

TD4 - Théorie des nombres

Corrigé

1 Nombre premiers

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 n_p et n'_p vérifiant $n = \prod_p p^{n_p} = \prod_p p^{n'_p}$. On a $n \geq 2$. On note p_0 un nombre premier tel que $n_{p_0} > 0$. Alors $p_0 | \prod_p p^{n_p}$, donc $p_0 | \prod_p p^{n'_p}$, de sorte que $n'_{p_0} > 0$. On divise par p_0 les deux écritures de n et on obtient ainsi deux factorisations pour n/p_0 . Ces deux factorisations sont identiques, par minimalité de n . En remultipliant par p_0 , on obtient que les deux factorisations de n sont identiques. Absurde.

3. PGCD(m,n), PPCM(m,n).

$\text{PGCD}(m,n) = \prod_p p^{\min(m_p, n_p)}$. En résumé, Vous prenez les plus petit facteurs de chacun (mais qui apparaissent dans les deux). Exemple $200 = 2^3 * 5^2$, $2500 = 2^2 * 5^4$, alors le PGCD est $2^2 * 5^2 = 100$.

$\text{PPCM}(m,n) = \prod_p p^{\max(m_p, n_p)}$. En résumé, vous prenez les plus grand facteurs de chacun (pas obligé d'apparaître dans les deux). Exemple, PPCM est $2^3 * 5^4 = 5000$.

Remarque : on a bien $200 * 2500 = 100 * 5000$.

4. Infini

Soit P l'ensemble des nombres premiers. On suppose P fini, contenant les n éléments $\{p_1, \dots, p_n\}$. On considère le nombre $N = 1 + p_1 * p_2 * \dots * p_n$. N est strictement supérieur à tout nombre de P , donc N ne peut pas être premier. N admet donc au moins un diviseur premier p_k élément de P . Donc

(a) p_k divise N

(b) p_k divise $p_1 * p_2 * \dots * p_n$ (puisque'il en fait parti)

Donc p_k divise $N - p_1 * p_2 * \dots * p_n$, différence qui est égale à 1. Donc 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 a 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 son 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 $p^2 \leq n$.

2 Indicateurs d'Euler

1. Calcul :

$$\varphi(15) = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$$

$$\varphi(16) = |\{1, 3, 5, 7, 9, 11, 13, 15\}| = 8$$

$$\varphi(17) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}| = 14$$

$$\varphi(18) = |\{1, 5, 7, 11, 13, 17\}| = 6$$

$$\varphi(19) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}| = 18$$

Remarque : Pour un nombre premier $\varphi(n) = n - 1$.

2. Vérification :

Diviseur de 10 : $\{1, 2, 5, 10\}$. Diviseur de 11 : $\{1, 11\}$. Diviseur de 12 : $\{1, 2, 3, 4, 6, 12\}$. Diviseur de 13 : $\{1, 13\}$. Diviseur de 14 : $\{1, 2, 7, 14\}$.

$$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(10) = 4, \varphi(11) = 10, \varphi(12) = 4, \varphi(13) = 12, \varphi(14) = 6.$$

$$\text{Pour } n = 10 : 10 = \varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4.$$

Pareil pour le reste.

3. Démonstration :

On considère les n fractions suivantes $1/n, 2/n, \dots, (n-1)/n, n/n$. On cherche à les mettre sous forme irréductible a/d , avec $\text{pgcd}(a, d) = 1$. On a nécessairement $d|n$. L'ensemble des d forme donc l'ensemble des diviseurs de n . Pour chaque d , il y a $\varphi(d)$ numérateurs a qui apparaissent. Donc si on considère un sous-ensemble constitué des fractions de dénominateur d , il contient $\varphi(d)$ éléments. Le nombre total de fraction est n , de manière évidente la somme des cardinaux de chaque sous-ensemble est n aussi donc on en déduit le résultat.

