

TD5 - Théorie des nombres

Corrigé

Exercice 1 : Nombres de Mersenne, nombres de Fermat

1. *Nombres de Mersenne.* On a $a^n - 1 = (a - 1)(1 + a + \dots + a^{n-1})$ et $a^n - 1$ premier, donc $a - 1 = 1$, puis $a = 2$. Écrivons ensuite $n = pq$. L'entier $2^n - 1 = (2^q)^p - 1 = (2^q - 1)(1 + 2^q + \dots + 2^{q(p-1)})$ est premier, donc l'un des deux facteurs vaut 1, ce qui entraîne $q = 1$ ou $q = n$. Donc n est premier.
2. *Nombres de Fermat.* Si n est impair, on a $x^n + 1 = (x + 1)(1 - x + x^2 - \dots + x^{n-1})$, donc $x + 1$ divise $x^n + 1$. Si n n'est pas une puissance de 2, il a au moins un facteur impair $p > 1$. On écrit $n = pq$. Alors $2^n + 1 = (2^q)^p + 1 = (2^q + 1)(1 - 2^q + 2^{q \cdot 2} - \dots + 2^{q(n-1)})$ est divisible par $2^q + 1$, donc non premier. n doit donc être une puissance de 2.
3. Pour montrer que deux nombres sont premiers entre eux, montrons que leur pgcd est 1. Soient $n \in \mathbb{N}$ et $k \in \mathbb{N}^*$. On a $F_{n+k} - 1 = 2^{2^{n+k}} - 1 = (2^{2^n})^{2^k} - 1 = (F_n - 1)^{2^k}$. Comme $(F_n - 1)^{2^k} = \sum_{i=0}^{2^k} \binom{2^k}{i} F_n^{2^k-i} (-1)^i$, on a $(F_n - 1)^{2^k} \equiv 1 \pmod{F_n}$. Donc, modulo F_n , on a $F_{n+k} \equiv 2$. On note d le pgcd de F_n et F_{n+k} . On a $d = \text{pgcd}(F_{n+k}, F_n) = \text{pgcd}(F_n, F_{n+k} \pmod{F_n}) = \text{pgcd}(F_n, 2)$. Comme F_n est impair, on a $d = 1$. Donc les F_n sont premiers entre eux deux à deux.

Autre démonstration du fait qu'il y ait une infinité de nombre premier. Pour tout $n \in \mathbb{N}$, notons p_n un facteur premier de F_n . Comme les F_n sont premiers entre eux deux à deux, les p_n sont distincts. Comme il y a une infinité de nombre F_n , on a donc une infinité de nombres premiers.

Exercice 2

Remarquons d'abord que tout entier est égal modulo 9 à la somme de ses chiffres en base 10, puisque $10^i \equiv 1 \pmod{9}$, pour tout $i \in \mathbb{N}$. Donc, modulo 9, les nombres A , B , C et 4444^{4444} sont égaux. Or, modulo 9, $4444 \equiv 4 + 4 + 4 + 4 \equiv -2$ et $4444 \equiv 3 \cdot 1481 + 1$, donc modulo 9, $4444^{4444} \equiv ((-2)^3)^{1481} \cdot (-2) \equiv (-8)^{1481} \cdot (-2) \equiv -2$. Donc $C \equiv 7 \pmod{9}$. Ensuite, comme $4444^{4444} \leq 10000^{5000} = 10^{20000}$, il a au plus 20000 chiffres, donc A vaut au plus $9 \cdot 20000 = 180000$, donc a au plus 6 chiffres. Donc B vaut au plus $6 \cdot 9 = 54$, d'où $C \leq 5 + 9 = 14$. Il en ressort que $C = 7$.

Exercice 3

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 .

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. $M = -1 + 6N!$ est impair, donc n'est pas divisible par 2. De plus, M vaut -1 modulo 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 $p_i \equiv 1 \pmod{6}$, donc $M \equiv 1 \pmod{6}$. Absurde, car $M \equiv -1 \pmod{6}$ par construction.

Exercice 4 : Nombres parfaits

1. On écrit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. On a

$$\sigma(n) = \sum_{0 \leq \beta_1 \leq \alpha_1, \dots, 0 \leq \beta_k \leq \alpha_k} p_1^{\beta_1} \dots p_k^{\beta_k} = \prod_{i=1}^k (1 + p_i + \dots + p_i^{\alpha_i}) = \prod_{i=1}^k \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$$

D'où, $\sigma(mn) = \sigma(m)\sigma(n)$, lorsque m et n sont premiers entre eux.

