Quel est le nombre premier

qui apparaît le plus souvent

comme le k-ième facteur premier d'un entier ?

Pourquoi le nombre **23** qui est le neuvième nombre premier est le nombre qui apparaît le plus souvent comme le cinquième facteur d'un entier ?

1ère PARTIE

PLAN de l'exposé 1ére partie

Définition (s) d'un nombre premier (NP)

Reconnaissance géométrique d'un NP

La place du nombre 1

La liste des 25 premiers NP

Spirale de ULAM

Il y a une infinité de NP

Décomposition d'un entier en facteurs premiers :
Les 3 propriétés démontrées par EUCLIDE
Existence de la décomposition
Unicité de la décomposition

Nombres premiers entre eux

Théorème de CESÀRO

Jean-Paul DELAHAYE

Merveilleux nombres premiers
Voyage au cœur de l'arithmétique

Dans son avant-propos, J-P DELAHAYE cite deux mathématiciens – Leonard EULER et Carl Friedrich GAUSS – parmi les plus grands de tous les temps qui avaient bien compris l'importance des NP ainsi que leur mystère.

« Les mathématiciens ont tenté, en vain jusqu'à ce jour, de découvrir une régularité dans la suite des nombres premiers, et nous avons de bonnes raisons de croire qu'il y a là un mystère que l'esprit humain ne pénètrera jamais. Il suffit d'ailleurs, pour s'en convaincre, de jeter un regard sur une table de nombres premiers (que certains ont pris la peine de calculer jusqu'à plusieurs centaines de milliers) ; on est alors instantanément convaincu qu'il ne règne ni ordre, ni règle. »

Leonard EULER (1707 – 1783)

« Le problème de la distinction entre nombres premiers et nombres composés, et celui de la décomposition d'un nombre en produit de facteurs premiers sont les plus importants et les plus utiles de toute l'arithmétique. […] L'honneur de la science semble exiger qu'on cultive avec zèle tout progrès dans la solution de ces élégantes et célèbres questions. »

Carl Friedrich GAUSS (1777 – 1855)

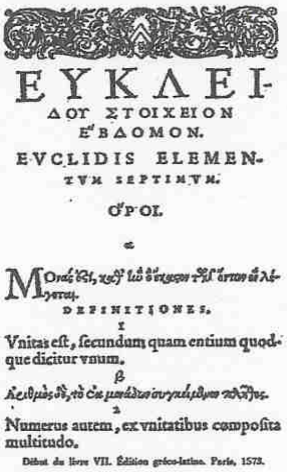
HARDY aimait dire que n'importe quel imbécile peut poser sur les nombres premiers des questions auxquelles l'homme le plus sage est incapable de répondre

La définition des nombres premiers par Euclide

Livre Septième. Définitions :

«L'unité est ce selon quoi chacune des choses existantes est dite une. Un nombre est un assemblage composé d'unités. Un nombre est une partie d'un nombre, le plus petit du plus grand, lorsque le plus petit mesure le plus grand. [...] Le nombre premier est celui qui est mesuré par l'unité seule. Le nombre composé est celui qui est mesuré par quelques nombres.» (traduction de F. Peyrard, 1819 ; voir le texte complet des premières définitions arithmétiques page 141)

L'idée de nombre que présente Euclide dans son traité est géométrique. C'est pourquoi il accompagne souvent ses démonstrations arithmétiques de dessins comportant des segments de droites. Pour Euclide, un nombre *A* est mesuré par un autre nombre *B* si l'on peut faire tenir *A* un nombre entier de fois dans *B*, comme lorsqu'on mesure la longueur d'un segment en reportant une règle un certain nombre de fois sur le segment :



ΕΥΚΛΕΙ-
ΔΟΥ ΣΤΟΙΧΕΙΟΝ
Ε' ΒΔΟΜΟΝ.
EVCLIDIS ELEMEN-
TVM SEPTIMVM.

ΟΡΟΙ.

