Chapitre 1

THÉORIE DES NOMBRES

1.1 Divisibilité

Soient a et b deux entiers avec $a \neq 0$. On dit que a *divise* b si $b = ac$ pour un certain entier c. On dit aussi que b est divisible par a ou que b est un multiple de a. On note $a|b$ ou $b = \mathcal{M}a$ (b multiple de a).

Proposition 1.1

1) Si $a \mid b$, $b \neq 0$, alors $|a| \leq |b|$.
2) Si $a \mid b$ et $b \mid c$, alors $a \mid (\alpha b + \beta c)$ pour tous entiers α et β.
3) Si $a \mid b$ et $a \mid (b \pm c)$, alors $a \mid c$.
4) $a \mid a$ (réflexivité).
5) Si $a \mid b$ et $b \mid c$, alors $a \mid c$ (transitivité).
6) Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$. □

Théorème 1.1 Division euclidienne

Soient a et b deux entiers avec $a \neq 0$, alors il existe un unique couple (q, r) d'entiers tels que :

$$b \;=\; aq + r, \qquad\qquad 0 \leq r < |a|.$$

Exemple 1.1 (**OIM, 1959**)

Pour tout $n \in \mathbb{N}^*$, la fraction $\dfrac{21n+4}{14n+3}$ est irréductible. □

On a clairement

$$2\,(21n+4) - 3\,(14n+3) \;=\; -1.$$

Donc, tout diviseur commun à $21n+4$ et à $14n+3$ divise 1, donc il est égal à 1, et la fraction est irréductible.

Exemple 1.2 Soit $n \in \mathbb{N}^*$ un entier. Montrer que $3^{2^n}+1$ est divisible par 2 mais n'est pas divisible par 4. □

Il est clair que 3^{2^n} est un entier impair, et par suite $3^{2^n}+1$ est un entier pair. On a :

$$3^{2^n} \;=\; \left(3^2\right)^{2^{n-1}} \;=\; 9^{2^{n-1}} \;=\; (8+1)^{2^{n-1}}.$$

On rappelle que le développement de $(x+y)^m$ est donné par :

$$(x+y)^m \;=\; x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + \cdots + \binom{n}{n-1}xy^{m-1} + y^m.$$

En prenant, dans l'expression ci-dessus, $x = 8, y = 1$ et $m = 2^{n-1}$, on voit que tous les termes du membre de droite (sauf $y^m = 1$) est un multiple de 8 (qui est aussi un multiple de 4), donc le reste de la division de 3^{2^n} par 4 est égal à 1, et le reste de la division de $3^{2^n}+1$ par 4 est égal à 2.
Remarque : on peut aussi raisonner directement modulo 4 en considérant la relation $3^{2^n} = (4-1)^{2^n}$.

Exemple 1.3 Déterminer le plus grand entier $n \in \mathbb{N}^*$ pour lequel n^3+100 est divisible par $n+10$. □

En divisant on a :

$$n^3 + 100 \;=\; (n+10)\left(n^2 - 10n + 100\right) - 900.$$

Donc, si $n+10$ divise n^3+100, alors il doit diviser aussi 900. Comme le plus grand diviseur de 900 est lui-même, alors on doit avoir $n+1 = 900$, c'est-à-dire $n = 899$. La réciproque est claire.

Exemple 1.4 Quels sont les entiers $n \in \mathbb{N}^*$ tels que $\lfloor\sqrt{n}\rfloor$ divise n ? □

Soit $a \in \mathbb{N}^*$ tel que $a^2 \leq n < (a+1)^2$, alors $a \leq \sqrt{n} < a+1$ et $\lfloor\sqrt{n}\rfloor = a$. Comme $\lfloor\sqrt{n}\rfloor \,|n$ alors $n = ab$ avec $b \in \mathbb{N}^*$. De $a^2 \leq n = ab < (a+1)^2$ il résulte que

$$a \;\leq\; b \;<\; \frac{a^2+2a+1}{a} \;=\; a+2+\frac{1}{2} \;\leq\; a+3.$$

Par suite $b \in \{a, a+1, a+2\}$, et les solutions du problème sont a^2, a^2+a, a^2+2a pour $a \in \mathbb{N}^*$.

