TD 09
Arithmétique des entiers

1 Exercices corrigés en classe

Exercice 1. Soit n dans $\mathbb{N}^*$. Montrer que 11 divise $2^{6n-5}+3^{2n}$ et que 17 divise $3\times 5^{2n-1}+2^{3n-2}$.

Exercice 2. Soit k dans $\mathbb{N}^*$. Existe-il a dans $\mathbb{N}$ tel que $[\![a, a+k]\!]$ ne contienne aucun nombre premier ?

Exercice 3. Soient a et b deux entiers tels que $a^2|b^2$. Montrer que $a|b$.

Exercice 4. *Nombres de Mersenne*.

1. Soit $n>1$. Montrer que si a^n-1 est premier, alors $a=2$ et n est premier.

2. On pose, pour n dans $\mathbb{N}$, $M_n=2^n-1$. Montrer que

$$M_k \wedge M_l = M_{k\wedge l}.$$

(on regardera les restes dans l'algorithme d'Euclide pour M_k et M_l).

Exercice 5. Soient n un entier naturel non nul, p un nombre premier. Démontrer que

$$v_p(n!)=\left\lfloor \frac{n}{p^1}\right\rfloor+\left\lfloor \frac{n}{p^2}\right\rfloor+\left\lfloor \frac{n}{p^3}\right\rfloor+\cdots+\left\lfloor \frac{n}{p^n}\right\rfloor.$$

2 Exercices à faire en TD

Plan de travail

1. Des exercices de base sur les congruences : le 6, 7 et 8. Le 10 est plus difficile !

2. Des exercices sur les notions de pgcd et ppcm : le 11, le 12, le 13 sont assez basiques, le 14 est conseillé (classique), le 15 est simple quand on a la solution mais peut parfois poser problème !

3. Des exercices sur les nombres premiers, utilisant la notion de valuation (16 et 17), d'autres sur le petit théorème de Fermat (18) et d'autres plus généraux (20 et 21)

4. Le théorème de Wilson est un exercice intéressant (19)

5. Des exercices un peu plus accessoires sur les résolutions d'équations arithmétiques : équations avec pgcd et ppcm (24), des équations diophantiennes (23 et 25), un résultat qui utilise ou les valuations, ou des résultats d'analyse (26).

6. Enfin, le dernier exercice (27) est un oral d'ENS, très difficile mais intéressant !

Minimum vital faire le 6, questions 1 et 2, le 7, question 1, le 11, questions 1 et 2, le 14, le 16, le 23.

2.1 Divisibilité –congruences

Exercice 6. *Jouons avec les congruences*. ◐○○

1. Déterminer le reste modulo 11 de $2^{123}+2^{121}$.

2. Montrer que $\forall n \in \mathbb{N},\ 7|3^{2n+1} + 2^{n+2}$.

3. Montrer que $\forall n \in \mathbb{N},\ n^2|(n+1)^n - 1$.

Exercice 7. ●◐○ Soit n un entier naturel non nul. Montrer que...

1. ...$n^3(n^6 - 1)$ est divisible par 8.

2. ...$n^3 - n$ est divisible par 3.

3. ...$3^{n+3} - 4^{4n+2}$ est divisible par 11.

4. ...lorsque n est impair, $n(n^2 - 1)$ est divisible par 24.

Exercice 8. ●◐○ Un nombre palindrome est un nombre qui se lit indifféremment de gauche à droite ou de droite à gauche. Par exemple, 2002, 12321 sont des nombres palindromes. Prouver qu'un nombre palindrome ayant un nombre pair de chiffres est divisible par 11.

Exercice 9. ●●○ Soit x un entier naturel non nul, $x = \overline{a_N a_{N-1} \dots a_1 a_0}$ son écriture en base 10 (a_0 est le chiffre des unités, a_1 des dizaines, etc.)

