Université Paris 12 Janvier 2014
Licences d'Informatique et de Mathématiques
2013-2014

TD de Mathématiques Discrètes
TD 1 - Arithmétique

Fait par : Farah AIT SALAHT

Exercice 1 : Nombres premiers

On note $\mathcal{P}$ l'ensemble des nombres premiers positifs. On rappelle que pour tout entier naturel non nul n, il existe un suite $(v_p(n))_{p\in\mathcal{P}}$ d'entiers naturels nuls sauf un nombre fini d'entre eux vérifiant

$$n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$$

Cette écriture s'appelle la décomposition en facteurs premiers de l'entier n.

1. Donner la décomposition en facteurs premiers des entiers $10, \ldots, 14$.
2. Pour tout entier naturel non nul n, prouver l'unicité de la suite $(v_p(n))_{p\in\mathcal{P}}$.
3. Soient m et n deux entiers naturels non nuls. Donner la décomposition en facteurs premiers des entiers $\text{pgcd}(m,n)$ et $\text{ppcm}(m,n)$ en fonction de la décomposition de m et celle de n.
4. Montrer que $\mathcal{P}$ est infini.
5. Trouver un entier naturel non nul n vérifiant $n! + 1 \notin \mathcal{P}$.
6. Trouver un entier naturel non nul n vérifiant
$$1 + \prod_{\substack{p\in\mathcal{P}\\ p\leq n}} p \notin \mathcal{P}$$
7. Soit n est un entier naturel non nul qui n'appartient pas à $\mathcal{P}$. Établir l'existence d'un entier p vérifiant simultanément $p|n$ et $p^2 \leq n$.

Corrigé :

L'ensembles de tous nombres premiers est noté par $\mathcal{P} = \{2, 3, 5, 7, \ldots\}$. Remarquons que $1 \notin \mathcal{P}$. De plus, 0 et 1 ne sont ni premiers ni composés.
Proposition. Pour tout entier naturel non nul n, il existe une suite $(v_p)_{p\in\mathcal{P}}$ d'entiers naturels nuls sauf un nombre fini d'entre eux vérifiant

$$n = \prod_{p\in\mathcal{P}} p^{v_p} = 2^{v_2} \times 3^{v_3} \times 5^{v_5} \times \ldots$$

Cette écriture s'appelle la **décomposition en facteurs premiers** de l'entier n. La suite $\{v_p\}$ est encore notée $\{v_p(n)\}$.

1. Décomposition de 10 à 14 :
$10 = 2 * 5$, 11 est premier, $12 = 2^2 * 3$, 13 est premier, $14 = 2 * 7$.
2. Preuve de l'unicité de la décomposition :
On suppose l'existence d'un entier naturel non nul n minimal tel qu'il existe deux suites distinctes v_p et v'_p vérifiant $n = \prod_{p\in\mathcal{P}} p^{v_p} = \prod_{p\in\mathcal{P}} p^{v'_p}$. On a $n \geq 2$ car les nombres 0 et 1 ne sont pas composés. On note $p0$ un nombre premier tel que $v_{p0} > 0$. Alors $p0| = \prod_p p^{v_p}$, donc $p0| = \prod_p p^{v'_p}$ de sorte que $v'_{p0} > 0$. On divise par $p0$ les deux écritures de n et on obtient ainsi deux factorisations pour $n/p0$. Ces deux factorisations sont identiques, par minimalité de n. En remultipliant par $p0$, on obtient que les deux factorisations de n sont identiques. Absurde.

