SUJET 0

Travail demandé

Les candidats doivent étudier puis présenter le dossier joint à travers un exposé de synthèse d'une durée comprise entre 15 et 20 minutes.

Si l'étude de la totalité du dossier et la préparation d'un exposé cohérent dans la durée impartie ne vous paraissent pas possible, vous pouvez décider de vous limiter à une partie du dossier.

Remarques générales

Les textes proposés, quelle que soit leur origine, peuvent présenter des défauts (coquilles typographiques, négligence ou sous-entendus de l'auteur, voire erreurs...) qui, sauf exception, n'ont pas été corrigés.

Ils peuvent contenir des exercices qu'il n'est pas demandé de résoudre. Néanmoins, vous pouvez vous aider des énoncés de ces exercices pour enrichir votre exposé.

Les documents fournis peuvent être annotés. Ils seront récupérés, ainsi que vos supports d'exposé, à l'issue de l'examen. Il est important que les candidats sachent que leurs éventuelles annotations ne seront pas lues par l'examinateur et ne seront donc pas prises en compte pour la notation.

Remarques particulières

1. Ne pas s'inquiéter de la numérotation des parties du texte ou des ajouts manuels. Pour faciliter la lecture, certains passages ont été retirés, d'autres ont pu être réaménagés ou légèrement modifiés.

2. Nous disons qu'un entier a est *divisible* par un entier non nul b (ou que b est un *diviseur* de a ou encore que a est un *multiple* de b) s'il existe un entier c tel que $a = bc$. On note $b \mid a$ qu'on lit : b *divise* a. En particulier, 1 divise tout entier non nul et tout entier divise 0. Si b ne divise pas a, on note $b \nmid a$.

3. Dans le texte, la fonction log est le logarithme népérien, c'est-à-dire le logarithme de base e, noté usuellement ln.

4. On note $\pi(x)$ le nombre de nombres premiers compris entre 1 et x.

CHAPITRE I

La suite des nombres premiers (1)

1.2 Nombres premiers

Dans ce paragraphe, et jusqu'au paragraphe §2.9, les nombres considérés sont en général des entiers strictement positifs. Dans l'ensemble des entiers strictement positifs, il existe une sous-classe de nombres particulièrement importante, celle des *nombres premiers*. Un nombre p est dit *premier* si

(i) $p > 1$

(ii) p n'admet aucun autre diviseur positif que 1 et p.

Par exemple 37 est un nombre premier. Il est très important de remarquer que 1 n'est pas considéré comme premier. Dans ce chapitre et le suivant, nous réservons la lettre p pour désigner des nombres premiers.

Un nombre strictement plus grand que 1 est dit *composé* s'il n'est pas premier.

Notre premier théorème est le suivant :

Théorème 1 *Tout entier strictement supérieur à 1 est produit de nombres premiers.*

Soit n un entier strictement positif. De deux choses l'une : soit n est premier, et alors il n'y a rien a démontrer, soit n a des diviseurs qui sont strictement compris entre 1 et n. Soit m le plus petit de ces diviseurs, alors m est premier : en effet, sinon

$$\exists \ell \quad 1 < \ell < m \quad \text{et} \quad \ell \mid m.$$

Or

$$\ell \mid m \Rightarrow \ell \mid n$$

ce qui contredit le fait que m est le plus petit diviseur de n strictement supérieur à 1.

Donc n est soit premier, soit divisible par un nombre premier p_1 plus petit que n. Dans ce cas, nous avons

$$n = p_1 n_1, \qquad 1 < n_1 < n.$$

Soit n_1 est premier, et il n'y a rien de plus à démontrer, soit n_1 est divisible par un nombre premier p_2 plus petit que n_1, auquel cas

$$n = p_1 n_1 = p_1 p_2 n_2, \qquad 1 < n_2 < n_1 < n.$$

En répétant cet argument, nous obtenons une suite décroissante de nombres, n, $n_1, \ldots, n_{k-1}, \ldots$ qui sont tous strictement plus grands que 1, et pour lesquels la même alternative se présente toujours. Tôt ou tard, nous tombons dans le premier cas, à savoir que n_{k-1} est premier. Nous le notons p_k, et alors

$$n = p_1 p_2 \cdots p_k \tag{1.2.1}$$

Ainsi

$$666 = 2 \cdot 3 \cdot 3 \cdot 37.$$

Si $ab = n$, alors a et b ne peuvent pas être simultanément strictement plus grands que $\sqrt{n}$. Nous en déduisons que tout nombre composé n est divisible par un nombre premier p inférieur ou égal à $\sqrt{n}$.

