Index

3 page 50 Combien de nombres premiers

Combien de nombres premiers ?

1. Étude d 'exemples

a) $2\times3\times5 + 1 = 31$ qui est premier.

31 n'est pas dans la liste initiale.

b) $2\times3\times5\times7 + 1 = 211$ qui est premier.

31 n'est pas dans la liste initiale.

$2\times5\times37 + 1 = 371$. Les diviseurs premiers sont 7 et 53.

7 et 53 ne sont pas dans la liste initiale.

Dans les trois cas, les nombres premiers trouvés ne font pas partie de la liste initiale.

Autrement dit, il semble que si on a une liste de nombres premeirs, on peut construire trouver au moins un nombre premier supplémentaire.

2. On se donne une liste de nombres premiers : p_1 , p_2 , …, p_r

On pose N = $p_1p_2\ldots p_r$ + 1 (produits des nombres premiers de la liste + 1)

1er cas : N est premier

N ne peut pas être dans la liste précédente

puisque N est strictement supérieur à chacun des entiers p_i pour un entier i tel que $1 \leqslant i \leqslant r$.

2ième cas :

N n'est pas premier, il existe donc un entier premier p qui divise N.

Montrons que p n'est pas dans la liste des p_1 , p_2 , …, p_r

Raisonnement par l'absurde.

Supposons que p est dans la liste p_1 , p_2 , …, p_r alors p divise le produit P = $p_1p_2\ldots p_r$

Comme p divise N, p divise la différence N – P = 1

En conséquence, $p = 1$ ce qui est contradictoire avec p premier.

Dans les deux cas, on a trouvé un nombre premier qui n'est pas dans la liste initiale.

Commentaires sur le texte d'Euclide :
les nombres sont représentés par unsegment.
Le mot " mesuré " correspond à " divisible ".
Dans l'antiquité, les nombres étaient des objets géométriques (longueurs) et dire qu'un nombre EF est mesuré par un autre nombre G signifie qu'on peut donner la proportion $\frac{EF}{G}$ (cf . commensurable)

Exemple : 371 est mesuré par 7
(On a 53 fois la longueur 7 dans la longueur 371)

Problème 4 page 62

Les nombres de Mersenne s'écrivent sous la forme $M_n = 2^n - 1$, $n \in \mathbb{N}$.

Partie A : Exploration

1) Étude des nombres pour n de 0 à 20

	n	Mn	Statut	
1	n	Mn	Statut	
2	0	0	non premier	
3	1	1	non premier	
4	2	3	premier	
5	3	7	premier	
6	4	15	non premier	15=5*3
7	5	31	premier	
8	6	63	non premier	63=3*3*7
9	7	127	premier	
10	8	255	non premier	255=3*5*17
11	9	511	non premier	
12	10	1023	non premier	1023 = 3 * 11 * 31
13	11	2047	non premier	2047 = 23 * 89
14	12	4095	non premier	4095 = 3 * 3 * 5 * 7 * 13
15	13	8191	premier	
16	14	16383	non premier	16383 = 3 * 43 * 127
17	15	32767	non premier	32767 = 7 * 31 * 151
18	16	65535	non premier	65535 = 3 * 5 * 17 * 257
19	17	131071	premier	
20	18	262143	non premier	262143 = 3 * 3 * 3 * 7 * 19 * 73
21	19	524287	premier	
22	20	1048575	non premier	1048575 = 3 * 5 * 5 * 11 * 31 * 41

Quand n est composé alors M_n est composé

Quand n est premier alors M_n peut être premier ou non premier (11 est premier, M_{11} n'est pas premier).

(Voir aussi la partie C où sont étudiés M_{19} et M_{23}).

2) Si $a = 1$, l'égalité $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + 1)$ est vérifiée (les deux membres sont nuls).

si $a \neq 1$, considérons la suite géométrique de premier terme 1 et de raison a.

La somme des n premiers termes est : $1 + ... + a^{n-1} = \frac{a^n - 1}{a-1}$, ce qui prouve l'égalité proposée :

$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + 1)$

Soit n un entier composé : $n = pq$ avec p et q entiers strictement supérieurs à 1.

$2^n = (2^p)^q$

Appliquons l'égalité précédente avec $a = 2^p$ et $n = q$.

$(2^p)^q - 1 = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + ... + 1)$

Comme $p > 1$, $2^p - 1 > 1$

Le nombre $2^n - 1$ est donc composé si n est composé.

3) Supposons que $2^n - 1$ admette un diviseur premier d.

On a alors : $2^n - 1 \equiv 0$ (modulo d) , soit : $2^n \equiv 1$ (d).

Partie B : Nombres de Mersenne lorsque *p* est premier.

p est premier.

$M_p = 2^p - 1$ est divisible par un nombre premier d.

Soit M_p est premier et il est divisible par lui-même. ($d = M_p$)

Soit M_p n'est pas premier, et alors il existe un diviseur d de M_p qui est premier.

***d* est nécessairement impair** puisque $2^p - 1$ est impair.

On a donc : $d \geqslant 3$ et d premier.

I est l'ensemble des entiers naturels n non nuls tels $2^n \equiv 1$ (d)

$I = \{n / n \in \mathbb{N}^* \text{ et } 2^n \equiv 1 (d)\}$

1) $2^p - 1$ est divisible par d. d'où, $2^p - 1 \equiv 0$ (d), soit : $2^p \equiv 1$ (d).

$p \in I$, donc, p est non vide.