2. Comme $2^p - 1$ est premier, il n'a que deux diviseurs 1 et lui-même. Donc $\sigma(2^p - 1) = (2^p - 1) + 1 = 2^p$. En appliquant la formule précédente, on a $\sigma(2^{p-1}) = 2^p - 1$. Donc, d'après la question précédente, $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = 2n$.
3. Comme n est pair, on écrit $n = 2^{p-1}m$, avec $p \geq 2$ et m impair. Alors $\sigma(n) = \sigma(2^{p-1})\sigma(m) = (2^p - 1)\sigma(m)$. Or, comme n est parfait, on a aussi $\sigma(n) = 2n = 2^p m$. Donc $2^p m = (2^p - 1)\sigma(m)$ et ainsi on obtient que $2^p - 1$ divise $2^p m$. Comme $2^p - 1$ et 2^p sont premiers entre eux, $2^p - 1$ divise m . On écrit donc $m = (2^p - 1)\ell$. Revenons à $2^p m = \sigma(n) = (2^p - 1)\sigma(m)$. On a donc $(2^p - 1)\sigma(m) = 2^p(2^p - 1)\ell$, et ainsi $\sigma(m) = 2^p \ell = 2^p \ell - \ell + \ell = (2^p - 1)\ell + \ell = m + \ell$. Si $\ell > 1$, m a au moins trois diviseurs distincts, qui sont 1, ℓ et m , donc $\sigma(m) \geq m + \ell + 1$. Absurde, donc $\ell = 1$, $m = 2^p - 1$ et $\sigma(m) = m + 1$, donc les seuls diviseurs de m sont m et 1. m est donc premier.

Exercice 5 : Théorème de Liouville

Soit m une solution. Comme $p > 5$, on a $(p-1)! + 1$ impair, donc p^m est impair, puis p impair. En outre, $2 < \frac{p-1}{2} < p-1$ et $\frac{p-1}{2} \in \mathbb{N}$ car p est impair, donc $(p-1)^2 = 2(\frac{p-1}{2})(p-1)$ divise $(p-1)!$. On a de plus $(p-1)! = p^m - 1 = (p-1)(1 + p + \dots + p^{m-1})$, donc $p-1$ divise $1 + p + \dots + p^{m-1}$. Modulo $p-1$, on a donc $0 = 1 + 1 + \dots + 1^{m-1} = m$. En particulier, $m \geq p-1$, puis $p^m \geq p^{p-1} > (p-1)^{p-1} > (p-1)!$, puis $(p-1)! + 1 < p^m$. Absurde.

Exercice 6 : Algorithme d'Euclide étendu

1. $\text{pgcd}(49, 72) = 1$:

- $\text{PGCD}(72 ; 49) = \text{PGCD}(49 ; 23)$ car $72 = 49 \times 1 + 23$
- $\text{PGCD}(49 ; 23) = \text{PGCD}(23 ; 3)$ car $49 = 23 \times 2 + 3$
- $\text{PGCD}(23 ; 3) = \text{PGCD}(3 ; 2)$ car $23 = 3 \times 7 + 2$
- $\text{PGCD}(3 ; 2) = \text{PGCD}(2 ; 1)$ car $3 = 2 \times 1 + 1$
- $\text{PGCD}(2 ; 1) = \text{PGCD}(1 ; 0)$ car $2 = 1 \times 2 + 0$

2. Bezout, $au + bv = \text{pgcd}(a, b)$. La formule est $u = v'$ et $v = u' - \left\lfloor \frac{a}{b} \right\rfloor v'$, ce qui permet le calcul récursif des valeurs:

$a = 72$	$b = 49$	$u = -17$	$v = 25$
49	23	8	-17
23	3	-1	8
3	2	1	-1
2	1	0	1
1	0	1	0

3. L'inverse existe car $\text{pgcd}(49, 72) = 1$. Une fois que l'on a $72 \times -17 + 49 \times 25 = 1$, on a facilement que $49 \times 25 \equiv 1[72]$.