Μονάς ἐστι, κατ' ἣν ἕκαστον τῶν ὄντων ἓν λέγεται.
DEFINITIONES.
I
Vnitas est, secundum quam entium quodque dicitur vnum.
β
Ἀριθμὸς δέ, τὸ ἐκ μονάδων συγκείμενον πλῆθος.
2
Numerus autem, ex vnitatibus composita multitudo.

Début du livre VII. Édition gréco-latine. Paris, 1573.

Le nombre 4 mesure 12, car, en déplaçant trois fois une règle de longueur 4 le long d'un segment de longueur 12, on arrivera exactement au bout. Bien sûr, l'expression «*A* mesure *B*» est équivalente à notre expression «*A* divise *B*» ou «*B* est un multiple de *A*», avec la nuance que lorsque l'on emploie l'expression «*A* mesure *B*», il est sous-entendu que *A* est plus petit que *B*. C'est pourquoi Euclide n'a pas besoin, dans sa définition, de spécifier qu'un nombre est premier s'il est mesuré par l'unité *et par lui-même*.

Un nombre est un assemblage composé d'unités.

Un nombre est premier s'il est mesuré par l'unité et par lui-même.

Représentation des nombres entiers par correspondance avec l'aire de rectangles (ou de carrés) à côtés entiers

Le nombre **3**

1 x 3 **Rectangle linéaire**

Le nombre **4**

1 x 4

Rectangle carré

2 x 2

Le nombre **5**

1 x 5 **Rectangle linéaire**

Le nombre **6**

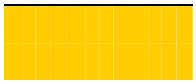
1 x 6

2 x 3

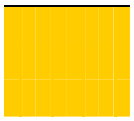
Il y a **2 rectangles** associés à 6 :
- un rectangle « linéaire »
Correspondant à 1x6 ou 6x1
- un rectangle 2x3 ou 2x3

Le nombre **12**

1 x 12



2 x 6



3 x 4

Il y a **3 rectangles** associés à 12 :
- un rectangle « linéaire »
Correspondant à 1x12 ou 12x1
- un rectangle 2x6 ou 6x2
- un rectangle 3x4 ou 4x3

Le nombre **13**

1 x 13 **Rectangle linéaire**

Les nombres ayant pour unique représentation rectangulaire un rectangle linéaire sont des NOMBRES PREMIERS.

Les nombres ayant au moins deux représentations rectangulaires sont des nombres composés.
Si, parmi les représentations des nombres, figure un carré, alors ces nombres sont des carrés.

Le nombre **16**

1 x 16
Rectangle linéaire

2 x 8 Rectangle

4 x 4 Rectangle carré

Quelques définitions :

« Un nombre premier est un entier naturel qui n'est divisible que par 1 et lui-même »

« Un nombre premier a pour ensemble de diviseurs une paire »

« Un nombre premier est un entier ayant un diviseur non trivial et un seul »

« Un nombre premier est un entier qui n'a pas de diviseur propre* »

*Soit un nombre entier n, un diviseur propre de n est un nombre différent de 1 et de n.

Et le nombre 1 ?

1 est-il considéré comme un nombre premier ?

Les avis sont partagés même si la majorité des mathématiciens lui refusent ce titre.

Parmi les raisons de refuser à 1 le qualificatif de nombre premier il y a le risque de ne pas respecter l'unicité de la décomposition d'un entier en facteurs premiers.
Par exemple : $12 = 2 \times 2 \times 3 = 1 \times 2 \times 2 \times 3 = 1 \times 1 \times 2 \times 2 \times 3$

Quelques remarques sur 1

Les Grecs ne considéraient pas que 1, ou l'UNITÉ soit un nombre.
C'était la MONADE, l'UNITÉ INDIVISIBLE depuis laquelle avaient grandi tous les autres nombres.
D'après EUCLIDE, un nombre est un agrégat composé d'unités.
Et l'allemand KOBEL écrivait en 1537 :
« D'où l'on comprend que 1 n'est pas un nombre, mais une génératrice, un commencement et une fondation pour tous les autres nombres »
Pour les Grecs, 1 était à la fois pair et impair (pair +1 = impair et impair + 1 = pair).
Ils avaient également noter que 1 est le seul entier qui produit plus par addition que par multiplication ($a + 1 > a \times 1$)