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément : appelons p_0 cet élément.

$0 \notin I$ par définition de I.

$1 \notin I$ car $2 \equiv 1$ est faux quelque soit $d \geqslant 3$.

Conséquence : $p_0 \geqslant 2$.

2) $n = p_0 \times q + r$ avec $0 \leqslant r < p_0$. (Division euclidienne de n par p_0).

$2^n = 2^{p_0 q + r} = (2^{p_0})^q \times 2^r$

Or, $n \in I$, donc, $2^n \equiv 1$ (d)

$p_0 \in I$ donc $2^{p_0} \equiv 1$ (d), puis : $(2^{p_0})^q \equiv 1$ (d).

On obtient : $2^n \equiv 2^r$ (d), soit : $2^r \equiv 1$ (d) et $0 \leqslant r < p_0$

Comme r est strictement inférieur au plus petit élément non nul de I, nécessairement $r = 0$.

Conclusion : $n = p_0 \times q$ Si $n \in I$ alors est un multiple de p_0 .

Comme $p \in I$, p est un multiple de p_0 , mais, comme p est premier, on a : $p = p_0$.

3) Énoncé du petit théorème de Fermat : Si p est premier et si a n'est pas divisible par p alors $a^p \equiv a$ (p)

ou encore $a^{p-1} \equiv 1$ (p)

Si d est premier alors $2^{d-1} \equiv 1$ (d).

D'après ce théorème, $d - 1 \in I$.

$d - 1 = p \times q + r$ avec $0 \leqslant r < p$. (Division euclidienne de $d - 1$ par p).

$2^{d-1} = 2^{pq+r} = (2^p)^q \times 2^r$

Or, $2^{d-1} \equiv 1$ (d)

$2^p \equiv 1$ (d), puis : $(2^p)^q \equiv 1$ (d).

On obtient : $2^{d-1} \equiv 2^r$ (d), soit : $2^r \equiv 1$ (d) et $0 \leqslant r < p$

Comme r est strictement inférieur au plus petit élément non nul de I, nécessairement $r = 0$.

Conclusion : $d - 1 = p \times q$

Or, on sait que d est impair, c'est-à-dire que $d - 1$ est pair, d'où, $d - 1 = p \times 2k$ où $k \in \mathbb{N}$.

$d = 2kp + 1$

Partie C : Deux nombres de Mersenne M_{19} et M_{23} .

1) L'entier $M_{19} = 2^{19} - 1 = 524\,287$

Comme 19 est un nombre premier, le résultat du B.3. s'applique et les diviseurs d de M_{19} sont de la forme $2 \times 19k + 1 = 38k + 1$ avec $k \in \mathbb{N}$. (Pour l'étude qui suit k est non nul).

a) il suffit de chercher les entiers naturels d inférieurs à $\sqrt{M_{19}}$.

Comme $\sqrt{M_{19}} \approx 724{,}07$, on cherche k entier naturel non nul tel que $38k + 1 \leqslant 724$, soit : $k \leqslant \frac{723}{38}$.

Comme $\frac{723}{38} \approx 19{,}02$, on étudie les diviseurs $d = 38k + 1$ avec k entier de 1 à 19.

b) Si $k = 3m + 1$ alors $d = 38(3m + 1) + 1 = 3(38m + 13)$ d est composé.

Si $k = 5m + 3$ alors $d = 38(5m + 3) + 1 = 5(38m + 23)$ d est composé.

Si $k = 7m + 2$ alors $d = 38(7m + 2) + 1 = 7(38m + 11)$ d est composé.

(Remarques sur ces nombres :

On peut ajouter $k = 13m + 1$, car, $38 \times 1 + 1 = 39$ est un multiple de 13

$k = 11m + 2$, car, $38 \times 2 + 1 = 77$ est un multiple de 11

On cherche des nombres de la forme $38 \times a + 1$ non premiers ... $a = 1$ donne $39 = 3 \times 13$ $q = 3$ ou $q = 13$

a = 2 donne 77 = 7×11 *q = 7 ou q = 11*

a = 3 donne 115 = 5×23 *q = 5 ou q = 23*

les nombres de la forme 38(qm + a) + 1 sont factorisables par q)

c) Finalement :

k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
$3m+1$	x			x			x			x			x			x			x
$5m+3$			x					x					x					x	
$7m+2$		x							x							x			

Il reste à étudier les diviseurs 38×5 + 1 = 191, 38×6 + 1 = 229 ; 38×11 + 1 = 419 ; 38×12 + 1 = 457,

38×14 + 1 = 533 = 13×41 n'est pas premier, 38×15 + 1 = 571,

38×17 + 1 = 647

M_{19} n'est divisible par aucun de ces sept nombres : il est premier.

2) L'entier $M_{23} = 2^{23} - 1 = 8\,388\,607$

Comme 23 est un nombre premier, le résultat du B.3. s'applique et les diviseurs *d* de M_{23} sont de la forme $2\times23k + 1 = 46k + 1$ avec $k \in \mathbb{N}$.

En testant la division de M_{23} par 47, on obtient : 8 388 607 = 47×178 481

M_{23} n'est pas un nombre premier.

Partie D : Le test de Lucas-Lehmer

S est la suite définie par $\begin{cases} S_0 = 4 \\ S_i = S_{i-1}^2 - 2 \quad \text{pour} \quad i \geqslant 1 \end{cases}$

1) Proposition : " Tous les termes de *S* sont divisibles par 2 "

Par récurrence :

Le premier terme S_0 est divisible par 2.