Les nombres premiers qui interviennent dans (1.2.1) ne sont pas forcément distincts et ne sont pas ordonnés. Si nous les ordonnons par ordre croissant, regroupons les facteurs correspondant à un même nombre premier et modifions les notations de manière appropriée, il vient

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad (a_1 > 0, a_2 > 0, \ldots, p_1 < p_2 < \ldots). \tag{1.2.2}$$

Nous disons alors que n est écrit sous la *forme standard*.

1.3 Énoncé du théorème fondamental de l'arithmétique

Dans la démonstration du théorème 1, rien n'indique que la décomposition de n provenant de (1.2.2) est unique, ou encore, ce qui revient au même, que l'écriture (1.2.1) est *unique* à l'ordre des facteurs près. L'étude de cas particuliers suggère pourtant qu'il y a bien unicité.

Théorème 2 (Théorème fondamental de l'arithmétique) *La forme standard de tout entier strictement positif n est unique : la décomposition de n en produit de facteurs premiers est unique, à l'ordre des facteurs près.*

Le théorème 2 est la base de l'arithmétique systématique ; nous ne l'utiliserons pas dans ce chapitre et nous repoussons sa démonstration complète au paragraphe §2.10. Prouvons dès maintenant que c'est un corollaire de l'énoncé plus simple suivant :

Théorème 3 (Premier théorème d'Euclide) *Si p est un nombre premier et si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

Acceptons ce théorème pour le moment, afin d'en déduire le théorème 2. La démonstration du théorème 2 est alors ramenée à celle du théorème 3, qui est donnée au paragraphe §2.10.

Voici un corollaire immédiat du théorème 3 :

$$p \mid abc\cdots\ell \Rightarrow p \mid a \text{ ou } p \mid b \text{ ou } p \mid c\ldots \text{ ou } p \mid \ell.$$

En particulier, si a, b, $\ldots$, ℓ sont premiers, alors p est égal à l'un des nombres a, b, $\ldots$, ℓ. Supposons maintenant que nous ayons deux décompositions

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j},$$

chaque décomposition étant un produit de facteurs premiers écrit sous la forme standard. Alors $p_i \mid q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}$ pour tout i de sorte que chacun des p est un certain q (de même, chaque q est un certain p). Par suite, $k = j$ et, comme les deux ensembles sont ordonnés par ordre croissant, nous avons $p_i = q_i$ pour tout i.

Si maintenant $a_i > b_i$, en divisant les deux membres par $p_i^{b_i}$, il vient

$$p_1^{a_1} \cdots p_i^{a_i - b_i} p_k^{a_k} = p_1^{b_1} \cdots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \cdots p_k^{b_k}.$$

Le membre de gauche est alors divisible par p_i, et non le membre de droite ; contradiction. De même $b_i > a_i$ soulève une contradiction. Il en résulte $a_i = b_i$, et le théorème 2 est démontré.

La raison pour laquelle 1 ne peut pas être compté comme nombre premier est maintenant apparente : si 1 était premier, le théorème 2 serait faux car nous pourrions multiplier la décomposition de n en facteurs premiers par n'importe quelle puissance de 1.

1.4 La suite des nombres premiers

Les plus petits nombres premiers sont

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$$

Il est facile de construire une table de nombres premiers inférieurs à un nombre entier fixé N, par une procédure appelée « crible d'Ératosthène ». Nous avons remarqué que si $n \leqslant N$ et si n n'est pas premier, alors n est divisible par un nombre premier inférieur ou égal à $\sqrt{N}$. Nous écrivons les nombres

$$2, 3, 4, 5, 6, \ldots, N$$

et nous barrons successivement

(i) 4, 6, 8, 10, ... *i. e.* 2^2 et tous les nombres pairs qui le suivent,

(ii) 9, 15, 21, 27, ... *i. e.* 3^2 et tous les multiples de 3 non encore barrés qui le suivent,

(iii) 25, 35, 55, 65, ... *i. e.* 5^2 le carré du premier nombre non barré restant après 3, puis tous les multiples de 5 non encore barrés, ...

La procédure se poursuit jusqu'à ce que le nombre restant, après avoir barré les derniers multiples, soit plus grand que $\sqrt{N}$. Les nombres qui n'ont pas été barrés sont premiers. Toutes les tables de nombres premiers dont nous disposons à l'heure actuelle ont été obtenues en utilisant des versions améliorées de cette procédure.

Ces tables montrent que la suite des nombres premiers est infinie. Elle est connue jusqu'à 100 000 000. Il y a 664 579 nombres premiers inférieurs à 10 millions et 6 134 entre 9 900 000 et 10 000 000. Il y en a 50 847 478 d'inférieurs à 1 000 000 000, mais il ne sont pas connus individuellement. Des nombres premiers très grands sont également connus, la plupart de la forme $2^p - 1$ (voir §2.5) ; le plus grand qui ait été trouvé à l'heure actuelle s'écrit avec plus de 6 500 chiffres.