Exemple 1.5 (**Russie, 1998**)
Soit n un entier naturel non nul. Montrer que tout nombre strictement supérieur à $\frac{n^4}{16}$ peut s'écrire, d'au plus une façon, comme le produit de deux de ses diviseurs ayant une différence $\leq n$. □

Supposons, par l'absurde, qu'il existe $a > c \geq d > b$ tels que :

$$a - b \leq n \qquad \text{et} \qquad ab = cd > \frac{n^4}{16}.$$

On pose $p = a + b$, $q = a - b$, $r = c + d$ et $s = c - d$, alors :

$$p^2 - q^2 = 4ab = 4cd = r^2 - s^2 > \frac{n^4}{4}.$$

D'où, $p^2 - r^2 = q^2 - s^2 \leq q^2 \leq n^2$. Or, $r^2 > \frac{n^4}{4}$ (i.e. $r > n^2/2$) et $p > r$, par suite

$$p^2 - r^2 > \left(\frac{n^2}{2} + 1\right)^2 - \left(\frac{n^2}{2}\right)^2 \geq n^2 + 1$$

contradiction.

Exemple 1.6 (**Russie, 1998**)
Montrer que pour tout entier $n > 1$ il existe trois entiers naturels distincts a, b et c, compris entre n^2 et $(n+1)^2$, et tels que $a^2 + b^2$ est divisible par c. □

En prenant $a = n^2+2$, $b = n^2+n+1$, $c = n^2+1$, on voit que $a^2+b^2 = \big(2n^2 + 2n + 5\big)\, c$.

Exemple 1.7 (**OIM, 1970**)
Déterminer l'ensemble des naturels n tels que l'on puisse décomposer l'ensemble $\{n, n+1, n+2, n+3, n+4, n+5\}$ en deux parties disjointes non vides dont les produits des éléments qui les composent sont égaux. □

Au moins un des six nombres consécutifs est divisible par 5. D'après la condition de l'exercice, il s'ensuit que deux nombres doivent être divisibles par 5. Ces deux nombres sont forcément n et $n + 5$. D'où, n et $n + 5$ sont dans deux ensembles différents. Comme $n(n + 1) > n + 5$ pour $n \geq 3$, il s'ensuit que la partition requise ne peut pas être faite avec des ensembles de cardinalité différente. Donc chacun doit contenir 3 éléments. On considère les deux possibilités suivantes :
(a) $\{n, n+2, n+4\} \cup \{n+1, n+3, n+5\}$,
(b) $\{n, n+3, n+4\} \cup \{n+1, n+2, n+5\}$.

Dans le cas (a), on a : $n < n+1 < n+2 < n+3$, et $n+4 < n+5$, ce qui donne $n(n+2)(n+4) < (n+1)(n+3)(n+5)$, d'où ce cas est impossible.
Dans le cas (b), la condition du problème donne :

$$n(n+3)(n+4) \ = \ (n+1)(n+3)(n+5).$$

On obtient $n^2+5n+10=0$, et cette équation n'a pas de solutions réelles.
En conclusion, le problème n'a pas de solutions.

Exemple 1.8 (**OIM, 1998**)
Déterminer tous les couples (a,b) d'entiers naturels non nuls telles que ab^2+b+7 divise a^2b+a+b. □

Comme ab^2+b+7 divise a^2b+a+b on a aussi ab^2+b+7 divise $b(a^2b+a+b)-a(ab^2+b+7)$. Par suite ab^2+b+7 divise b^2-7a. On distingue trois cas.
Cas 1 : $b^2-7a=0$: alors $b^2=7k$, $a=7k^2$. Pour tout entier $k \geq 1$, les couples $(7k^2,7k)$ sont solutions du problème.
Cas 2 : $b^2-7a>0$: alors $ab^2+b+7 \leq b^2-7a$, et on obtient une contradiction :

$$b^2-7a \ < \ b^2 \ < \ ab^2+b+7.$$

Cas 3 : $b^2-7a<0$: alors $ab^2+b+7 \leq 7a-b^2$. C'est possible seulement si $b^2<7$, c'est-à-dire $b=1$ ou $b=2$.
$\diamond$ Si $b=1$, alors $a+8|a^2+a+1$, c'est-à-dire $a+8|a(a+8)-7(a+8)+57$, d'où $a+8|57$ et on obtient $a+8=19$ ou $a+8=49$, ce qui donne $a=11$ ou $a=49$.
$\diamond$ Si $b=2$, alors on obtient $4a+9|a+22$, ce qui donne $4a+9 \leq a+22$, i.e. $3a \leq 13$, ceci ne donne pas une solution.
En conclusion, les solutions sont : $(7k^2,7k)$, $(11,1)$ et $(49,1)$.