Supposons un entier *k* tel que S_k divisible par 2. Le carré de S_k est divisible par 2, et par conséquent, le suivant $S_{k+1} = S_k^2 - 2$ est divisible par 2

L'axiome de récurrence permet de conclure :

tous les termes de la suite *S* sont divisibles par 2.

2) *p* est un entier premier.

R_i est le reste de la division euclidienne de S_i par M_p, c'est-à-dire : $S_i \equiv R_i \ (M_p)$ et $0 \leqslant R_1 < M_p$.

a) En appliquant les propriétés des congruences, on a : $S_i^2 \equiv R_i^2 \ (M_p)$, puis, $S_i^2 - 2 \equiv R_i^2 - 2 \ (M_p)$

D'où, $S_{i+1} \equiv R_i^2 - 2 \ (M_p)$. Or, $S_{i+1} \equiv R_{i+1} \ (M_p)$ par définition de la suite *R*.

Par transitivité des congruences : $R_{i+1} \equiv R_i^2 - 2 \ (M_p)$

b) Tableur :

	A	B	C	D	E	F	G	H
1	p (premier)	3	5	7	11	13	17	19
2	M_p	7	31	127	2047	8191	131071	524287
3								
4	i	R_i	R_i	R_i	R_i	R_i	R_i	R_i
5	0	4	4	4	4	4	4	4
6	1	0	14	14	14	14	14	14
7	2	5	8	67	194	194	194	194
8	3	2	0	42	788	4870	37634	37634
9	4	2	29	111	701	3953	95799	218767
10	5	2	2	0	119	5970	119121	510066
11	6	2	2	125	1877	1857	66179	386344
12	7	2	2	2	240	36	53645	323156
13	8	2	2	2	282	1294	122218	218526
14	9	2	2	2	1736	3470	126220	504140
15	10	2	2	2	510	128	70490	103469
16	11	2	2	2	129	0	69559	417706
17	12	2	2	2	263	8189	99585	307417
18	13	2	2	2	1616	2	78221	382989
19	14	2	2	2	1529	2	130559	275842
20	15	2	2	2	165	2	0	85226
21	16	2	2	2	612	2	131069	523263
22	17	2	2	2	1988	2	2	0
23	18	2	2	2	1432	2	2	524285
24	19	2	2	2	1575	2	2	2
25	20	2	2	2	1706	2	2	2
26	21	2	2	2	1647	2	2	2
27	22	2	2	2	332	2	2	2
28	23	2	2	2	1731	2	2	2
29	24	2	2	2	1598	2	2	2
30	25	2	2	2	993	2	2	2
31	26	2	2	2	1440	2	2	2
32	27	2	2	2	2034	2	2	2
33	28	2	2	2	167	2	2	2
34	29	2	2	2	1276	2	2	2
35	30	2	2	2	809	2	2	2

c) Pour $p = 11$, aucun reste n'est nul, et, on a vu au A.1. que M_{11} n'est pas premier.

d) Il semble que $R_i = 0$ lorsque $i = p - 2$ pour tous les autres p premiers de 3 à 19.

On pose $r = p - 2$

On a vu au A.1. que les nombres de Mersenne correspondants étaient des nombres premiers.

e) À partir du rang p (c-à-d : $r + 2$), il semble que les restes sont égaux à 2.

f) Si, pour r, S_r est un multiple de $2^p - 1 = M_p$ alors $S_r \equiv 0\ (M_p)$

Or, $S_r \equiv R_r\ (M_p)$ R_r

d'où, $R_{r+1} \equiv S_{r+1} \equiv 0^2 - 2 \equiv (-2)\ (M_p)$ (par définition de la suite S)

puis, $R_{r+2} \equiv S_{r+2} \equiv (-2)^2 - 2 \equiv 2\ (M_p)$ (par définition de la suite S)

Si à partir d'un certain rang k, $R_k \equiv 2\ (M_p)$, tous les restes suivants sont congrus à 2, puisque $2^2 - 2 = 2$.

3) Propriété de Lucas-Lehmer :

Si, pour p premier supérieur ou égal à 3, $S_{p-2} \equiv 0\ (M_p)$, alors, M_p est un nombre premier.

a) L'algorithme lié à cette propriété va donc calculer le reste de rang $p - 2$ (c'est le nombre r du D.2)

Saisir p (//p est un nombre premier supérieur ou égal à 3)

s ← 4 ; M ← $2^p - 1$ //le premier reste est 4 ; M est le nombre de Mersenne associé à *p*.

Pour *k* de 1 jusqu'à *p* – 2 faire : //on instaure une boucle pour calculer

s ← reste dans la division euclidienne de $s^2 - 2$ par M //les restes définis par une relation de

Fin Pour //récurrence : $R_{i+1} \equiv R_i^2 - 2$ (modulo M)

Si s = 0 alors Afficher " M est un nombre premier

sinon Afficher " M n'est pas un nombre premier "