3. PGCD(m,n), PPCM(m,n).
   Exemple : $20 = 2^2 * 5$ et $50 = 2 * 5^2$, le $pgcd(20, 50) = 2 * 5$; $200 = 2^3 * 5^2$ et $2500 = 2^2 * 5^4$, le pgcd(200,2500)=$2^2 * 5^2$. Alors le $PGCD(n, m) = \prod_p p^{min(m_p, n_p)}$. En résumé, Vous prenez les plus petit facteurs de chacun (mais qui apparaissent dans les deux).
   Exemple : le PPCM (plus petit multiple commun) $ppcm(20, 50) = 2^2 * 5^2 = 100$ et le $ppcm(200, 2500) = 2^3 * 5^4 = 5000$ ($200 * 25 = 2 * 2500$). Ainsi, $PPCM(n, m) = \prod_p p^{max(m_p, n_p)}$. En résumé, vous prenez les plus grand facteurs de chacun (pas obligé d'apparaître dans les deux), par exemple le $ppcm(15, 20)$ on sait que $20 = 2^2 * 5$ et $15 = 3 * 5$ le ppcm correspondant est $2^2 * 3 * 5 = 60$.
4. Infini
   Soit $\mathcal{P}$ l'ensemble des nombres premiers. On suppose $\mathcal{P}$ est fini et contient n éléments $\{p_1, \ldots, p_n\}$. On considère le nombre $N = 1 + p_1 * p_2 * \ldots p_n$. N est strictement supérieur à tout nombre de $\mathcal{P}$, donc N n'appartient pas à $\mathcal{P}$ et ne peut donc pas être premier. De plus, $N \geq 1$, par définition , N possède au moins un diviseur premier p_k élément de $\mathcal{P}$. Donc
   – a) p_k divise N
   – b) p_k divise $p_1 * p_2 * \ldots p_n$ (puisqu'il en fait parti)
   Ainsi p_k divise $N - p_1 * p_2 * \ldots p_n$ (toute combinaison linéaire à coefficient entiers de ces deux deux nombre, et notamment leur différence), différence qui est égale à 1. Alors p_k divise 1, ce qui est impossible car son seul diviseur est 1 et que 1 n'est pas premier.
   Contradiction.
5. Pour éviter de faire croire aux étudiants que tout nombre du type "je multiplie plein de nombres" + 1 est premier (suite à la démonstration précédente). "N = 4", alors $N! = 24$ donc $N! + 1 = 25$ et 25 n'est pas premier.
6. Pour éviter l'adaptation du genre "il suffit de prendre que des nombres premiers" + 1, comme la démonstration précédente. Il faut monter à 13 : $2 * 3 * 5 * 7 * 11 * 13 + 1 = 30031 = 59 * 509$.
7. $p^2 \leq n$
   On choisit un entier n différent de 0 et de 1 et non-premier. On nomme p sont plus petit diviseur autre que 1, on a $1 < p < n$. Comme p divise n, il existe q tel que $pq = n$. q n'est pas nul car $n \neq 0$, q n'est pas 1 car $n \neq p$, donc $q > 1$. Comme $p > 1$, $pq > q$, donc $n > q$. Ainsi, $1 < q < n$ et q divise n. Comme p est le plus petit diviseur et que q est aussi diviseur, $p \leq q$. Donc $p^2 \leq pq$. Donc $p^2 \leq n$.

Exercice 2 : Indicateur d'Euler

Montrer qu'il existe une infinité de nombres premiers de la forme $6k - 1$, avec $k \in \mathbb{N}^*$.

Corrigé :

1.

► Comme le reste dans une division par 6 peut etre 0, 1, 2, 3, 4 ou 5, tout entier naturel est nécessairement de la forme $6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$ ou $6k + 5$.

– S'il est de la forme $6k$, il n'est jamais premier car il est divisible par 6.
– S'il est de la forme $6k + 2$, il n'est jamais premier (sauf si $k = 0$) car il est divisible par 2 et n'est pas égal a 2.
– S'il est de la forme $6k + 3$, il n'est jamais premier (sauf si $k = 0$) car il est divisible par 3 et n'est pas égal a 3.
– S'il est de la forme $6k + 4$, il n'est jamais premier car il est divisible par 2 (et different de 2).

Conclusion : un nombre premier strictement supérieur a 3 est nécessairement de la forme $6k + 1$ ($k \geq 1$) ou $6k + 5$ ($k \geq 0$).
Comme $6k + 5 = 6(k + 1) - 1 = 6K - 1$, on peut finalement dire que tout nombre premier est nécessairement de la forme $6k + 1$ ou $6k - 1$, avec $k \geq 1$.

▶ Remarquons d'abord que tout nombre premier p tel que $p \neq 2$ et $p \neq 3$ est, $k \in \mathbb{N}^*$, soit de la forme $6k+1$ soit de la forme $6k-1$. Pour le montrer, considérons un nombre premier p qui n'est ni 2, ni 3. Sa classe modulo 6 ne peut valoir que -1 ou 1. En effet, si elle valait 0, 6 diviserait p, qui ne serait donc pas premier. Si elle valait 2, 2 diviserait p, mais p est premier différent de 2. Si elle valait 3, 3 diviserait p, mais p est premier différent de 3. Enfin, si elle valait 4, 2 diviserait p, ce qui conduit encore une fois à une contradiction. Donc finalement, la classe de p modulo 6 vaut -1 ou 1.