4. Refaire les questions 1 et 2...

(a) Pour 436 et 237:

- $\text{PGCD}(436 ; 237) = \text{PGCD}(237 ; 199)$ car $436 = 237 \times 1 + 199$
- $\text{PGCD}(237 ; 199) = \text{PGCD}(199 ; 38)$ car $237 = 199 \times 1 + 38$
- $\text{PGCD}(199 ; 38) = \text{PGCD}(38 ; 9)$ car $199 = 38 \times 5 + 9$
- $\text{PGCD}(38 ; 9) = \text{PGCD}(9 ; 2)$ car $38 = 9 \times 4 + 2$
- $\text{PGCD}(9 ; 2) = \text{PGCD}(2 ; 1)$ car $9 = 2 \times 4 + 1$
- $\text{PGCD}(2 ; 1) = \text{PGCD}(1 ; 0)$ car $2 = 1 \times 2 + 0$

Donc $\text{pgcd}(436, 237) = 1$

Solution particulière de l'équation $436u + 237v = 1$ où $1 = \text{pgcd}(436, 237)$

- $436 = 1 \times 237 + 199$, $199 = 1 \times 436 - 1 \times 237$
- $237 = 1 \times 199 + 38$, $38 = -1 \times 436 + 2 \times 237$
- $199 = 5 \times 38 + 9$, $9 = 6 \times 436 - 11 \times 237$
- $38 = 4 \times 9 + 2$, $2 = -25 \times 436 + 46 \times 237$
- $9 = 4 \times 2 + 1$, $1 = 106 \times 436 - 195 \times 237$

Solution particulière : (106, -195)

Solution particulière de l'équation $436u + 237v = 1$: (106, -195)

(b) Pour 534 et 408

- $\text{PGCD}(534 ; 408) = \text{PGCD}(408 ; 126)$ car $534 = 408 \times 1 + 126$
- $\text{PGCD}(408 ; 126) = \text{PGCD}(126 ; 30)$ car $408 = 126 \times 3 + 30$
- $\text{PGCD}(126 ; 30) = \text{PGCD}(30 ; 6)$ car $126 = 30 \times 4 + 6$
- $\text{PGCD}(30 ; 6) = \text{PGCD}(6 ; 0)$ car $30 = 6 \times 5 + 0$

Donc $\text{pgcd}(534, 408) = 6$

Solution particulière de l'équation $534u + 408v = 6$ où $6 = \text{pgcd}(534, 408)$

- $534 = 1 \times 408 + 126$, $126 = 1 \times 534 - 1 \times 408$
- $408 = 3 \times 126 + 30$, $30 = -3 \times 534 + 4 \times 408$
- $126 = 4 \times 30 + 6$, $6 = 13 \times 534 - 17 \times 408$

Solution particulière : (13, -17)

Solution particulière de l'équation $534u + 408v = 6$: (13, -17)

5. Les inverses

(a) Résoudre $169x \equiv 1[420]$

Faisable car $\text{pgcd}(169, 420) = 1$

Solution particulière de l'équation $169u + 420v = 1$: (169, -68)

Donc, on a $169 \times 169 \equiv 1[420]$

- (b) Résoudre $187x \equiv 1[420]$
 Faisable car $\text{pgcd}(187, 420) = 1$
 Solution particulière de l'équation $187u + 420v = 1 : (-137, 61)$
 Donc on a $187 \times -137 \equiv 1[420]$, autrement dit $187 \times 283 \equiv 1[420]$
- (c) Résoudre $338x \equiv 1[420]$
 Impossible, car $\text{pgcd}(338, 420) = 2$ (donc pas inversible dans $\mathbb{Z}/420\mathbb{Z}$)
- (d) Résoudre $209x \equiv 1[420]$
 Faisable car $\text{pgcd}(209, 420) = 1$
 Solution particulière de l'équation $209u + 420v = 1 : (209, -104)$
 Donc on a $209 \times 209 \equiv 1[420]$

Exercice 7 : Congruences

1. Résoudre $7x \equiv 2[9]$

Le solution existe car 7 est premier, donc 7 est premier avec 9, donc leur pgcd divise 2, la solution cherchée. Solution particulière de l'équation $7u + 9v = 1 : (4, -3)$. On a donc $7u \equiv 1[9]$, mais aussi $7x \equiv 2[9]$. On a donc $7ux \equiv 2u[9]$ et donc $x \equiv 2u[9]$. Finalement, $x \equiv 8[9]$.

2. Résolution du système:

Les deux équations admettent individuellement une solution car 7 et 11 sont premier.

- (a) Première étape, résoudre $3x \equiv 2[11]$. Solution particulière de l'équation $3u + 11v = 1 : (4, -1)$. On a donc $3 \times 4 \equiv 1[11]$. Comme on cherche $3x \equiv 2[11]$, on trouve $3 \times (4 \times 2) \equiv 2[11]$ et $3 \times 8 \equiv 2[11]$. Finalement $x \equiv 8[11]$.
- (b) Etape intermédiaire, le changement de variable. $x \equiv 8[11]$ s'écrit aussi comme $x = 11k + 8$. Si on substitue dans la deuxième congruence, on obtient $3 \times (11k + 8) \equiv 4[7]$ et finalement $5k \equiv 1[7]$.
- (c) Deuxième étape, résoudre $5k \equiv 1[7]$. Solution particulière de l'équation $5u + 7v = 1 : (3, -2)$. On a donc $5 \times 3 \equiv 1[7]$. Finalement, $k \equiv 3[7]$.
- (d) Etape finale, le changement de variable à l'envers. On $x = 11(3 + 7k') + 8$, donc $x = 41 + 77k'$ et solution finale $x \equiv 41[77]$.