Fin Si

c) Les capacités de certains logiciels limitent leur exploitation

Syntaxe pour Algobox (vite dépassé : les résultats sont approchés et faux pour p = 107, 607)

```
VARIABLES
  p EST_DU_TYPE NOMBRE
  M EST_DU_TYPE NOMBRE
  s EST_DU_TYPE NOMBRE
  k EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
  AFFICHER "Entrer un nombre premier >= 3"
  LIRE p
  M PREND_LA_VALEUR pow(2,p)-1
  s PREND_LA_VALEUR 4
  POUR k ALLANT_DE 1 A p-2
    DEBUT_POUR
    s PREND_LA_VALEUR (pow(s,2)-2)%M
    FIN_POUR
  SI (s==0) ALORS
    DEBUT_SI
    AFFICHER "Lenombre de Mersenne M"
    AFFICHER p
    AFFICHER "  est un nombre premier"
    FIN_SI
    SINON
      DEBUT_SINON
      AFFICHER "Lenombre de Mersenne M"
      AFFICHER p
      AFFICHER "  n'est pas un nombre premier"
      FIN_SINON
FIN_ALGORITHME
```

Syntaxe pour Xcas

```
1 Prog Edit Ajouter
saisir(p);
s:=4;M:=2^p-1;
pour k de 1 jusque p-2 faire
s:=irem(s^2-2,M);
fpour;
si s==0 alors afficher ("Mp est premier");
sinon afficher("Mp n'est pas premier");
fsi:;
```

Syntaxe pour Scilab

```
1 p=input("p premier =")
2 s=4;M=2^p-1
3 for k=1:(p-2)
4     s=reste(s^2-2,M)
5 end
6 if s==0 then afficher("Mp premier")
7 else afficher("Mp non premier")
8 end
```

Syntaxe pour TI (vite dépassé : les résultats sont approchés et faux pour p = 107 et dépasse les capacités pour 607)

```
PROGRAM:MERSENNE
:Prompt P
:4→S
:2^P-1→M
:For(K,1,P-2)
:S²-2→D
:iPart(D/M)→Q
:D-M*Q→S
:End
:If S=0
:Then
:Disp "M PREMIER
"
:Else
:Disp "M NON PRE
MIER"
:End
```

les nombres proposés M_{107} , M_{607} , M_{3217} sont premiers.

Copies d'écran de Xcas

```
Mp est premier
Evaluation time: 3.651
( [1, 107 ], 4, 162259276829213363391578010288127, 0, Done )
```

```
Mp est premier
Evaluation time: 2.902
[1, 607 ], 4, 531137992816767098689588206552468627329593117727031923199444138200403559860852242739162502265229285668889321
```

```
Mp est premier
Evaluation time: 11.716
[1, 3217 ], 4, 259117086013202627776246767922441530941818887553125427303974923161874019266586362086201209516800483406550
```

1 page 64

Rappels : connaître les critères de divisibilité par 2, par 3, par 5 et par 11.

2 691 Comme 2 + 6 + 9 + 1 = 18 est un multiple de 3, 2 691 est divisible par 3.

5 741 n'est divisible ni par 2, ni par 3, ni par 5, ni par 11.

$\sqrt{5741}$ a pour partie entière 75

On teste les facteurs 7, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 et 73.

5 743 n'est divisible ni par 2, ni par 3, ni par 5, ni par 11.

$\sqrt{5743}$ a pour partie entière 75

On teste les facteurs 7, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 et 73.

6 425 est divisible par 5.

8 191 n'est divisible ni par 2, ni par 3, ni par 5, ni par 11.

$\sqrt{8191}$ a pour partie entière 90

On teste les facteurs 7, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, .79, 83, 89

10 152 est pair, donc, divisible par 2

172 413 Comme 1 + 7 + 2 + 4 + 1 + 3 = 18 est un multiple de 3, 172 413 est divisible par 3.

736 747 Comme (7 + 6 + 4) – (3 + 7 + 7) = 0, 736 747 est divisible par 11.

Nombres	**2 691**	**5 741**	**5 743**	**6 425**	**8 191**	**10 152**	**172 413**	**736 747**
Premiers	Non	Oui	Oui	Non	Oui	Non	Non	non
Facteur évident	3			5		2	3	11

3 page 64 Curiosités

nombres premiers jumeaux : deux nombres premiers dont la différence est 2

Exemples : 17 ; 19 ; 5 741 ; 5743 ;

Paire de nombres premiers : Deux nombres premiers écrits avec les mêmes chiffres mais en sens inverse.

Exemples : 1 933 et 3 391

1) Si deux entiers forment une paire de nombres premiers, le chiffre des unités ne peut pas être pair et ne peut pas être 5.

Le chiffre des unités de l'un est le premier chiffre de l'autre, d'où, un entier de la paire de nombres premiers ne peut avoir pour premier chiffre que 1, 3, 7 ou 9

2) Les paires de nombres premiers à deux chiffres :

13 et 31 ; 17 et 71 ; 37 et 73 ; 79 et 97

4 page 64

a et *b* deux entiers naturels **premiers**.
(*a* et *b* sont donc supérieurs ou égaux à 2)

1) Le produit $a \times b$ n'est pas premier. Il est divisible par a et par b
Il existe au moins un diviseur propre du nombre $P = ab$.
2) La somme $a + b$ peut être un nombre premier.
exemple : $2 + 3 = 5$
Remarque : pour avoir $a + b$ premier, nécessairement, l'un des deux entiers est 2.
si a et b sont premiers et strictement supérieurs à 2 alors leur somme est paire et strictement supérieure à 2.

---

9 page 64 Nombres de Fermat

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

1) 2) 3)

n	**0**	**1**	**2**	**3**	**4**	**5**
F_n	3	5	17	257	65537	4 294 967 297
premier	Oui	Oui	Oui	Oui	Oui	NON

F_5 est divisible par 641

---

11 page 65

n est un entier naturel.