On ne parlera pas ici du nombre ZÉRO
Qui est le nombre du vide,
Arrivé tardivement,
Parfois neutre, parfois absorbant,
Scolairement décourageant.
Tout commence concrètement avec UN

Tout de même quel paradoxe !
UN est donc le premier nombre
Mais UN n'est pas un nombre premier

Cependant, avec seulement des chiffres 1, on peut fabriquer des NP très particuliers : les REP-UNITS.

On les note R_n où *n* désigne le nombre de chiffres 1 :

R_2 = 11
R_{19} = 1 111 111 111 111 111 111
R_{23} = 11 111 111 111 111 111 111 111
Le suivant a 317 chiffres 1…

Les 25 premiers NP en rouge dans le tableau suivant

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	100

Une autre présentation plus originale est la SPIRALE de Stanislaw ULAM
(ci-dessous de 1 à 400)

362	363	364	365	366	**367**	368	369	370	371	372	**373**	374	375	376	377	378	**379**	380	381
361	290	291	292	**293**	294	295	296	297	298	299	300	301	302	303	304	305	306	**307**	382
360	289	226	**227**	228	**229**	230	231	232	**233**	234	235	236	237	238	**239**	240	**241**	308	**383**
359	288	225	170	171	172	**173**	174	175	176	177	178	**179**	180	**181**	182	183	242	309	384
358	287	224	169	122	123	124	125	126	**127**	128	129	130	**131**	132	133	184	243	310	385
357	286	**223**	168	121	82	**83**	84	85	86	87	88	**89**	90	91	134	185	244	**311**	386
356	285	222	**167**	120	81	50	51	52	**53**	54	55	56	57	92	135	186	245	312	387
355	284	221	166	119	80	49	26	27	28	**29**	30	**31**	58	93	136	187	246	**313**	388
354	**283**	220	165	118	**79**	48	25	10	**11**	12	**13**	32	**59**	94	**137**	188	247	314	**389**
353	282	219	164	117	78	**47**	24	9	**2**	**3**	14	33	60	95	138	189	248	315	390
352	**281**	218	**163**	116	77	46	**23**	8	1	4	15	34	**61**	96	**139**	190	249	316	391
351	280	217	162	115	76	45	22	**7**	6	**5**	16	35	62	**97**	140	**191**	250	**317**	392
350	279	216	161	114	75	44	21	20	**19**	18	**17**	36	63	98	141	192	**251**	318	393
349	278	215	160	**113**	74	**43**	42	**41**	40	39	38	**37**	64	99	142	**193**	252	319	394
348	**277**	214	159	112	**73**	72	**71**	70	69	68	**67**	66	65	100	143	194	253	320	395
347	276	213	158	111	110	**109**	108	**107**	106	105	104	**103**	102	**101**	144	195	254	321	396
346	275	212	**157**	156	155	154	153	152	**151**	150	**149**	148	147	146	145	196	255	322	**397**
345	274	**211**	210	209	208	207	206	205	204	203	202	201	200	**199**	198	**197**	256	323	398
344	273	272	**271**	270	**269**	268	267	266	265	264	**263**	262	261	260	259	258	**257**	324	399
343	342	341	340	339	338	**337**	336	335	334	333	332	**331**	330	329	328	327	326	325	400

EXISTENCE D'UNE INFINITÉ DE NOMBRES PREMIERS

Comme on peut s'en douter, EUCLIDE ne s'est pas exprimé aussi brutalement.
Il s'est contenté d'affirmer que **« pour toute quantité donnée de nombres premiers,il y en a un plus grand »**, ce qui est une façon assez hypocrite de parler de l'infini …

(J-P DELAHAYE)

Il existe des démonstrations assez nombreuses de ce théorème.
Citons les principaux auteurs de ces démonstrations :

- EUCLIDE qui, le premier, a démontré ce théorème au IIIème siècle av. J.-C.
- EULER en 1737 qui démontre par la théorie analytique des nombres.
- POLYA vers 1920 qui utilise les nombres de FERMAT.
- ERDÖS vers 1938.