Ces données nous suggèrent le théorème suivant :

Théorème 4 (Second théorème d'Euclide) *Il existe une infinité de nombres premiers.*

Nous démontrerons ce résultat au paragraphe §2.1.

La répartition « moyenne » des nombres premiers est très régulière, sa densité décroît lentement mais régulièrement. Parmi les cinq premiers blocs de 1 000 nombres, il se trouve

$$168, 135, 127, 120, 119$$

nombres premiers respectivement ; et parmi les cinq derniers blocs de 1 000 nombres inférieurs à 10 000 000 il s'en trouve

$$62, 58, 67, 64, 53.$$

Les 53 derniers nombres premiers se répartissent en paquets de

$$5, 4, 7, 4, 6, 3, 6, 4, 5, 9$$

éléments respectivement dans chacune des dix centaines du dernier millier.

D'un autre côté, la répartition locale des nombres premiers est extrêmement irrégulière.

Tout d'abord, les tables font apparaître de longues séquences de nombres composés, par exemple, le nombre premier 370 261 est suivi de 111 nombres composés. Il est facile de voir que ces longues séquences doivent apparaître. Supposons que

$$2, 3, 5, \ldots, p$$

sont les nombres premiers plus petits que p. Alors tous les entiers jusqu'à p sont divisibles par l'un de ces nombres premiers. Donc, en notant

$$2 \cdot 3 \cdot 5 \cdots p = q,$$

les $p - 1$ nombres

$$q + 2, q + 3, q + 4, \ldots, q + p$$

sont composés. Si le théorème 4 est vrai, alors p peut être choisi aussi grand que nous le voulons ; sinon, tous les nombres sont composés à partir d'un certain rang.

Théorème 5 *Il existe des séquences de nombres composés consécutifs, dont la longueur dépasse n'importe quel nombre donné N.*

D'autre part nous trouvons dans les tables des couples de nombres premiers aussi grands que nous le souhaitons et qui, comme 3, 5 ou 101, 103, diffèrent de 2. Il existe 1 224 couples $(p, p + 2)$ inférieurs à 100 000 et 8 169 inférieurs à 1 000 000. Ceci semble justifier la conjecture suivante :

Il existe une infinité de couples de nombres premiers de la forme $(p, p+2)$.

Il est même raisonnable de conjecturer un résultat plus fort. Les nombres p, $p + 2$ et $p + 4$ ne peuvent pas être simultanément premiers car l'un d'entre eux est forcément divisible par 3. En revanche, il n'y a aucune raison évidente pour que p, $p + 2$ et $p + 6$ ne soient pas simultanément premiers et les tables montrent que les triplets de nombres premiers de la forme $(p, p + 2, p + 6)$ apparaissent, eux aussi, indéfiniment. Ceci nous amène à formuler la conjecture suivante :

Il existe une infinité de triplets de nombres premiers de la forme $(p, p + 2, p + 6)$ *et de la forme* $(p, p + 4, p + 6)$.

Nous pouvons multiplier de telles conjectures, concernant des ensembles plus grands de nombres premiers, mais leur démonstration ou leur réfutation reste, jusqu'à présent, hors de portée des mathématiciens.

1.6 Quelques notations

Nous allons souvent utiliser les symboles

$$O, o, \sim \tag{1.6.1}$$

et, occasionnellement, les symboles

$$\prec, \succ, \asymp . \tag{1.6.2}$$

Ces symboles sont définis comme suit.

Supposons que n est une variable entière qui tend vers l'infini et x une variable continue qui tend vers l'infini ou vers zéro ou vers une certaine valeur finie, que $\phi(n)$ ou $\phi(x)$ est une fonction à valeurs strictement positives de n ou de x, et que $f(n)$ ou $f(x)$ est une autre fonction quelconque de n ou de x. Alors

(i) $f = O(\phi)$ signifie que $|f| < A\phi$[†] pour toute valeur de n ou x, avec A indépendant de n ou de x ;

(ii) $f = o(\phi)$ signifie que $f/\phi \to 0$;

et

(iii) $f \sim \phi$ signifie que $f/\phi \to 1$.