1 a) $n^2 - 6n + 5 = (n - 1)(n - 5)$

b) Si $n \geqslant 7$ alors $n - 1 \geqslant 6$ et $n - 5 \geqslant 2$.

L'entier $(n^2 - 6n + 5)$ étant le produit de deux entiers naturels supérieurs ou égaux à 2 est un entier composé (non premier).

Remarque :

Soit $P(n) = n^2 - 6n + 5$

Si $n = 0$, $P(0) = 5$ est un nombre premier

Si $n = 1$, $P(1) = 0$ n'est pas un nombre premier

Si $n = 2$, $P(2) = -3$ et $|P(2)| = 3$ est un nombre premier

Si $n = 3$, $P(3) = -4$ et $|P(3)| = 4$ n'est pas un nombre premier

Si $n = 4$, $P(4) = -5$ et $|P(4)| = 5$ est un nombre premier

Si $n = 5$, $P(5) = 0$ n'est pas un nombre premier

Si $n = 6$, $P(6) = 5$ est un nombre premier

2 a) $2n^2 - 11n + 9 = (n - 1)(2n - 9)$

Recherche d'une condition suffisante pour que $2n^2 - 11n + 9$ soit un entier composé.

$n - 1$ ET $2n - 9$ sont des entiers supérieurs ou égaux à 2 si $n \geqslant 6$

En effet : $n - 1 \geqslant 2$ si et seulement si $n \geqslant 3$

$2n - 9 \geqslant 2$ si et seulement si $n \geqslant 6$

Si $n \geqslant 6$ alors $2n^2 - 11n + 9$ est un entier composé.

Soit $Q(n) = 2n^2 - 11n + 9$

Si $n = 0$, on a : Q(0) = 9 n'est pas un nombre premier.

Si $n = 1$, Q(1) = 0 n'est pas un nombre premier.

Si $n = 2$, Q(2) = –5 n'est pas un nombre composé

Si $n = 3$, Q(3) = –6 est un entier composé.

Si $n = 4$, Q(4) = –3 n'est pas un nombre composé

Si $n = 5$, Q(5) = 4 est un entier composé.

Conclusion : L'entier $2n^2 - 11n + 9$ est toujours composé sauf pour $n = 2$ et $n = 4$.

---

12 page 65

1) Développer $(a^2 - a + 1)(a^2 + a + 1) = [(a^2 + 1) - a\,][(a^2 + 1) + a]$

$= (a^2 + 1)^2 - a^2$

$= a^4 + 2a^2 + 1 - a^2 = a^4 + a^2 + 1$

2) Le nombre $a^4 + a^2 + 1$ est donc factorisable en produit de deux facteurs : $(a^2 - a + 1)$ et $(a^2 + a + 1)$.

3) Application : $10\,101 = 10^4 + 10^2 + 1$

d'où, $10\,101 = (10^2 - 10 + 1)(10^2 + 10 + 1) = 91 \times 111$ $\quad$ $(91 = 7 \times 13$ et $111 = 3 \times 37)$

---

15 page 65

Proposition à démontrer : (implication)

Si la somme de deux nombres entiers a et b est un nombre premier, alors a et b sont premiers entre eux.

Contraposée de la proposition :

Si a et b ne sont pas premiers entre eux, alors la somme de ces deux nombres n'est pas un nombre premier.

Démonstration de la contraposée :

a et b ne sont pas premiers entre eux d'où, il existe un entier d différent de 1 qui est un diviseur commun à a et b. $\quad a = dq$ *et* $b = dq'$

d divise donc la somme $a + b$. $\quad a + b = dq + dq' = d(q + q')$.

Conclusion :

Une implication et sa contraposée étant des propositions équivalentes,
la proposition à démontrer est vraie.

---

19 page 67

Marie-Sophie Germain (1776- 1831).

Mathématicienne qui publia avec les plus grands mathématiciens de son époque en publiant les premiers travaux sous un nom d'emprunt masculin.

$n \in \mathbb{N}$, $N = n^4 + 4$.

1 a) Soit $n = 10k$ avec $k \in \mathbb{N}$.

$N = (10k)^4 + 4 = 2^4 \times 5^4 \times k^4 + 4 = 4(2^2 \times 5^4 \times k^4 + 1)$.

Comme $2^2 \times 5^4 \times k^4 + 1 \in \mathbb{N}$, N est un multiple de 4

Autre méthode :

pour montrer que N est un multiple de 4, il suffit de montrer que $N \equiv 0\ (4)$

On sait : $10 \equiv 2\ (4)$, d'où, $10^4 \equiv 2^4\ (4)$. Or, $2^4 = 16$, d'où, $10^4 \equiv 0\ (4)$.