Voici la démonstration d'EUCLIDE :

Considérons un nombre fini non nul de NP.

Appelons *p* le plus grand d'entre eux et formons le produit : 2 x 3 x … x *p* de tous les NP jusqu'à *p*, produit* qui contient en facteurs tous les NP envisagés initialement.

Le nombre N = 2 x 3 x … x *p* + 1 est plus grand que 1.
Or, on sait que tout nombre entier autre que 1 est divisible par au moins un nombre premier.
Donc le nombre N est divisible par au moins un nombre premier *q*.

Montrons que *q* est plus grand que *p*. En effet, dans le cas contraire (c'est-à-dire si *q* est plus petit que *p*), *q* diviserait le produit 2 x 3 x … x *p*.
Comme il divise déjà N = 2 x 3 x … x *p* + 1, il diviserait leur différence ce qui est absurde puisque cette différence est le nombre 1.

Donc le NP *q* est plus grand que le NP *p*.

Il est toujours possible de trouver un NP plus grand que tous ceux envisagés au départ : c'est ce qu'il fallait démontrer.

*** le produit 2 x 3 x … x *p* de tous les NP jusqu'à *p* est appelé une primorielle**.

Notons au passage que le nombre N lui-même peut être premier, auquel cas on a évidemment *q* = N. C'est ce qui se passe dans les cas les plus simples :

2 + 1 = 3 ; (2 x 3) + 1 = 7 ; (2 x 3 x 5) + 1 = 31
(2 x 3 x 5 x 7) + 1 = 211 ; (2 x 3 x 5 x 7 x 11) + 1 = 2 311.

Les nombres 3, 7, 31, 211 et 2 311 sont des NP.
Par contre, le suivant est composé : (2 x 3 x 5 x 7 x 11 x 13) + 1 = 30 031 et 30 031 = 59 x 509.
Le NP suivant est assez loin :

(2 x 3 x 5 x 7 x 11 x 13 x 17 x 19 x 23 x 29 x 31) + 1 =) + 1 = 200 560 490 531..

L'ENSEMBLE DES NOMBRES PREMIERS EST UN « GROS INFINI »

L'ensemble des NP, de densité limite nulle, est-il un gros ou un petit infini, au regard du critère de la série des inverses ?
C'est un gros infini, car on sait, depuis qu'EULER l'a démontré en 1737, que la somme des inverses des NP diverge.

Théorème de raréfaction d' EULER
:
La somme des inverses des NP vaut + ∞

$$\sum_{p(premier)} \frac{1}{p} = +\infty$$

Remarquons que ce théorème donne bien des indications sur la raréfaction (dont on sait, par le théorème de LEGENDRE, qu'elle se produit), mais de façon négative : il indique que l'infini des NP est un gros infini, ce qui signifie que ceux-ci ne se raréfient pas très vite. Il existe un troisième théorème de raréfaction, démontré indépendamment par HADAMARD et de la VALLÉE POUSSIN plus d'un siècle après celui d'EULER, et qui fournit la vitesse précise de la raréfaction.

L'hypothèse de RIEMANN, si un jour on la démontre, sera un autre théorème de raréfaction, encore plus précis.