Exercice 8 : Théorème de Wilson

Démonstration 1: Courte, mais notion a priori hors cours?

Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps fini. Donc le produit de tous les éléments non nuls est égal à -1 (propriété des corps finis). Autrement dit, $1 \times 2 \times \dots \times p-1 \equiv -1[p]$ et $(p-1)! \equiv -1[p]$.

Démonstration 2: Utilise simplement la congruence (mais beaucoup plus long).¹

1. Si $(p-1)! \equiv -1[p]$, alors p est premier :

En effet, si p est *non premier*, il admet au moins un diviseur d tel que $1 < d < p$ et par conséquent $p = kd$ avec également $1 < k < p$.

- Si k et d sont distincts, k et d sont alors présents dans la liste $1, 2, 3, \dots, (p-1)$ et il suit que $(p-1)!$ est divisible par p , donc que $(p-1)! \equiv 0[p]$.

¹Source: http://serge.mehl.free.fr/anx/th_wilson.html

- Si k et d sont égaux, alors $p = k^2$. Si k est non premier, on peut se ramener au cas ci-dessus. Une difficulté surgit si k est premier : il est clair cependant que k est présent dans la liste $1, 2, 3, \dots, (p-1)$. Montrons alors que l'on rencontre un multiple de k dans la liste $(k+1)(k+2)\dots(p-1)$. On a $p-1 = k^2-1 = (k+1)(k-1)$.
 - Si $k > 2$, alors $p-1 \geq 2k$, car $k+1 > k$ et c'est gagné : le double de k , au moins, figure dans la liste.
 - Si $k = 2$, alors $p = 4$ et $(p-1)! = 6$. Or $6 \equiv 2[4]$ et non pas -1 (équivalent à 3)

En conclusion, si p n'est pas premier, $(p-1)!$ ne peut être congru à $-1 [p]$. On a donc ainsi prouvé, par contraposition, notre proposition.

2. Si p est premier, alors $(p-1)! \equiv -1[p]$:

- si $p = 2$, c'est gagné : le cas est trivial car $(2-1)! = 1$ et $1 \equiv -1[2]$
- Pour $p > 2$, considérons la liste de facteurs $2, 3, \dots, p-2$ extraites du produit $(p-1)!$. Nous avons un nombre pair $p-3$ de valeurs car p est premier supérieur à 2 . Montrons que l'on peut associer à tout facteur x de la liste un unique facteur y de la liste autre que x de sorte que $xy \equiv 1[p]$.
 - Unicité : si $xy \equiv 1[p]$ et si $xz \equiv 1[p]$, alors $x(y-z) \equiv 0[p]$. Comme p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est intègre (pas de diviseurs de 0), donc $x \equiv 0$ (à rejeter) ou $(y-z) \equiv 0$, c'est dire que $y \equiv z[p]$ et comme y et z sont inférieurs à p , il suit que $y = z$.
 - Existence : pour k vérifiant $2 \leq k \leq p-2$, considérons la liste $k, 2k, 3k, \dots, k(p-1)$. Tous ces produits sont distincts et non nuls. Ils le sont aussi (distincts et non nuls) modulo p puisque p est premier (supposer $ak = bk[p]$ et raisonner comme précédemment) et forment donc une suite de $p-1$ nombres modulo p , à savoir $1, 2, \dots, (p-1)$. Un seul de ces produits vaut 1 modulo p .
 - * Ce n'est pas k puisque $2 \leq k \leq p-2$.
 - * Ce n'est pas $k(p-1)$ car $k(p-1) = kp - k \equiv -k[p] \equiv p - k[p]$. Donc $k(p-1)$ est au moins égal à 2 .
 - * C'est donc un produit de la liste $2k, 3k, \dots, k(p-2)$ et c'est gagné.
- Ainsi en regroupant les facteurs de $(p-1)!$ deux par deux, nous aurons, modulo p :

$$(p-1)! = 2 \times 3 \times \dots \times (p-2) \times (p-1) \equiv 1 \times 1 \times \dots \times (p-1) \equiv p-1 \equiv -1$$