Ainsi

$$10x = O(x), \qquad \sin x = O(1), \qquad x = O(x^2),$$
$$x = o(x^2), \qquad \sin x = o(x), \qquad x + 1 \sim x,$$

lorsque $x \to \infty$ et

$$x^2 = O(x), \qquad x^2 = o(x), \qquad \sin x \sim x, \qquad 1 + x \sim 1,$$

lorsque $x \to 0$. Il est à noter que $f = o(\phi)$ implique, et est plus restrictif, que $f = O(\phi)$.

Maintenant, expliquons les symboles (1.6.2) :

(iv) $f \prec \phi$ signifie que $f/\phi \to 0$ et c'est équivalent à $f = o(\phi)$;

(v) $f \succ \phi$ signifie que $f/\phi \to \infty$;

(vi) $f \asymp \phi$ signifie que $A\phi < f < A\phi$,

où les deux constantes A (qui ne sont pas les mêmes, bien sûr) sont toutes deux strictement positives et indépendantes de n ou de x. Ainsi $f \asymp \phi$ signifie que « f est de même ordre de grandeur que ϕ ».

La lettre A, comme dans (vi), désignera très souvent une *constante positive non spécifiée*. Les valeurs des différents A ne sont en général pas identiques, même lorsque ces A apparaissent dans une même formule ; de plus, même si nous pouvons leur faire correspondre des valeurs précises, ces valeurs n'interviennent pas dans l'argumentation.

[†] $|f|$ désigne le module ou la valeur absolue de f, comme en analyse.

Jusqu'ici, nous avons défini (par exemple) $f = O(1)$, mais pas $O(1)$ d'une manière isolée. Nous aurons besoin de notations plus souples. Nous convenons donc que $O(\phi)$ désigne *une fonction f non spécifiée telle que* $f = O(\phi)$. Nous pouvons alors écrire, par exemple,

$$O(1) + O(1) = O(1) = o(x)$$

lorsque $x \to \infty$, ce qui veut dire « si $f = O(1)$ et $g = O(1)$, alors $f + g = O(1)$ et *a fortiori* $f + g = o(x)$ ». De même, nous pouvons écrire

$$\sum_{\nu=1}^{n} O(1) = O(n),$$

ce qui signifie que la somme de n termes, tous bornés par une constante, est plus petite qu'un multiple constant de n.

Remarquons que la relation « $=$ », entre les symboles O et o, n'est pas symétrique en général. Par exemple, $o(1) = O(1)$ est toujours vraie, alors que $O(1) = o(1)$ est en général fausse. Nous pouvons aussi observer que $f \sim \phi$ est équivalent à $f = \phi + o(\phi)$ ou à

$$f = \phi(1 + o(1)).$$

Dans ce cas, nous disons que f et ϕ sont *asymptotiquement équivalents* ou que f est *asymptotique* à ϕ.

Définissons encore une expression qui nous sera utile par la suite. Si P est une propriété que peut avoir un entier strictement positif, notons $P(x)$ le nombre d'entiers inférieurs à x qui possèdent la propriété P. Si

$$P(x) \sim x,$$

lorsque $x \to \infty$, *i. e.* si le nombre d'entiers inférieurs à x qui ne possèdent pas la propriété P est un $o(x)$, alors nous disons que *presque tous les nombres* possèdent la propriété P. Ainsi, nous verrons que $\pi(x) = o(x)$, de sorte que presque tous les nombres sont composés.

1.8 Énoncé du théorème des nombres premiers

Après cette introduction, nous pouvons énoncer le théorème:

Théorème 6 (Théorème des nombres premiers) *Le cardinal de l'ensemble de nombres premiers inférieurs à x est asymptotiquement équivalent à $x/\log x$, c'est-à-dire*

$$\pi(x) \sim \frac{x}{\log x}.$$

Ce théorème est le résultat central pour la théorie de la répartition des nombres premiers. Il est difficile à démontrer. En revanche, il y a une démonstration beaucoup plus facile du théorème plus faible :

Théorème 7 (Théorème de Tchebychef) *L'ordre de grandeur de $\pi(x)$ est $x/\log x$, autrement dit*

$$\pi(x) \asymp \frac{x}{\log x}.$$

La comparaison entre le théorème 6 et les résultats des tables est intéressante. Les valeurs de $\pi(x)$ pour $x = 10^3$, $x = 10^6$ et $x = 10^9$ sont respectivement :

$$168, \qquad 78\,498 \quad \text{et} \quad 50\,847\,478;$$

et les valeurs de $x/\log x$, arrondies à l'entier le plus proche, sont

$$145, \qquad 72\,382 \quad \text{et} \quad 48\,254\,942.$$

Les rapports sont donc

$$1,159\ldots, \qquad 1,084\ldots, \qquad 1,053\ldots;$$

et montrent un début de convergence – pas très rapide – vers 1. La différence entre les valeurs exactes et les valeurs approchées est justifiée par la théorie générale.