$\pi(m)$ est le nombre de NP inférieurs à $m = 10^p$

En comparant les deux pyramides, on perçoit l'évolution de la proportion des NP parmi les nombres entiers.

p	$m = 10^p$	$\pi(m)$	% [$\pi(m) / 10^p$]
1	10	4	40
2	100	25	25
3	1 000	168	16,8
4	10 000	1 229	12,29
5	100 000	9 592	9,592
6	1 000 000	78 498	7,849 8
7	10 000 000	664 579	6,645 79
8	100 000 000	5 761 455	5,761 455
9	1 000 000 000	50 847 534	5,084 753 4
10	10 000 000 000	455 052 511	4,550 525 11
11	100 000 000 000	4 118 054 813	4,118 054 813
12	1 000 000 000 000	37 607 912 018	3,760 781 201 8
13	10 000 000 000 000	346 065 536 839	3,460 655 368 39
14	100 000 000 000 000	3 204 941 750 802	3,204 941 750 802
15	1 000 000 000 000 000	29 844 570 422 669	2,984 457 042 266 9

La proportion de NP est d'environ 2,22 % pour 10^{20}.
Elle passe au dessous de 2 % pour 10^{23} : ~1,925 %.

DÉCOMPOSITION D'UN ENTIER EN FACTEURS PREMIERS

Voici comment Jean DIEUDONNÉ présente les propriétés des NP dans son livre « *Pour l'honneur de l'esprit humain* » paru en 1987 :

« A ma connaissance, dans aucune civilisation antique autre que la civilisation grecque, on n'avait songé avant le V^{e} siècle avant J.-C à la décomposition d'un entier en facteurs premiers. Cette décomposition, que nous écrivons maintenant :

$$n = p_1^{k1_1} p_2^{k2} \ldots p_r^{ki}$$

où $p_1 p_2 \ldots p_r$ sont des NP et les k_i des exposants au moins égaux à 1, n'apparaît pas explicitement chez EUCLIDE faute de notations adéquates.

Mais il démontre les trois propriétés suivantes (exprimées en langage moderne) :

a/ Tout entier est premier ou divisible par un nombre premier (Livre VII, 31)

b/ Si p est un nombre premier, une puissance p^m ne peut être divisible que par les nombres p^r avec $r < m$ (Livre IX, 13).

c/ Si un nombre premier divise un produit ab et ne divise pas a, il divise b (Livre VII, 32).

A partir de là, il est facile, en raisonnant par récurrence, d'établir l'existence et l'unicité de la décomposition.»

EXISTENCE ET UNICITÉ

DE LA DÉCOMPOSITION EN FACTEURS PREMIERS

Tout nombre entier supérieur à 1 (ou supérieur ou égal à 2) s'écrit de manière unique (à l'ordre près) sous la forme d'un produit de facteurs premiers.

Démonstration de l'existence de cette décomposition pour tout nombre entier

Initialisation

2 s'écrit $2 = 2$.

Par convention, un nombre seul est considéré comme un produit de un facteur.

Hypothèse de récurrence

Soit un entier n, $n > 2$

On suppose que tous les entiers entre 2 et $n - 1$ s'écrivent comme produit de facteurs premiers.

Généralisation de cette propriété à l'entier n

Montrons que cela est aussi vrai pour n.

Rappelons la propriété suivante démontrée par EUCLIDE :

(1) « Tout nombre supérieur à 1 est divisible par un nombre premier »

Nous savons d'après (1) que n est divisible par un nombre premier noté p.

Donc $n = q \times p$ avec $1 < p \leq n$.

On doit envisager deux cas possibles : $p = n$ ou $p < n$

Si $p = n$ et $q = 1$ alors n est un nombre premier, c'est-à-dire p.

(Par convention, un nombre seul est considéré comme un produit de un facteur)

Si $p < n$ alors $2 < q \leq n - 1$.

D'après l'hypothèse de récurrence, q est un produit de nombres premiers.

Par conséquent, n l'est aussi puisqu'il s'écrit $n = q \times p$.

Cela clôt la démonstration.