Exemple 1.9 (**OIM, 1992**)
Déterminer tous les entiers a,b,c avec $1<a<b<c$ et tels que $(a-1)(b-a)(c-1)$ est un diviseur de $abc-1$. □

On pose $a-1=x$, $b-1=y$ et $c-1=z$, alors les conditions du problème deviennent : $1 \leq x < y < z$ et $xyz|xy+yz+zx+x+y+z$. L'idée de la démonstration est de prouver qu'on ne peut pas avoir $xyz \leq xy+yz+zx+x+y+z$ pour une infinité de triplets (x,y,z) d'entiers naturels non nuls. On pose

$$f(x,y,z) \ = \ \frac{xy+yz+zx+x+y+z}{xyz} \ = \ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx}.$$

Il est facile de voir que f est décroissante par rapport à l'une de ses variables (les deux autres

étant considérées constantes). Par symétrie, et comme x, y, z sont distincts, alors on a :

$$f(x,y,z) \;\leq\; f(1,2,3) \;=\; 2+\frac{5}{6} \;<\; 3.$$

Donc, on a $f(x,y,z)=1$ ou $f(x,y,z)=2$. On doit donc résoudre les équations :

$$xy+yz+zx+x+y+z \;=\; kxyz \qquad\qquad \text{avec } k=1 \text{ ou } k=2.$$

On a $f(3,4,5)=\dfrac{59}{60}<1$, donc $x\in\{1,2\}$. De plus, $f(2,3,4)=\dfrac{35}{24}<2$, donc pour $x=2$ on a nécessairement $k=1$. On distingue alors les trois cas possibles.
Cas 1 : $x=1$ et $k=1$: on obtient l'équation $1+2(y+z)+yz=yz$, et qui n'a pas de solutions.
Cas 2 : $x=1$ et $k=2$: on obtient l'équation $1+2(y+z)=yz$, c'est-à-dire $(y-2)(z-2)=5$, ce qui donne $y=3$ et $z=7$.
Cas 3 : $x=2$ et $k=1$: on obtient l'équation $2+3(y+z)=yz$, c'est-à-dire $(y-3)(z-3)=11$, ce qui donne $y=4$ et $z=15$.
En conclusion, les seules solutions sont $(a,b,c)=(2,4,8)$ et $(a,b,c)=(3,5,16)$.

Exemple 1.10 (**Roumanie, 1998**)
Déterminer tous les entiers strictement positifs x, n tels que x^n+2^n+1 est un diviseur de $x^{n+1}+2^{n+1}+1$. □

Tout d'abord si $n=1$ on a : $x+3=x+2+1 | x^2+4+1=x^2+5=(x+3)(x-3)+14$. Donc, $x+3$ divise 14, ce qui donne $x=4$ ou $x=11$.
On suppose dans la suite que $n\geq 2$. Pour $x\in\{1,2,3\}$ on a :

$$\begin{aligned}
1+2^n+1 \;&<\; 1+2^{n+1}+1 \;<\; 2\left(1+2^n+1\right)\\
2^n+2^n+1 \;&<\; 2^{n+1}+2^{n+1}+1 \;<\; 2\left(2^n+2^n+1\right)\\
2\left(3^n+2^n+1\right) \;&<\; 3^{n+1}+2^{n+1}+1 \;<\; 3\left(3^n+2^n+1\right).
\end{aligned}$$

Donc, x^n+2^n+1 ne divise pas $x^{n+1}+2^{n+1}+1$ dans ces cas là. Maintenant, pour $x\geq 4$, on a : $x^n=\dfrac{x^n}{2}+\dfrac{x^n}{2}\geq\dfrac{2^{2n}}{2}+\dfrac{x^2}{2}$, d'où

$$\left(2^n+1\right)x \;\leq\; \frac{\left(2^n+1\right)^2+x^2}{2} \;=\; \frac{2^{2n}+2^{n+1}+1+x^2}{2} \;<\; 2^{n+1}+x^n+2^n+2.$$

Par conséquent :

$$\begin{aligned}
(x-1)\left(x^n+2^n+1\right) \;&=\; x^{n+1}+2^n x+x-x^n-2^n-1\\
&<\; x^{n+1}+2^{n+1}+1 \;<\; x\left(x^n+2^n+1\right)
\end{aligned}$$

et par suite $x^n + 2^n + 1$ ne divise pas $x^{n+1} + 2^{n+1} + 1$.
En conclusion, les seules solutions sont $(x, n) = (4, 1)$ et $(x, n) = (11, 1)$.