1. Démontrer que 7 divise x si, et seulement si 7 divise $5a_0 + \overline{a_N a_{N-1} \dots a_2 a_1}$.

2. Démontrer que 7 divise x si, et seulement si 7 divise $\overline{a_N a_{N-1} \dots a_2 a_1} - 2a_0$.

3. On propose une recette pour déterminer si un grand nombre est divisible par 7. Soit par exemple le nombre 7905669884. On l'écrit en séparant les nombres en paquets de 3 :

7 905 669 884

puis on fait la somme alternée $7 - 905 + 669 - 884 = -1113$.
On prend la valeur absolue du résultat, 1113 et, s'il est divisible par 7, alors le nombre de départ l'est !
(ici, on utilise la méthode du 2 : $111 - 2 \times 3 = 105$, $10 - 2 \times 5 = 0$ donc 7 divise 105 donc 1113 donc 7905669884).
Expliquer cette méthode.

Exercice 10. ●●● On pose, pour tout n dans $\mathbb{N}$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Montrer que pour tout $n \geqslant 2$, H_n n'est pas entier.

2.2 PGCD, PPCM

Exercice 11. ◐○○ Soit $n \in \mathbb{N}^*$.

1. Trouver le pgcd de $n! + 1$ et $(n+1)! + 1$.

2. Montrer que $2n + 1$ et $14n + 3$ sont premiers entre eux.

3. Montrer que $n^4 + 3n^2 + 1$ et $n^3 + 2n$ sont premiers entre eux.

Exercice 12. ●●○ Soit $(P, m) \in (\mathbb{N}^*)^2$. Trouver une condition nécessaire et suffisante pour qu'il existe deux entiers dont le produit soit P et le ppcm m. Comment déterminer alors les entiers solutions ? À titre d'exemple, traiter le cas $P = 24$, $m = 12$.

Exercice 13. ●◐○ Soit $n \in \mathbb{N}^*$. Montrer que $\text{ppcm}(1, 2, \dots, 2n) = \text{ppcm}(n+1, \dots, 2n)$.

Exercice 14. ●●○

1. Montrer que pour tout n dans $\mathbb{N}$, il existe un unique couple $(a_n, b_n) \in \mathbb{Z}^2$ tel que

$$(1+\sqrt{2})^n = a_n + \sqrt{2}b_n.$$

2. Montrer que pour tout n dans $\mathbb{N}$, $\text{pgcd}(a_n, b_n) = 1$.

Exercice 15. ●●○ Soit a et b deux entiers naturels non nuls.

1. On suppose $\text{pgcd}(a, b) = 1$. Déterminer le pgcd de ab et $a + b$.

2. Dans le cas général, quel est le pgcd de $a + b$ et $\text{ppcm}(a, b)$?

2.3 Nombres premiers, décomposition en facteurs premiers

Exercice 16. ◐○○ Soient a et b deux entiers naturels tels qu'il existe n dans $\mathbb{N}^*$ tel que a^n divise b^n. Montrer que a divise b.

Exercice 17. ●○○ Soit n un entier positif. Montrer que $\sqrt{n} \in \mathbb{N} \Leftrightarrow \sqrt{n} \in \mathbb{Q} \Leftrightarrow n$ est un carré parfait (i.e. $\exists k \in \mathbb{N}$, $n = k^2$).

Exercice 18. *Applications du petit théorème de Fermat*. ●●○

1. Quel est le reste de la division euclidienne de $2^{70^{71}}$ par 13 ?

2. Montrer que pour tout $n \in \mathbb{Z}$, on a $n^7 \equiv n$ [42].

3. Trouver les nombres premiers p tels que p divise $2^p + 1$.

Exercice 19. *Théorème de Wilson*. ●●○ Soit p un nombre premier différent de 2.

1. Montrer que $(p-1)^2 \equiv 1[p]$.

2. Montrer que $x^2 \equiv 1[p]$ si, et seulement si $x \equiv 1[p]$ ou $x \equiv -1[p]$.

3. Soit n dans $\{1, 2, \ldots, p-1\}$ Montrer qu'il existe un unique entier m dans $\{1, 2, \ldots, p-1\}$ tel que $mn \equiv 1[p]$. Quand a-t-on $m = n$?