On a alors : $10^4 .k^4 + 4 \equiv 0 \times k^4 + 0$ ..... CQFD

b) soit a, le dernier chiffre de n
On peut écrire : $n = 10^k + a$ avec $0 \leqslant a \leqslant 9$ ou encore : $n \equiv a\ [10]$ avec $0 \leqslant a \leqslant 9$
D'après les propriétés des congruences, $n^4 \equiv a^4 \equiv b\ [10]$, avec $0 \leqslant b \leqslant 9$
puis $n^4 + 4 \equiv b + 4\ [10]$, avec $0 \leqslant b \leqslant 9$
$2^4 = 16 = 1 \times 10 + 6$ $\quad 2^4 \equiv 6\ [10]$, $\quad 4^4 = (2^2)^4 = (2^4)^2$, d'où, $4^4 \equiv 6^2 \equiv 6\ [10]$
et $8^4 = (2 \times 4)^4$, d'où, $8^4 \equiv 6 \times 6 \equiv 6\ [10]$
$3^4 = 81 = 8 \times 10 + 1$ $\quad 3^4 \equiv 1\ [10]$, comme $6^4 = (2 \times 3)^4$, on a : $6^4 \equiv 6 \times 1 \equiv 6\ [10]$
et $9^4 \equiv 1 \times 1 \equiv 1\ [10]$
$5^4 = 625 = 62 \times 10 + 5$ $\quad 5^4 \equiv 5\ [10]$
$7^4 = 49 \times 49$ d'où, $7^4 \equiv 9 \times 9 \equiv 1\ [10]$

Dans ce tableau, a est le chiffre des unités de n et b celui de n^4
$b + 4$ donne le nombre d'unités de N.

a	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
b	0	1	6	1	6	5	6	1	6	1
$b + 4$	4	5	10	5	10	9	10	5	10	5

N est un multiple de 5 si et seulement si le dernier chiffre est 0 ou 5
N est un multiple de 5 si et seulement si le dernier chiffre de n est 1 ou 2 ou 3 ou 6 ou 8 ou 9.
N n'est pas un multiple de 5 si et seulement si le dernier chiffre de n est 0 ou 5.
Commentaire : (pour préparer la question d))
On a montré toutes les implications suivantes :
(Condition suffisante) implique (Condition nécessaire)
On traduit dans une recherche par : Il suffit d'avoir (CS)
il faut avoir (CN)
(I_1) : Si N n'est pas multiple de 5 alors n est un multiple de 5.
(I_2) (réciproque de (I_1)) : Si n est un multiple de 5 alors N n'est pas un multiple de 5
(I_3) (contraposée de (I_1)) : Si n n'est pas multiple de 5 alors N est un multiple de 5.
(I_4) (contraposée de (I_2) ou réciproque de (I_3)) : Si N est un multiple de 5 alors n n'est pas multiple de 5.

c) $n = 5$ $\quad N = 629 = 17 \times 37$
$n = 15$ $\quad N = 50\ 629 = 197 \times 257$
$n = 25$ $\quad N = 390\ 629 = 577 \times 677$
Ces nombres N ne sont pas premiers.

d) **Le seul cas où une implication est fausse est**
le cas où la condition nécessaire est fausse quand la condition suffisante est vraie.
Dans tous les autres cas, l'implication est vraie.
Table de vérité d'une implication :

Condition suffisante : (CS)	**Condition nécessaire : (CN)**	**Implication : (CS) ⇒ (CN)**
V	V	V
V	F	F
F	V	V
F	F	V

(1) : si n est multiple de 5 alors on ne peut pas savoir s'il est premier ou non.
(on sait que si n est multiple de 10 alors N n'est pas premier puisqu'il est divisible par 4).
(2) FAUX: si n n'est pas multiple de 5 alors N n'est pas premier puisqu'il est divisible par 5. (d 'après b/) (I_3)
(3) On ne peut pas savoir : pour que N soit premier, il faut que n ne soit pas multiple de 5
La contraposée de cette proposition commence par : Il suffit que n soit multiple de 5 ....
(il faut que) " n n'est pas multiple de 5 " est une condition nécessaire de " N est premier "
(4) FAUX : pour que N soit premier, il suffit que n ne soit pas multiple de 5
" n n'est pas multiple de 5 " est une condition nécessaire de " N est premier "
la condition" n n'est pas multiple de 5 " n'est pas suffisante.
La phrase : Si n n'est pas multiple de 5 " alors " N est premier " est fausse d'après b/

2 a) Afin de démontrer cette égalité : $n^4 + 4m^4 = (n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn)$,
on développe $(n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn) = ... = n^4 + 4m^4$
Remarquer : $(n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn) = (n^2 + 2m^2)^2 - (2mn)^2$
$= n^4 + 2\times n^2 \times 2m^2 + (2m)^2 - (2mn)^2 = n^4 + 4m^4$

b) La factorisation de $5^4 + 4$ s'obtient en faisant : $n = 5$ et $m = 1$
$n^2 + 2m^2 + 2mn = 25 + 2 + 10 = 37$
$n^2 + 2m^2 - 2mn = 25 + 2 - 10 = 17$

Celle de $15^4 + 4$ en faisant $n = 15$ et $m = 1$,
la factorisation de N pour $n = 35$ est : $35^2 + 2\times1\times1 + 2\times35\times1 = 1\,297$ par $35^2 + 2\times1\times1 - 2\times35\times1 = 1\,157$
$1157\times1297 = 1\,500\,629$
$35^4 + 4 = 1\,500\,629$

3) Les nombres de la forme $n^4 + 4$ ne sont jamais premiers.
Le 2a) prouve que $n^4 + 4\times1^4 = (n^2 + 2 + 2n)(n^2 + 2 - 2n)$

---

32 page 67

1 a) $4 = 2^2$, $9 = 3^2$, $16 = 2^4$, $25 = 5^2$, $36 = 2^2\times3^2$, $49 = 7^2$, $64 = 2^6$, $81 = 3^4$, $100 = 2^2\times5^2$.

b) les exposants sont pairs.

c) Un nombre entier est un carré parfait si et seulement si tous les exposants sont pairs.