Démonstration de l'unicité de cette décomposition pour tout nombre entier

Supposons l'existence de deux suites de NP :

$$p_1 \le p_2 \le p_3 \le ... \le p_i \le ... \le p_r \quad \text{et} \quad s_1 \le s_2 \le s_3 \le ... \le s_j \le ... \le s_t$$

Supposons également qu'un nombre entier n admette deux décompositions distinctes :

$$n = p_1 \times p_2 \times p_3 \times ... \times p_i \times ... \times p_r = s_1 \times s_2 \times s_3 \times ... \times s_j \times ... \times s_t$$

Comparons p_1 et s_1

Il y a 3 cas possibles :

$$p_1 < s_1 \quad \text{ou} \quad p_1 = s_1 \quad \text{ou} \quad p_1 > s_1$$

En fait $p_1 < s_1$ et $p_1 > s_1$ sont analogues pour la démonstration.
Il suffit donc de traiter $p_1 < s_1$ ou $p_1 = s_1$

On suppose $p_1 = s_1$

Si $p_1 = s_1$ alors $\frac{n}{p_1} = p_2 \times p_3 \times ... \times p_i \times ... \times p_r = s_2 \times s_3 \times ... \times s_j \times ... \times s_t$

On en déduit que $p_2 \times p_3 \times ... \times p_i \times ... \times p_r = s_2 \times s_3 \times ... \times s_j \times ... \times s_t$

(On peut recommencer et supposer que $p_2 = s_2$ etc. …)

Les deux suites sont identiques.

On suppose $p_1 < s_1$. (On propose une démonstration par l'absurde)

Si $p_1 < s_1$ alors p_1 divise le produit $s_1 \times s_2 \times s_3 \times ... \times s_j \times ... \times s_t$

Donc p_1 divise l'un des facteurs s_j.
Mais, par hypothèse, p_1 et s_j étant des NP, la seule possibilité est l'égalité $p_1 = s_j$.
Or, par hypothèse, $s_j \ge s_1$

Si $p_1 < s_1$ et $s_1 < s_j$ alors $p_1 < s_1 < s_j$ (1)

Or nous avons précédemment déduit que $p_1 = s_j$. (2)
Il est impossible de vérifier à la fois (1) et (2).
Nous aboutissons donc à une contradiction. Par conséquent : $p_1 < s_1$ est fausse.
Donc ; $p_1 = s_1$

Les deux suites sont identiques.

NOMBRES PREMIERS ENTRE EUX

Définition

Si deux nombres entiers a et b non nuls n'ont aucun autre facteur commun que 1 (facteur inévitable), alors on dit que ces deux nombres sont premiers entre eux

On peut résumer de la façon suivante :

$[a \in IN^*, b \in IN^*$ et pgcd $(a ; b) = 1]$ <===> ***a* et *b*** premiers entre eux.

Cas particuliers : pgcd $(1 ; 1) = 1$

Quel que soit l'entier n non nul pgcd $(1 ; n) = 1$

Remarques

Si p et q sont deux NP alors (*a fortiori*) p et q sont premiers entre eux.

Deux nombres entiers consécutifs, n et $n + 1$, $n \neq 0$, sont premiers entre eux.

Théorème de BACHET

(connu – à tort – sous le nom d'identité de BEZOUT)

Si a et b sont premiers entre eux, autrement dit si pgcd $(a ; b) = 1$, alors il existe deux entiers relatifs x et y tels que $ax + by = 1$.

Par exemple :

pgcd $(15 ; 22) = 1$, il existe $(x ; y) = (3 ; -2)$ tels que : $15 \times 3 + 22 \times (-2) = 1$

L'INDICATEUR D'EULER

(ou FONCTION INDICATRICE D'EULER)

On note $\varphi(n)$ l'indicateur de n pour l'entier n.

Par définition, **$\varphi(n)$ est égal au nombre d'entiers entre 0 et n qui sont premiers avec n**.

On convient que $\varphi(0) = 0$ et $\varphi(1) = 1$.

Exemple : 12 est premier avec 1, 5, 7 et 11.
Donc $\varphi(12) = 4$.