Si

$$y = \frac{x}{\log x},$$

alors

$$\log y = \log x - \log\log x,$$

et

$$\log\log x = o(\log x),$$

donc

$$\log y \sim \log x \quad \text{et} \quad x = y\log x \sim y\log y.$$

La fonction inverse de $x/\log x$ est alors asymptotiquement équivalente à $x\log x$.

Nous déduisons de cette remarque que le théorème 6 est équivalent au

Théorème 8

$$p_n \sim n\log n.$$

De même, le théorème 7 est équivalent au

Théorème 9

$$p_n \asymp n\log n.$$

Le 664 999-ième nombre premier est 10 006 721. Nous incitons le lecteur à comparer ce résultat avec le théorème 8.

Ce que nous souhaitons dire sur les nombres premiers et leur répartition se trouve dans trois chapitres. Ce chapitre introductif contient quelques définitions et explications préliminaires : nous n'avons rien démontré excepté le théorème 1 qui est facile, bien qu'important. Dans le chapitre 2, nous démontrons en particulier les théorèmes 3 et 4 d'Euclide. Le premier de ces théorèmes implique (comme nous l'avons vu en §1.3) le « théorème fondamental de l'arithmétique » (théorème 2), indispensable pour presque toute la suite. Nous en donnons deux démonstrations dans les paragraphes §§2.10–2.11. Nous démontrons le théorème 4 dans les paragraphes §2.1, §2.4 et §2.6, par plusieurs méthodes ; certaines d'entre elles nous permettent d'approfondir ce théorème.

CHAPITRE II

La suite des nombres premiers (2)

2.1 Première démonstration du second théorème d'Euclide

La démonstration initiale d'Euclide pour le théorème 4 est la suivante.

Soit 2, 3, 5, ..., p les nombres premiers jusqu'à p et soit

$$q = 2 \cdot 3 \cdot 5 \cdots p + 1. \tag{2.1.1}$$

Alors q n'est divisible par aucun des nombres 2, 3, 5, ..., p. Donc soit q est premier, soit il est divisible par un nombre premier compris entre p et q. Dans les deux cas, il existe un nombre premier plus grand que p. Ce qui démontre le théorème.

Ce théorème est équivalent à

$$\pi(x) \to \infty. \tag{2.1.2}$$

2.2 Autres conséquences de l'argument d'Euclide

Si p est le n-ième nombre premier p_n et si q est défini comme en (2.1.1), nous avons clairement :

$$q < p_n^n + 1$$

pour tout $n > 1$[†], et par suite

$$p_{n+1} < p_n^n + 1.$$

Cette inégalité permet de borner supérieurement le taux de croissance de p_n et de minorer celui de $\pi(x)$.

Nous pouvons cependant calculer des limites plus précises ainsi. Supposons que

[†]L'égalité a lieu lorsque $n = 1$, $p = 2$ et $q = 3$.

$$p_n < 2^{2^n} \tag{2.2.1}$$

pour $n = 1, 2, \ldots, N$. L'argument d'Euclide montre alors que

$$p_{N+1} \leqslant p_1 p_2 \cdots p_N + 1 < 2^{2+4+\cdots+2^N} < 2^{2^{N+1}}. \tag{2.2.2}$$

Puisque l'inégalité (2.2.1) est vraie pour $n = 1$, elle est vraie pour tout n.

Supposons maintenant que $n \geqslant 4$ et

$$e^{e^{n-1}} < x \leqslant e^{e^n}.$$

Alors[†]

$$e^{n-1} > 2^n, \qquad e^{e^{n-1}} > 2^{2^n};$$

et ainsi

$$\pi(x) \geqslant \pi(e^{e^{n-1}}) \geqslant \pi(2^{2^n}) \geqslant n,$$

d'après (2.2.1). Comme $\log\log x \leqslant n$, nous en déduisons que

$$\pi(x) \geqslant \log\log x$$

pour $x > e^{e^3}$; et il est clair que l'inégalité est aussi vraie pour $2 \leqslant x \leqslant e^{e^3}$. Nous avons donc démontré le

Théorème 10

$$\pi(x) \geqslant \log\log x \qquad (x \geqslant 2).$$

Nous avons ainsi progressé par rapport au théorème 4 et nous avons trouvé un minorant de l'ordre de grandeur de $\pi(x)$. Ce minorant est évidemment très mauvais, puisque pour $x = 10^9$, il donne $\pi(x) \geqslant 3$, alors que la valeur exacte de $\pi(x)$ est au-delà de 50 millions.

2.3 Nombres premiers dans certaines progressions arithmétiques

L'argument d'Euclide peut être utilisé dans d'autres directions.