En effet : Soit un carré parfait $A = a^2$

Soit $a = \prod_{i=1}^{i=k} p_i^{\alpha_i}$ où tous les p_i $(1 \leqslant i \leqslant k)$ sont des nombres premiers et α_i un entier indiquant le nombre de facteurs égaux à p_i dans la décomposition de a.

On a alors : $A = \left(\prod_{i=1}^{i=k} p_i^{\alpha_i}\right)^2 = \prod_{i=1}^{i=k} p_i^{2\alpha_i}$ Les exposants sont pairs.

Réciproquement : Soit une décomposition où tous les exposants des facteurs premiers sont pairs.

$\prod_{i=1}^{i=k} p_i^{2\alpha_i} = \left(\prod_{i=1}^{i=k} p_i^{\alpha_i}\right)^2$ est donc un carré parfait.

2) On pose $\sqrt{2} = \frac{a}{b}$ où a, b entiers et $b \geqslant 2$.

a) On a donc : $2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, soit : $a^2 = 2b^2$.

b) Puisque b^2 est un carré, les exposants sont des nombres pairs.

L'exposant de 2 dans la décomposition de b^2 est soit 0, soit $2n$.

L'exposant de 2 dans la décomposition de $2b^2$ est soit 1, soit $2n + 1$.

On a donc : l'exposant de 2 dans la décomposition de a^2 est impair.

c) Or, d'après 1c), l'exposant de 2 est pair dans la décomposition d'un carré parfait.

Il y a donc une contradiction due à l'hypothèse introduite au 2).

On ne peut pas poser : $\sqrt{2} = \frac{a}{b}$ où a, b entiers et $b \geqslant 2$.

$\sqrt{2}$ est un irrationnel.

---

34 page 67 Carré parfait

1) ***Propriété à démontrer :***

A est un carré parfait si et seulement si dans sa décomposition en facteurs premiers, tous les exposants sont pairs.

Sens direct :

Soit A un carré parfait.

Il existe un entier a tel que $A = a^2$.

Soit $a = \prod_{i=1}^{i=k} p_i^{\alpha_i}$ où tous les p_i $(1 \leqslant i \leqslant k)$ sont des nombres premiers et α_i un entier indiquant le nombre de facteurs égaux à p_i dans la décomposition de a.

On a alors : $A = \left(\prod_{i=1}^{i=k} p_i^{\alpha_i}\right)^2 = \prod_{i=1}^{i=k} p_i^{2\alpha_i}$ Les exposants sont pairs.

Réciproquement : Soit une décomposition où tous les exposants des facteurs premiers sont pairs.

$\prod_{i=1}^{i=k} p_i^{2\alpha_i} = \left(\prod_{i=1}^{i=k} p_i^{\alpha_i}\right)^2$ est donc un carré parfait.

2) Soit x un réel.

Si $x = a\sqrt{b}$ avec a et b entiers naturels supérieurs ou égaux à 2 alors $x^2 = a^2 b$ où b n'est pas un carré parfait.

D'après le 1), au moins un exposant dans la décomposition de x^2 est impair.

Réciproquement, si dans la décomposition en facteurs premiers de x^2, au moins un exposant est impair,

alors $x = a\sqrt{b}$.

Preuve :

$x^2 = \prod_{i=1}^{i=k} p_i^{\beta_i}$ où tous les p_i $(1 \leqslant i \leqslant k)$ sont des nombres premiers.

soit les facteurs premiers p_i $(1 \leqslant i \leqslant j$ et $j \leqslant k)$ dont les exposants sont impairs, $\beta_i = 2\alpha_i + 1$

et les facteurs premiers p_i ($j \leqslant i \leqslant k$) dont les exposants sont pairs, $\beta_i = 2\alpha_i$.

on peut écrire $x^2 = \prod_{i=1}^{i=k} p_i^{2\alpha_i} \times \prod_{i=1}^{i=j} p_i$

alors $x = a\sqrt{b}$ où $a = \prod_{i=1}^{i=k} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{i=j} p_i$.

Illustration : $x^2 = 3^7 \times 5^4 \times 11^2 \times 17^5 \times 19^8$ $\quad p_1 = 3,\ p_2 = 17\ ;\ p_3 = 5,\ p_4 = 11,\ p_5 = 19$

$\beta_1 = 7,\ \beta_2 = 5,\ \beta_3 = 4,\ \beta_4 = 2,\ \beta_5 = 8$

$\alpha_1 = 3,\ \alpha_2 = 2,\ \alpha_3 = 2,\ \alpha_4 = 1,\ \alpha_5 = 4$

$$x^2 = \prod_{i=1}^{i=5} p_i^{2\alpha_i} \times \prod_{i=1}^{i=2} p_i$$

$$a = \prod_{i=1}^{i=5} p_i^{\alpha_i} = 3^3 \times 17^2 \times 5^2 \times 11^1 \times 19^4 \text{ et } b = 3 \times 17$$

$$x = 3^3 \times 17^2 \times 5^2 \times 11^1 \times 19^4 \times \sqrt{3 \times 17}$$

a et b entiers supérieurs ou égaux à 2.
x s'écrit $a\sqrt{b}$ si et seulement si dans la décomposition en facteurs premiers de x^2 au moins un exposant est impair.

---

36 page 67

$a = 3^\alpha \times 7^\beta$ et $(\alpha + 1)(\beta + 1) = 21$

On ne peut pas avoir $\alpha + 1 = 1$ ou $\beta + 1 = 1$, car, il y a au moins un 3 et un 7 d'après le texte.