3 Algorithme d'Euclide

1. Démonstration :

Prenons deux nombres entiers a et b dont l'on cherche le PGCD d . En utilisant la division euclidienne, on a $a = qb + r$ (q est le quotient et r le reste). Par définition, $a \bmod b = r$. Donc $a \bmod b = a - qb$. Par définition toujours, d divise a et d divise b , donc d divise $a \bmod b$. Comme d est le plus grand diviseur commun de a et b , alors il l'est aussi pour b et $a \bmod b$.

2. Exemple :

$$\text{pgcd}(325, 214) = \text{pgcd}(214, 111) = \text{pgcd}(111, 103) = \text{pgcd}(103, 8) = \text{pgcd}(8, 7) = \text{pgcd}(7, 1) = \text{pgcd}(1, 0) = 1.$$

$$\text{pgcd}(1170, 1326) = \text{pgcd}(1326, 1170) = \text{pgcd}(1170, 156) = \text{pgcd}(156, 78) = \text{pgcd}(78, 0) = 78.$$

4 Exercices

1. $\text{pgcd}(a,b)=1999$

On cherche les couples $(a;b)$ tels que :

$$\begin{cases} a + b = 11994 \\ \text{pgcd}(a, b) = 1999 \end{cases}$$

Nous avons :

$$\begin{cases} a = 1999a' \\ b = 1999b' \\ \text{pgcd}(a', b') = 1 \end{cases}$$

Donc $a + b = 11994$ équivaut à $1999a' + 1999b' = 11994$. Soit :

$$\begin{cases} a' + b' = 6 \\ \text{pgcd}(a', b') = 1 \end{cases}$$

D'où $(a'=1 \text{ et } b'=5)$ ou $(a'=5 \text{ et } b'=1)$. Il s'ensuit $(a=1999 \text{ et } b=9995)$ ou $(a=9995 \text{ et } b=1999)$.

2. $\text{pgcd}(a,b)=\text{ppcm}(a,b)=b+9$

On pose $\text{pgcd}(a, b) = d$ et $\text{ppcm}(a, b) = m$. L'équation devient $d + m = b + 9$.

Nous avons $a = da'$ et $b = db'$ avec $\text{pgcd}(a', b') = 1$. Sachant que $dm = ab$, alors

$$\begin{aligned} dm &= a'd * b'd \\ m &= \frac{a'd * b'd}{d} \\ m &= a'b'd \end{aligned}$$

On peut alors écrire :

$$\begin{aligned} d + a'b'd &= db' + 9 \\ d(1 + a'b') &= db' + 9 \end{aligned}$$

d divise $d(1 + a'b')$ et db' , donc d divise 9. Donc $d=1$ ou $d=3$ ou $d=9$.

(a) $d=1$:

$$\begin{aligned} 1 + m &= b + 9 \\ m &= b + 8 \\ ab &= b + 8 \\ b(a - 1) &= 8 \end{aligned}$$

Donc b divise 8, donc les couples sont $(a=9, b=1)$, $(a=5, b=2)$ et $(a=3, b=4)$.

(b) $d=3$:

$$\begin{aligned} 3 + m &= b + 9 \\ m &= b + 6 \\ \frac{ab}{3} &= b + 6 \\ ab &= 3b + 18 \\ b(a - 3) &= 18 \end{aligned}$$

Donc b divise 18, donc il n'y a qu'un couple $(a=9, b=3)$.

(c) $d=9$

En remplaçant de la même manière on obtient $b(a - 9) = 0$. Comme $b \neq 0$, alors $a = 9$ et $b = 9k$, $k \in \mathbb{N}^*$ tel que $m = 9k$, $d = 9$, $m + d = 9 + b$.

3. $2\text{ppcm}(a,b)+7\text{pgcd}(a,b)=111$

Même type de correction. On obtient $d = 1$ ou $d = 3$ ou $d = 37$. Ensuite :

(a) $d=1 \Rightarrow (a=1, b=52)$ ou $(a=4, b=13)$ et inversement (4 solutions)

(b) $d=3 \Rightarrow (a=3, b=45)$ ou $(a=9, b=15)$ et inversement (4 solutions)

(c) Impossible