Théorème 11 *Il existe une infinité de nombres premiers de la forme* $4n + 3$.

Définissons q par la formule :

$$q = 2^2 \cdot 3 \cdot 5 \cdots p - 1,$$

[†]Ceci n'est pas vrai pour $n = 3$.

plutôt que par l'équation (2.1.1). Alors q est de la forme $4n+3$ et il n'est divisible par aucun nombre premier inférieur ou égal à p. Il ne peut être un produit de nombres premiers de la forme $4n+1$ uniquement, puisque le produit de deux nombres de cette forme est de la même forme. Par suite, il est divisible par un nombre premier de la forme $4n+3$ et plus grand que p.

Théorème 12 *Il y a une infinité de nombres premiers de la forme* $6n+5$.

L'argument est similaire : nous définissons q par

$$q = 2 \cdot 3 \cdot 5 \cdots p - 1$$

et nous remarquons que tout nombre premier, excepté 2 ou 3, est de la forme $6n+1$ ou $6n+5$, et que le produit de deux nombres de la forme $6n+1$ est de la même forme.

Les nombres premiers de la forme $4n+1$ sont aussi en nombre infini mais cela est plus difficile à établir. Il faut admettre un théorème que nous démontrons plus loin (§20.3) :

Théorème 13 *Si a et b n'ont pas de diviseur commun, alors tout diviseur premier impair de a^2+b^2 est de la forme $4n+1$.*

En admettant ce résultat, nous pouvons montrer qu'il existe une infinité de nombres premiers de la forme $4n+1$. En fait nous pouvons démontrer le théorème suivant

Théorème 14 *Il existe une infinité de nombres premiers de la forme* $8n+5$.

Nous posons

$$q = 3^2 \cdot 5^2 \cdot 7^2 \cdots p^2 + 2^2,$$

qui est une somme de deux carrés sans diviseur commun. Le carré d'un entier impair $2m+1$ s'écrit

$$4m(m+1)+1$$

et il est donc de la forme $8n+1$, de sorte que q est de la forme $8n+5$. En remarquant que, d'après le théorème 13, tout facteur premier de q est de la forme $4n+1$ et donc de la forme $8n+1$ ou $8n+5$ et que le produit de deux nombres de la forme $8n+1$ est de la même forme, nous terminons la démonstration du théorème comme précédemment.

Tous ces résultats sont des cas particuliers d'un théorème bien connu de Dirichlet.

Théorème 15* (Théorème de Dirichlet) *Si a est strictement positif et si a et b n'ont pas de diviseur commun autre que 1, alors il y a une infinité de nombres premiers de la forme $an + b$.*

La démonstration de ce résultat est trop complexe pour être expliquée dans ce livre. Cependant, il existe des démonstrations plus simples lorsque b est égal à 1 ou à -1.

2.4 Deuxième démonstration du théorème d'Euclide

La seconde démonstration que nous donnons du théorème 4 est due à Pólya. Elle repose sur une propriété des nombres appelés « nombres de Fermat ».

Les nombres de Fermat sont, par définition, les nombres de la forme

$$F_n = 2^{2^n} + 1$$

et donc

$$F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65\,537.$$

Ce sont des nombres très intéressants pour plusieurs raisons. Par exemple, Gauss a démontré que, si F_n est un nombre premier p, alors les polygones réguliers à p côtés sont constructibles à la règle et au compas.

La propriété des nombres de Fermat qui nous est utile est la suivante :

Théorème 16 *Deux nombres de Fermat distincts n'ont pas de diviseur commun autre que 1.*

Soit F_n et F_{n+k} deux nombres de Fermat, avec $k > 0$, tels que

$$m \mid F_n \quad \text{et} \quad m \mid F_{n+k}.$$

Si $x = 2^{2^n}$, alors

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1$$

et, par suite, $F_n \mid F_{n+k} - 2$. Donc

$$m \mid F_{n+k} \quad \text{et} \quad m \mid F_{n+k} - 2;$$

et, par conséquent, $m \mid 2$. Puisque F_n est impair, $m = 1$, ce qui termine la démonstration du théorème.

Nous en déduisons que chacun des nombres $F_1, F_2, \ldots, F_n$ est divisible par un nombre premier impair qui ne divise pas les autres. Il existe donc au moins n nombres premiers impairs inférieurs à F_n. Ceci termine la démonstration du théorème d'Euclide. Nous avons, en outre,

$$p_{n+1} \leqslant F_n = 2^{2^n} + 1$$

et cette inégalité, légèrement meilleure que (2.2.1), fournit manifestement une démonstration du théorème 10.

