\equiv 1 \mod [p_k]$ donc A n'est divisible par aucun des $p_1,p_2,...,p_n$.

   $>$ Et p_{n+1} et les autres nombres premier sont $>A$.

   Donc A n'est divisible par aucun facteur premier. OUPS ! ! ! !

   (b) Récurrence forte.