Le théorème de l'indicateur d'EULER permet d'énoncer les règles suivantes :

1 Si n et m sont deux entiers supérieurs à 0 et premiers entre eux alors :

$$\varphi(n \times m) = \varphi(n) \times \varphi(m)$$

2 Si n est une puissance kième d'un NP noté p, donc si $n = p^k$ alors :

$$\varphi(n) = p^k \left(1 - \frac{1}{p}\right)$$

Exemple : $\varphi(125) = 5^3 \left(1 - \frac{1}{5}\right) = 125 \times \frac{4}{5} = 100$

3 Si n possède les facteurs premiers $p_1, p_2^2 \ldots p_r^i$ alors :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

ou encore :

$$\varphi(n) = n\left[\prod_{\substack{p(premier) \\ p/n}} \left(1 - \frac{1}{p}\right)\right]$$

Exemples : $28 = 2^2 \times 7$ ===> $\varphi(28) = 28\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 28 \times \frac{3}{7} = 12$

PROBABILITÉ QUE DEUX NOMBRES ENTIERS

CHOISIS AU HASARD SOIENT PREMIERS ENTRE EUX

Soit m et n deux nombres choisis au hasard.

Considérons le NP 2 et cherchons la probabilité que 2 divise à la fois m et n :

La probabilité que 2 divise m est 1 / 2.

La probabilité que 2 divise n est 1 / 2.

La probabilité que 2 divise à la fois m et n est donc : $\frac{1}{2}\times\frac{1}{2}=\frac{1}{4}$

[En notant P pour pair et I pour impair, on a effectivement 4 cas possibles :

PP ; PI ; IP et II

Seul PP répond à la question]

Par suite, la probabilité que 2 ne divise pas à la fois m et n est :

$$1-\frac{1}{4}=\frac{3}{4} \quad \text{(ou 75 \%)}$$

Répétons le même raisonnement pour 3.

Nous aboutirons, pour que 3 divise à la fois m et n, à une probabilité de $\frac{1}{3}\times\frac{1}{3}=\frac{1}{9}$:et, pour que 3 ne divise ni m ni n, à une probabilité de $1-\frac{1}{9}=\frac{8}{9}$. (ou ~ 88 %)

Pour 5, on voit aisément que la probabilité pour que 5 ne divise pas à la fois m et n est :

$$1-\frac{1}{25}=\frac{24}{25} \quad \text{(ou ~ 96 \%)}$$

Si nous voulons maintenant connaître la probabilité pour que 2 nombres choisis au hasard dans IN ne soient divisibles à la fois ni par 2, ni par 3, ni par 5, il faut et il suffit de faire le produit des probabilités partielles :

$$\frac{3}{4}\times\frac{8}{9}\times\frac{24}{25}=\frac{16}{25} \quad \text{(ou 64 \%)}$$

.

Généralisation :

Pour tout NP noté p, la probabilité pour que p divise à la fois m et n est $\frac{1}{p^2}$. D'où il résulte que la probabilité pour que p ne divise ni m ni n est $1-\frac{1}{p^2}$

Appelons p_1, p_2, p_3 trois NP.
Pour que deux nombres entiers choisis au hasard ne soient divisibles ni par p_1, ni par p_2, ni par p_3, est : $\left(1-\frac{1}{{p_1}^2}\right)\left(1-\frac{1}{{p_2}^2}\right)\left(1-\frac{1}{{p_3}^2}\right)$

Le théorème de CESÀRO

En 1881, le mathématicien Ernesto CESÀRO (1859 – 1906) démontra que la probabilité que deux entiers naturels choisis au hasard dans IN soient premiers entre eux est égale à

$$\prod_{\substack{p=2 \\ p:premier}}^{\infty}\left(1-\frac{1}{p^2}\right)=\frac{6}{\pi^2}$$ **ou 0,607 927 … soit ~ 60,8 %**

C'est également la densité des nombres sans facteur carré (ou encore la probabilité pour qu'un nombre choisi au hasard ne soit pas divisible par un carré).

Remarque

La démonstration du résultat ci-dessus est étroitement lié à la somme des inverses des carrés des entiers naturels. En effet :

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+...+\frac{1}{n^2}$$

C'est le fameux « problème de Bâle » résolu par EULER en 1735.
Il démontra que cette somme converge, et plus précisément que :

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$$