2.6 Troisième démonstration du théorème d'Euclide

Soient 2, 3, 5, ..., p_j les j plus petits nombres premiers et soit $N(x)$ le nombre d'entiers n plus petits que x qui ne sont divisibles par aucun nombre premier $p > p_j$.

Si nous écrivons un tel n sous la forme

$$n = n_1^2 m,$$

où m n'a aucun facteur carré, *i. e.* n'est pas divisible par le carré d'un nombre premier, nous avons

$$m = 2^{b_1} 3^{b_2} \cdots p_j^{b_j}$$

où les b_j sont tous égaux à 0 ou 1.

Il y a seulement 2^j choix possibles pour les exposants et donc au plus 2^j valeurs différentes de m. De plus, nous avons $n_1 \leqslant \sqrt{n} \leqslant \sqrt{x}$. Il y a donc, au plus, $\sqrt{x}$ valeurs différentes de n_1. Ainsi,

$$N(x) \leqslant 2^j \sqrt{x}. \tag{2.6.1}$$

Si le théorème 4 est faux, le cardinal de l'ensemble des nombres premiers est fini, et nous notons $\{2, 3, 5, \ldots, p_j\}$ l'ensemble de tous les nombres premiers. Dans ce cas, $N(x) = x$ pour tout x et, par suite

$$x \leqslant 2^j \sqrt{x}, \qquad x \leqslant 2^{2j},$$

ce qui est faux pour $x \geqslant 2^{2j} + 1$.

Nous pouvons utiliser ces arguments pour montrer deux résultats supplémentaires.

Théorème 19 *La série*

$$\sum \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots \tag{2.6.2}$$

diverge.

Supposons la série convergente. Nous pouvons alors choisir un j tel que le reste de la série après le j-ième terme est plus petit que $1/2$, *i. e.*

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots < \frac{1}{2}.$$

Le cardinal de l'ensemble des entiers n tels que $n \leqslant x$ qui sont divisibles par p est inférieur ou égal à à x/p. Donc $x - N(x)$, le nombre d'entiers $n \leqslant x$ divisibles par au moins un des nombres $p_{j+1}, p_{j+2}, \ldots$, est inférieur à

$$\frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \cdots < \frac{1}{2}x.$$

Donc, d'après (2.6.1),

$$\frac{1}{2}x < N(x) \leqslant 2^j\sqrt{x}, \qquad x < 2^{2j+2},$$

or ceci est faux pour $x \geqslant 2^{2j+2}$. Donc la série est divergente.

Théorème 20

$$\pi(x) \geqslant \frac{\log x}{2\log 2} \qquad (x \geqslant 1); \qquad p_n \leqslant 4^n.$$

Posons $j = \pi(x)$, de sorte que $p_{j+1} > x$ et $N(x) = x$. Nous avons

$$x = N(x) \leqslant 2^{\pi(x)}\sqrt{x}, \qquad 2^{\pi(x)} \geqslant \sqrt{x}.$$

La première assertion du théorème suit en passant aux logarithmes. Si nous posons $x = p_n$, alors $\pi(x) = n$, et la seconde assertion est immédiate.

D'après le théorème 20, nous avons $\pi(10^9) \geqslant 15$, ce qui est évidemment très loin du compte.

2.9 Modules d'entiers

Donnons à présent la démonstration des théorèmes 3 et 2, que nous avons énoncés en §1.3. Nous en donnerons une autre démonstration en §2.11

. Dans ce paragraphe, entier signifie entier rationnel, positif ou négatif.

La démonstration repose sur la notion de « module » de nombres. Un module est un système S *de nombres tels que la somme et la différence de deux éléments de* S *sont encore des éléments de* S, *i. e.*

$$m \in S \quad \text{et} \quad n \in S \Rightarrow (m \pm n) \in S. \tag{2.9.1}$$

Les nombres d'un module ne sont pas forcément des entiers ni même des nombres rationnels ; ce peut être des nombres complexes ou des quaternions. Ici, nous nous intéressons uniquement à des modules d'entiers.

Le nombre 0 forme un module à lui tout seul (le *module nul*).

Nous déduisons de la définition de S que

$$a \in S \Rightarrow 0 = a - a \in S \quad \text{et} \quad 2a = a + a \in S.$$

En répétant cet argument, nous voyons que $na \in S$ pour tout entier n (positif ou négatif). Plus généralement

$$a \in S \quad \text{et} \quad b \in S \Rightarrow xa + yb \in S$$

pour x et y entiers. D'un autre côté, il est évident que, si a et b sont donnés, l'ensemble des valeurs $xa + yb$ forme un module.