4. Démontrer que $(p-1)! \equiv p-1[p]$.

5. Déduire de ce qui précède une preuve du théorème de Wilson : pour tout entier naturel q, q est premier si, et seulement si $(q-1)! \equiv q-1[q]$.

Exercice 20. *Nombres premiers jumeaux*. ●◐○ Deux nombres premiers p et q sont dits jumeaux si leur différence est égale à 2.

1. Donner des exemples de nombres premiers jumeaux.

2. Soient p et q deux nombres premiers. Montrer p et q sont jumeaux si, et seulement si $pq+1$ est un carré.

3. Montrer que si p et q sont deux nombres premiers jumeaux supérieurs ou égaux à 5, alors $p + q$ est divisible par 12.

Exercice 21. ●●◐ On veut montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$, avec $k \in \mathbb{Z}$. On note leur ensemble $\mathbb{P}_{3,4}$ et suppose, par l'absurde, que $\mathbb{P}_{3,4} = \{p_1, \ldots, p_N\}$ avec $N \in \mathbb{N}$. On pose $q = 4(p_1 \ldots p_N) - 1$.

1. Montrer que q possède un facteur premier congru à 3 modulo 4.

2. Montrer que ce facteur premier ne peut pas être égal à $p_1, \ldots, p_N$, et conclure.

Exercice 22. ●●◐

1. (question préliminaire) Démontrer qu'il existe une infinité de nombres de la forme $\frac{2^a}{3^b}$ (où a et b sont entiers) dans l'intervalle $\left[\frac{1}{\sqrt{2}}, \sqrt{2}\right]$.

On note, pour $n \in \mathbb{N}^*$, d_n le nombre de diviseurs de n compris entre $\sqrt{\frac{n}{2}}$ et $\sqrt{2n}$.

2. La suite $(d_n)_{n\in\mathbb{N}}$ est-elle convergente ?

3. La suite $(d_n)_{n\in\mathbb{N}}$ est-elle bornée ?

2.4 Résolution d'équations

Exercice 23. ●◐○

1. Trouver toutes les solutions en nombres entiers de $29x - 11y = 1$.

2. Résoudre dans $\mathbb{Z}^3$ l'équation $5x - 3y + 8z = 1$.

Exercice 24. ●○○ Résoudre dans $\mathbb{Z}^2$ le système $\begin{cases} x + y = 56, \\ x \vee y = 105. \end{cases}$

Exercice 25. ●●○ Soit p un nombre premier. Résoudre l'équation suivante d'équations $(x, y) \in \mathbb{N}^2$

$$x^2 + px = y^2.$$

Exercice 26. *Résolution de l'équation $x^y = y^x$.* ●●○ On veut résoudre l'équation $x^y = y^x$ d'inconnues $(x, y) \in \mathbb{N}^*$, non triviales, i.e. telles que $x \neq y$. On suppose $x < y$. On va proposer deux méthodes de résolution.

1. En étudiant les valuations p-adiques, montrer que $x|y$. Conclure.

2. Retrouver le même résultat en étudiant la fonction $x \mapsto \frac{\ln(x)}{x}$ sur $\mathbb{R}_+^*$.

Exercice 27. *Oral ENS.* ●●●

1. Montrer que pour tout (a, b) dans $(\mathbb{N}^*)^2$, $a\binom{a+b}{b}$ divise $\mathrm{ppcm}((b+i)_{1\leqslant i\leqslant a})$.

2. Montrer que pour tout $n \in \mathbb{N}$, $(n+1)\mathrm{ppcm}\left(\binom{n}{i},\ 0 \leqslant i \leqslant n\right) = \mathrm{ppcm}(1, 2, \ldots, n+1)$.

3. Démontrer que pour tout $n \geqslant 1$, $\mathrm{ppcm}(1, 2, \ldots, n) \geqslant 2^{n-1}$.

4. En déduire une minoration du nombre de nombres premiers inférieurs ou égaux à n.

Indications

1 Penser à transformer les puissances en puissances positives, puis calculer, par exemple 2^6 et 3^2 modulo 11, et utiliser les règles de calcul sur les congruences.