Deux cas : $\begin{cases} \alpha+1=3 \\ \beta+1=7 \end{cases}$ ou $\begin{cases} \alpha+1=7 \\ \beta+1=3 \end{cases}$.

$a = 3^2 \times 7^6$ ou $a = 3^6 \times 7^2$

---

64 page 70

1) $1000 = 3 \times 333 + 1$ d 'où $1000 \equiv 1\ (3)$

$2000 = 2 \times 1000$ d 'où $2000 \equiv 2\ (3)$

2) Soit p un entier.

Disjonction des cas :

$p \equiv 0\ [3], p + 1000 \equiv 1\ [3], p + 2000 \equiv 2\ [3],$

$p \equiv 1\ [3], p + 1000 \equiv 2\ [3], p + 2000 \equiv 0\ [3],$

$p \equiv 2\ [3], p + 1000 \equiv 0\ [3], p + 2000 \equiv 1\ [3],$

Dans tous les cas, un des entiers p, $p + 1\ 000$, $p + 2\ 000$ est divisible par 3.

En résumé :

p		***3k***	***3k + 1***	***3k + 2***
reste dans la division	de p	0	1	2
	de $p + 1000$	1	2	0

p		$3k$	$3k + 1$	$3k + 2$
euclidienne	de $p + 2000$	2	0	1
commentaire			$p + 2000$ est divisible par 3	$p + 1000$ est divisible par 3

Il reste un seul cas à étudier :

le seul multiple de 3 qui est un nombre premier est 3,

3, 1 003 et 2 003.

1 003 n'est pas dans la liste des nombres premiers. $1\,003 = 17 \times 59$

Dans tous les cas, au moins un des trois nombres p, $p + 1\,000$, $p + 2\,000$ n'est pas un nombre premier.

3) 11, 1511 et 3011 sont premiers.

Il existe au moins un p premier tel que p, $p + 1\,500$, $p + 3\,000$ sont tous les trois des nombres premiers.

(En prenant la liste des nombres premiers, on peut trouver aussi : (67 ; 1567 ; 3067) et (79 ; 1579 ; 3079)

---

79 page 73

1 a) p, $p + 10 \equiv p + 1$ (3) et $p + 20 \equiv p + 2$ (3)

Trois entiers consécutifs : un et un seul est multiple de 3.

b) La suite arithmétique de raison 10 ;

a, $b = a + 10$ et $c = a + 20$.

L'un des termes est multiple de 3 et les trois nombres sont premiers.

la seule possibilité est $a = 3$.

2) $3u + 13v + 23w = 0$

a) $3u + 13v + 23w \equiv v - w$ (3)

Puisque la somme est nulle : $3u + 13v + 23w = 0$ si et seulement si $v \equiv w$ (3)

b) $v = 3k + r$ et $w = 3k' + r$ (c'est le même reste r dans la division par 3 d'après 2a)) $0 \leqslant r \leqslant 2$

$3u + 13(3k + r) + 23(3k' + r) = 0$, soit : $3u + 39k + 69k' + 36r = 0$

$u = -13k - 23k' - 12r$

c) On a : $-2{,}5 \leqslant x \leqslant 2{,}5$ et $-2{,}5 \leqslant y \leqslant 2{,}5$ et $-2{,}5 \leqslant z \leqslant 2{,}5$

Si $r = 0$, $-2{,}5 \leqslant 3k \leqslant 2{,}5$ et $-2{,}5 \leqslant 3k' \leqslant 2{,}5$ et $-2{,}5 \leqslant -13k - 23k' \leqslant 2{,}5$

$k = 0$ et $k' = 0$, d'où, $u = 0$ $O(0 ; 0 ; 0)$

Si $r = 1$, $-2{,}5 \leqslant 3k + 1 \leqslant 2{,}5$ et $-2{,}5 \leqslant 3k' + 1 \leqslant 2{,}5$

$-3{,}5 \leqslant 3k \leqslant 1{,}5$ et $-3{,}5 \leqslant 3k' \leqslant 1{,}5$

$k = -1$ ou $k = 0$ et $k' = -1$ ou $k' = 0$,

$k = -1$ et $k' = -1$, alors, $x = 13 + 23 - 12 = 24$ impossible

$k = -1$ et $k' = 0$, alors, $x = 13 - 12 = 1$ $A(1 ; -2 ; 1)$

$k = 0$ et $k' = -1$, alors, $x = 23 - 12 = 11$ impossible

$k = 0$ et $k' = 0$, alors, $x = -12$ impossible

Si $r = 2$, $-2{,}5 \leqslant 3k + 2 \leqslant 2{,}5$ et $-2{,}5 \leqslant 3k' + 2 \leqslant 2{,}5$

$-4{,}5 \leqslant 3k \leqslant 0{,}5$ et $-4{,}5 \leqslant 3k' \leqslant 0{,}5$

$k = -1$ ou $k = 0$ et $k' = -1$ ou $k' = 0$,

$k = -1$ et $k' = -1$, alors, $x = 13 + 23 - 24 = 12$ impossible
$k = -1$ et $k' = 0$, alors, $x = 13 - 24 = -11$ impossible
$k = 0$ et $k' = -1$, alors, $x = 23 - 24 = -1$ $B(-1 ; 2 ; -1)$
$k = 0$ et $k' = 0$, alors, $x = -24$ impossible