Il est clair que tout module S différent du module nul contient certains nombres strictement positifs. Soit d le plus petit élément strictement positif de S. Si n est

un élément strictement positif quelconque de S, alors $n - zd \in S$ pour tout z. Si c est le reste de la division euclidienne de n par d et

$$n = zd + c,$$

alors $c \in S$ et $0 \leqslant c < d$. Puisque d est le plus petit élément strictement positif de S, $c = 0$ et $n = zd$. Donc

Théorème 23 *Tout module différent du module nul est constitué de tous les multiples d'un nombre strictement positif d.*

Nous définissons le plus grand commun diviseur (PGCD) de deux entiers a et b, non simultanément nuls, comme étant le plus grand entier d positif qui divise à la fois a et b. Nous le notons

$$d = (a, b).$$

Nous avons ainsi $(0, a) = |a|$. Nous définissons de même le plus grand commun diviseur

$$(a, b, c, \ldots, k)$$

d'un ensemble fini quelconque d'entiers positifs a, b, c, ..., k.

L'ensemble des nombres de la forme

$$xa + yb,$$

pour x et y entiers, est un module qui, d'après le théorème 23, est formé des multiples zc d'un certain entier positif c. Puisque c divise tout élément de S, il divise a et b et, par suite,

$$c \leqslant d.$$

D'autre part,

$$d \mid a \quad \text{et} \quad d \mid b \Rightarrow d \mid xa + yb,$$

de sorte que d divise tout élément de S, donc en particulier c. Il s'ensuit que

$$c = d$$

et que S est l'ensemble des multiples entiers de d.

Théorème 24 *Le module $xa + yb$ est formé des multiples de $d = (a, b)$.*

Il est clair que nous avons démontré en passant le

Théorème 25 *L'équation*

$$ax + by = n$$

admet des solutions entières x et y si et seulement si $d \mid n$. En particulier

$$ax + by = d$$

admet des solutions.

Théorème 26 *Tout nombre qui divise à la fois a et b divise également d.*

2.10 Démonstration du théorème fondamental de l'arithmétique

Nous avons maintenant les moyens de démontrer le théorème 3 d'Euclide, et donc le théorème 2.

Soit p un nombre premier qui divise ab. Si $p \not| a$ alors $(a, p) = 1$ et donc, d'après le théorème 24, il existe x et y tels que $xa + yp = 1$, de sorte que

$$xab + ypb = b.$$

Comme $p \mid ab$ et $p \mid pb$, nous en déduisons $p \mid b$.

Un argument similaire montre le

Théorème 27

$$(a, b) = d \quad et \quad c > 0 \Rightarrow (ac, bc) = dc.$$

En effet, il existe x et y tels que $xa + yb = d$ ou encore

$$xac + ybc = dc.$$

Donc $(ac, bc) \mid dc$. En outre, $d \mid a \Rightarrow dc \mid ac$ et $d \mid b \Rightarrow dc \mid bc$ et donc, si nous appliquons le théorème 26, $dc \mid (ac, bc)$. Nous avons donc bien $(ac, bc) = dc$.

2.11 Une autre démonstration du théorème fondamental

Nous appelons *anormal* tout nombre qui peut se décomposer en facteurs premiers de plusieurs manières. Soit n le plus petit entier anormal. Considérons deux décompositions différentes de n. Un nombre premier P ne peut pas apparaître simultanément dans les deux décompositions de n, car sinon n/P serait anormal et $n/P < n$. Nous avons donc

$$n = p_1 p_2 p_3 \cdots = q_1 q_2 \cdots ,$$

où les p et les q sont des nombres premiers, aucun p n'étant un q et inversement. Soit p_1 le plus petit des p ; comme n est composé nous avons $p_1^2 \leqslant n$. De même, si q_1 est le plus petit des q, alors $q_1^2 \leqslant n$; donc, comme $p_1 \neq q_1$, nous avons $p_1 q_1 < n$. Donc, si $N = n - p_1 q_1$, nous avons $0 < N < n$ et N n'est pas anormal. Nous avons $p_1 \mid n$, et donc $p_1 \mid N$ et, de même, $q_1 \mid N$. La factorisation de N en facteurs premiers étant unique et faisant apparaître p_1 et q_1, nous avons $p_1 q_1 \mid N$. Nous en déduisons que $p_1 q_1 \mid n$ et donc que $q_1 \mid n/p_1$. Or n/p est plus petit que n, il admet donc une unique décomposition en facteurs premiers $p_2 p_3 \cdots$. Comme q_1 n'est pas un p, ceci est impossible. Il ne peut donc exister aucun nombre anormal, d'où le théorème fondamental.

FIN