2 Faire intervenir des factorielles dans l'écriture de a (l'avantage est que $k!$ est divisible par **tous** les nombres entre 1 et k)

3 Utiliser les valuations.

4 Pour la première question, utiliser l'identité de Bernoulli et penser que si n n'est pas premier, $n = mp$ et $a^n - 1 = (a^m)^p - 1^p$...

5 Poser $K = \max\{i \in \mathbb{N},\ p^i \leqslant n\}$, et compter les entiers entre 1 et n divisibles par p^K, ceux divisibles par p^{K-1} mais pas par p^K, ceux divisibles par p^{K-1} mais par par p^{K-2}, etc.

6 Mêmes méthodes qu'en 1

7 Ne pas hésiter, lorsqu'on a des quantités dépendant de n, à disjoindre les cas (notamment n pair, n impair), et écrire explicitement ce qu'est un nombre pair ou impair.

8 Utiliser l'écriture en base 10.

9 Pour les deux premières questions, penser au fait que $x = \overline{a_N \dots a_1 0} + a_0$ et que 1 est congru à 50 ou à -20 modulo 7. Pour la dernière, penser au fait que $1000 \equiv -1[7]$.

10 Démontrer par récurrence sur n $\mathcal{P}_n$: Soit p tel que $2^p \leqslant n < 2^{p+1}$, alors $H_n = \dfrac{a}{2^p b}$ avec a et b impairs.

11 Ne pas nécessairement établir des relations de Bézout pour montrer que les nombres sont premiers entre eux, mais, pour le 1 par exemple, montrer que le pgcd des deux nombres divise $n!$, puis divise 1.

12 Démontrer par analyse-synthèse que la CNS est $m|P|m^2$.

13 Démontrer que l'ensemble des multiples communs de $(1, 2, \dots, 2n)$ et des multiples communs de $(n+1, \dots, 2n)$ sont les mêmes.

14 Pour la première question, une récurrence ou le binôme de Newton. Pour la seconde, le faire par récurrence, ou bien remarquer que $(1-\sqrt{2})^n = a_n - \sqrt{2}b_n$ et calculer $a_n^2 - 2b_n^2$: on obtient alors une relation de Bézout.

15 Utiliser des relations de Bézout successives, ou bien démontrer que $a+b$ et a sont premiers entre eux, puis que $a+b$ et b sont premiers entre eux.

16 Utiliser les valuations.

17 Pour une implication, c'est évident. Pour l'autre, écrire $\sqrt{n} = \dfrac{p}{q}$ et démontrer que q^2 divise p^2.

18 Se ramener à des applications du petit théorème de Fermat, notamment sous la forme $a^p \equiv a[p]$.

19 **1.** Dévlopper
2. Utiliser le théorème de Gauss (sa version pour les nombres premiers)
3. Utiliser une relation de Bézout.
4. Regrouper habilement les termes du produit.
5. Montrer que q vérifie une relation de Bézout avec tous les entiers entre 2 et $q-2$.

20 Un sens est évident. Pour le second, utiliser que $pq = (k-1)(k+1)$.

21 Faire essentiellement des raisonnements par l'absurde !

23 Pour la première, c'est une méthode de cours. Pour la seconde, résoudre d'abord une équation diophantienne de paramètre $z \in \mathbb{Z}$.

24 Démontrer que $x \wedge y = 1$ ou 7, et discuter selon ces deux valeurs.

25 Comme souvent dans les tâches de recherche, raisonner par analyse-synthèse. Montrer que si le produit de deux entiers naturels premiers entre eux est un carré, c'est que chacun de ces entiers est un carré !

26 Pour l'utilisation des valuations, penser à utiliser que si $x > 2$, pour tout $k \geqslant 2$, $k < x^{k-1}$. Pour l'étude de fonctions, ne l'étudier que sur $[1, +\infty[$.

27 Utiliser les valuations, remarquer que $a\binom{a+b}{b} = \frac{((b+a)!}{(a-1)!b!} = \frac{(b+1)\dots(b+a)}{(a-1)!}$. Les questions 2 et 3 sont beaucoup plus simples.