1.2 Nombres premiers

Définition 1.1 Un entier $p > 1$ est dit *premier* si ses seuls diviseurs sont 1 et lui-même. Un entier $n > 1$ qui n'est pas premier est dit *composé*. □

- ❑ Tout entier $n > 1$ admet au moins un diviseur premier. Si n est premier alors ce diviseur est lui-même. Si n n'est pas premier, on note $a > 1$ son plus petit diviseur. Si a n'est pas premier, alors $a = a_1 a_2$ avec $1 < a_1 \leq a_2 < a$ et $a_1 | n$, contradiction avec la minimalité de a.
- ❑ Si n est un nombre composé, alors il admet un diviseur premier $\leq \sqrt{n}$. En effet, en écrivant $n = ab$ avec $1 < a \leq b$ on voit que $n \geq a^2$, et donc $a \leq \sqrt{n}$.

Théorème 1.2 Théorème d'Euclide
Il existe une infinité de nombres premiers. □

Théorème 1.3 Décomposition en produit de nombres premiers
Tout entier $n > 1$ admet une unique (à une permutation près) décomposition en produit de nombres premiers. □

Exemple 1.11 On suppose que la décomposition en facteurs premiers de l'entier naturel N est donnée par $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ avec $p_1 < p_2 < \cdots < p_n$ et $\alpha_i \geq 1$. Alors, le nombre de diviseurs de N est égal à $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1)$. □

Tout diviseur de N est de la forme $p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ avec $0 \leq \beta_i \leq \alpha_i$. Comme il y a $\alpha_i + 1$ choix possibles pour chaque β_i, le résultat en découle immédiatement.

Exemple 1.12 Montrer que :
(i) 2 est le seul nombre premier pair.
(ii) Hormis 2 et 3, tous les autres nombres premiers sont de la forme $6k \pm 1$. □

Pour le (i) il est clair qu'un nombre > 2 est égal à $2n$ pour un $n > 1$, donc il n'est pas premier. Pour le (ii), tous les entiers sont de la forme

$$6k \pm 2, \qquad 6k \pm 1, \qquad 6k \qquad \text{ou} \qquad 6k + 3.$$

Les deux derniers sont divisibles par 3 (donc non premiers), et le premier est divisible par 2 (donc non premier). Il ne reste que $6k \pm 1$.

Exemple 1.13 Il existe une infinité de nombres premiers de la forme $6k - 1$. (Par exemple : $5, 11, 17, 23, \cdots$). □

On fait un raisonnement par l'absurde. Supposons que p est le plus grand nombre premier de la forme $6k - 1$, et posons $N = p! - 1$. Soit $N = p_1 p_2 \cdots p_k$ la décomposition de N en produit de nombres premiers, alors chacun des p_j est plus grand que p car sinon il diviserait N et $p!$ et donc divise 1, impossible. Comme p est le plus grand premier de la forme $6k - 1$, alors tous les p_j sont de la forme $6k + 1$ (d'après l'exemple précédent), et donc le reste de la division de N par 6 est égal à 1. Or, $N = p! - 1$ admet 5 comme reste lorsqu'il est divisé par 6. Contradiction.

Exemple 1.14 Montrer que si p et $p^2 + 2$ sont premiers, alors $p^3 + 2$ est aussi premier. □

On a affaire içi à un résultat dans un cas particulier, car de tels résultats généraux n'existent pas. Si $p > 3$ est un nombre premier, alors $p^2 + 2$ est de la forme $(6k - 1)^2 + 2 = 36k^2 - 12k + 3$ ou $(6k + 1)^2 + 2 = 36k^2 + 12k + 3$ pour un certain k. Ce ne sont pas des nombres premiers. Si $p = 2$, alors $p^2 + 2 = 6$ qui n'est pas un premier. Donc, forcément $p = 3$, et alors $3^2 + 2 = 11$ et $3^3 + 2 = 29$ sont des nombres premiers.