2.
Maintenant, montrons qu'il y a une infinité de nombre premier de la forme $6k-1$. Supposons qu'il n'y a qu'un nombre fini de nombres premiers de la forme $6k-1$, avec $k \in \mathbb{N}^*$. On note N le plus grand d'entre eux. $M = 6N! - 1$, ce nombre est impair, donc n'est pas divisible par 2. De plus, M vaut $-1 mod o 3$, donc 3 ne le divise pas. Soit p un facteur premier de M. Si p est de la forme $6k-1$, on a $p \leq N$, donc p divise $6N!$, puis p divise $6N! - M = 1$. Impossible. Donc p n'est pas de la forme $6k-1$. Comme p ne peut valoir ni 2, ni 3, il est de la forme $6k+1$ (voir remarque au début de l'exercice). Dans la décomposition de M en facteurs premiers, $p_1 \dots p_n$, on a $p_i = 1 mod 6$, donc $M = 1 mod 6$. Absurde, car $M = -1 mod 6$ par construction.

Exercice 3 : $\mathrm{pgcd}(a^n - 1, a^m - 1)$

Soient $a, m, n \in \mathbb{N}^*$, $a \geq 2$, et $d = \mathrm{pgcd}(a^n - 1, a^m - 1)$.

1. Soit $n = qm + r$ la division euclidienne de n par m. Démontrer que $a^n \equiv a^r (\mathrm{mod}\, a^m - 1)$.
2. En déduire que $d = \mathrm{pgcd}(a^r - 1,\, a^m - 1)$, puis que $d = a^{\mathrm{pgcd}(n,\, m)} - 1$.
3. À quelle condition $a^m - 1$ divise-t-il $a^n - 1$?

Corrigé :

1. On a $a^n = a^{qm+r} = a^r(a^{mq} - 1) + a^r$ et

$$a^{mq} - 1 = (a^m)^q - 1 = (a^m - 1)\sum_{k=0}^{q-1}(a^m)^k \tag{1}$$

donc $a^{mq} - 1$ est divisible par $a^m - 1$ ainsi $a^n \equiv a^r (\mathrm{mod}\, a^m - 1)$.
On peut également remarquer que $a^m \equiv 1 (\mathrm{mod}\, a^m - 1)$ donc $a^{qm} \equiv 1 (\mathrm{mod}\, a^m - 1)$ donc $a^{qm+r} \equiv a^r (\mathrm{mod}\, a^m - 1)$ i.e. $a^n \equiv a^r (\mathrm{mod}\, a^m - 1)$.

2. a)
De l'équation 1 nous avons

$$a^n - 1 = a^r\ (a^m - 1)\left(\sum_{k=0}^{q-1}(a^m)^k\right) + a^r - 1.$$

donc $a^n - 1 = a^r - 1 (\mathrm{mod}\, a^m - 1)$ et $0 \leq a^r - 1 \leq a^m - 1$ car $r < q$ et $a > 1$.
On sait que d divise $a^n - 1$ et $a^m - 1$ donc, d'après l'équation ci-dessus, d divise $a^r - 1$. Par conséquent,

$$d = \mathrm{pgcd}(a^r - 1,\, a^m - 1)$$

b)
On définit la suite d'entiers (r_k) par $r_0 = n$, $r_1 = m$ et si r_{k+1} est non nul, r_{k+2} est le reste de la division euclidienne de r_k par r_{k+1} i.e. on applique l'algorithme d'Euclide à n et m. On sait qu'il existe K tel que $a_K = \mathrm{pgcd}(n, m)$ et $a_{K+1} = 0$. D'après ce qui précède, on démontre par récurrence que $(a^{r_k} - 1)$ est la suite des entiers définis par l'algorithme d'Euclide appliqué à $a^n - 1$ et $a^m - 1$. Comme $a^{r_{K+1}} - 1 = 0$, c'est que $a^{r_K} - 1 = a^{\mathrm{pgcd}(n,m)} - 1$ est le pgcd de $a^n - 1$ et $a^m - 1$.

3. $a^m - 1$ divise $a^n - 1$ si et seulement si

$$\text{pgcd}(a^n - 1, a^m - 1) = a^m - 1 \iff a^{\text{pgcd}(n,m)} - 1 = a^m - 1.$$

Comme $a > 1$, cela signifie que $\text{pgcd}(n, m) = m$ i.e. m divise n.

Exercice 4

1. On admet que 1999 est premier. Déterminer l'ensemble des couples (a, b) d'entiers naturels vérifiant simultanément $a + b = 11994$ et $\text{pgcd}(a, b) = 1999$.
2. Déterminer l'ensemble des couples (a, b) d'entiers naturels non nuls vérifiant $\text{pgcd}(a, b) + \text{ppcm}(a, b) = b + 9$.
3. Même question avec $2\,\text{ppcm}(a, b) + 7\,\text{pgcd}(a, b) = 111$.

Corrigé :