Exemple 1.15 Soit $p > 3$ un nombre premier, alors 24 divise $p^2 - 1$. □

Comme tous les nombres premiers > 3 sont de la forme $6k \pm 1$ alors $p^2 - 1 = 12k(3k \pm 1)$. Si k est pair, alors 24 divise $p^2 - 1$. Si k est impair, alors $3k \pm 1$ est pair, et donc 24 divise $p^2 - 1$.

Exemple 1.16 Soit n un entier impair, alors $2^n + 1$ n'est jamais premier sauf pour $n = 1$. □

Si $n > 1$ est impair, alors $n = 2k + 1$ avec $k > 0$. Or, on a :

$$x^{2k+1} + y^{2k+1} \;=\; (x + y)\left(x^{2k} - x^{2k-1}y + x^{2k-2}y^2 - \cdots + y^{2k}\right)$$

donc en particulier

$$2^{2k+1} + 1 \;=\; (2 + 1)\left(2^{2k} - 2^{2k-1} + 2^{2k-2} - \cdots + 1\right)$$

et $2^n + 1$ est composé.

Exemple 1.17 (**Grande-Bretagne, 2002**)
On donne

$$34! \;=\; 295\,232\,799\,\,cd9\,\,604\,140\,847\,618\,609\,643\,\,5ab\,\,000\,000.$$

Déterminer la valeur des chiffres a, b, c et d. □

L'idée serait de trouver la décomposition en nombres premiers de 34! (au moins jusqu'à 11 car on connaît les critères de divisibilité par $2, 3, 5, 9$ et 11). Le nombre 7, par exemple, apparaît une fois dans $7, 14, 21$ et 28, donc il apparaît 4 fois dans la factorisation de 34!. Par suite :

$$34! \;=\; K \times 11^3 \times 7^4 \times 5^7 \times 3^{15} \times 2^{32}$$

où K est un produit de nombres premiers > 11. Grâce au facteur 5^7 on voit que 34! admet exactement sept chiffres 0 à la fin, donc $b = 0$ et $a > 0$. En laissant de côté ces 7 chiffres, ce qui reste est divisible par 8, et, comme 1000 est divisible par 8, alors il en est de même pour « $35a$ », par suite $a = 2$. Maintenant on a un diviseur de 9, donc la somme des chiffres est aussi divisible par 9, d'où $c + d$ est égal à 3 ou à 12. Finalement, le critère de divisibilité par 11 nous permet de dire que $d - c = 3$ ou $c - d = 8$. On déduit que $c = 0$ et $d = 3$. En conclusion, $(a, b, c, d) = (2, 0, 0, 3)$.

Exemple 1.18 Pour tout entier $n > 1$, le nombre $n^5 + n^4 + 1$ est composé. □

On a

$$\begin{aligned} n^5 + n^4 + 1 &= n^5 + n^4 + n^3 - n^3 - n^2 - n + n^2 + n + 1 \\ &= n^3\left(n^2 + n + 1\right) - n\left(n^2 + n + 1\right) + \left(n^2 + n + 1\right) \\ &= \left(n^2 + n + 1\right)\left(n^3 - n + 1\right). \end{aligned}$$

Les nombres $n^2 + n + 1$ et $n^3 - n + 1$ sont des entiers > 1, donc $n^5 + n^4 + 1$ est un nombre composé.
Remarque : le nombre complexe $j = \exp\left(\dfrac{2i\pi}{3}\right) = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ est racine « évidente » de $X^5 + X^4 + 1$, ce qui donne la factorisation par $X^2 + X + 1$.

Exemple 1.19 Déterminer tous les entiers naturels non nuls a et b tels que $a^4 + 4b^4$ est un nombre premier. □

On a

$$\begin{aligned} a^4 + 4b^4 &= a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2 \;=\; \left(a^2 + 2b^2\right)^2 - 4a^2b^2 \\ &= \left(a^2 + 2b^2 + 2ab\right)\left(a^2 + 2b^2 - 2ab\right) \;=\; \left[(a+b)^2 + b^2\right]\left[(a-b)^2 + b^2\right]. \end{aligned}$$