TD 18 : Arithmétique dans $\mathbb{Z}$

Divisibilité, nombres premiers entre eux

Ex 1 Montrer que : $\forall n \in \mathbb{N}, n \geqslant 2,\ 10 \mid (2^{2^n} - 6)$.
Comme 2 et 5 sont premiers entre eux, il suffit de montrer qu'ils divisent tous les deux le nombre en question. On calculera ensuite $2^{2^n} - 6$ modulo 5.

Ex 2 Montrer que la somme des cubes de trois entiers consécutifs est divisible par 9.
Calculer $(k-1)^3 + k^3 + (k+1)^3$, le factoriser puis conclure éventuellement par distinction de cas

Ex 3 Montrer que l'équation $x^3 + x^2 + 2x + 1 = 0$ n'a pas de solution dans $\mathbb{Q}$.
Supposer que $\frac{p}{q}$ est une olution, avec p et q premiers entre eux. Multiplier l'égalité vérifiée par p^3, puis la considérer modulo p. On a alors $p|q^3$ puis on conclut.

Ex 4 **Nombres de Fermat**

1. Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ est premier. Montrer que m est une puissance de 2.
   Supposer la négation : $m = pq$ avec q impair et p une puissance de 2. Calculer alors $2^m + 1 = (2^p)^q + 1$ et montrer qu'il se factorise par $2^p + 1$ au préalable, on peut montrer que : pour q un entier impair on a pour tout réel x , $x^q + 1 = (x+1)(x^{q-1} - x^{q-2} + \cdots + 1)$.
2. On pose $F_n = 2^{2^n} + 1$: $n^{\text{ème}}$ nombre de Fermat. Quelle est la parité de F_n ?
3. Montrer que
   (a) $F_{n+1} = (F_n - 1)^2 + 1$.
   (b) $\prod_{k=0}^{n} F_k = F_{n+1} - 2$.
4. En déduire que si $m \neq n$ alors $F_m \wedge F_n = 1$.

Ex 5 Résoudre le système suivant dans $(\mathbb{N}^*)^2$: $\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases}$ Chercher x et y sous la forme $18a$ et $18b$ avec $a \wedge b = 1$ et une autre information donnant ab.

Ex 6

1. Soient a et b deux entiers naturels tels que $0 < a < b$. Montrer que $(a+b) \wedge (a \vee b) = a \wedge b$. Ecrire $a = da'$ et $b = db'$ avec $d = a \wedge b$ et ramener cela à l'égalité $(a' + b') \wedge (a'b') = 1$. Justifier que ces deux entiers sont effectivement premiers entre eux.
2. Trouver a et b tels que $\begin{cases} a + b = 144 \\ a \vee b = 420 \end{cases}$ Se servir de la question précédente. $a = 12a'$ et $b = 12b'$.

Ex 7 **Équations diophantiennes**
Résoudre dans $\mathbb{Z}$ les équations :
(a) $221x + 247y = 15$ (b) $198x + 216y = 36$ (c) $323x - 391y = 612$

Nombres premiers

Ex 8 Soient $(a,b) \in \mathbb{Z}^2$. Montrer l'équivalence suivante :

$$7|a \text{ et } 7|b \iff 7|a^2 + b^2$$

Ex 9 Trouver tous les $n \in \mathbb{Z}$ tels que $n^4+4n^3+6n^2+4n+5$ soit premier.
Factoriser $(n+1)^4+4 = ((n+1)^2+2i)((n+1)^2-2i)$ puis de nouveau en remarquant que $i = \omega^2$ où on détemrine ω. En regroupant soigneusement les facteurs $n-z$ avec $n-\bar{z}$ on trouve la factorisation suivante : $n^4+4n^3+6n^2+4n+5 = (n^2+4n+5)(n^2+1)$

Ex 10 Montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$ et $6k+5$. Pour le premier : on suppose que l'ensemble E des tels nombres premiers est fini. On en fait le produit P puis on considère $4P-1$. On montre que ce nombre là est un nombre premier de la forme $4k+3$ et qu'il ne faisait pas partie de l'ensemble E ce qui est absurde

Ex 11 Soit $n \in \mathbb{N}, n \geqslant 2$. Démontrer qu'aucun des entiers consécutifs de $n!+2$ à $n!+n$ n'est premier.
En déduire que pour tout $n \in \mathbb{N}, n \geqslant 2$, il existe n entiers consécutifs non premiers.
Calculer $n!+k$ modulo k pour prouver que ce nombre est divisible par k

Décomposition en produit de facteurs premiers

Ex 12 Soit $n \in \mathbb{N}$, montrer que si n est un carré et un cube alors n est le carré d'un cube.
Interpréter le fait que n soit un carré en terme des valuations p-adiques de n. Idem pour être un cube, puis conclure

Ex 13 Trouver n de la forme 3^p5^q sachant que le produit de tous ses diviseurs est 45^{42}.
Commencer par justifier qu'un tel nombre ne peut qu'être sous la forme 3^a5^b, puis énumérer tous les diviseurs d'un tel nombre pour en calculer le produit et ainsi obtenir une condition sur a et b

Ex 14 Formule de Legendre

1. Trouver la puissance de 2 dans la décomposition en produit de facteurs premiers de 1000!
   $v_2(1\times 2\times \ldots \times 1000) = v_2(1)+v_2(2)+\ldots+v_2(1000)$
2. Soit $p \in \mathscr{P}$ et $n \in \mathbb{N}^*$. Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.
   Même raisonnement, puis dénombrer parmi $[\![1, n]\!]$ le nombre d'éléments divisibles par p mais pas p^2, par p^2 mais pas p^3 etc.
3. Application : Par combien de zéros se termine 2024! ? Cela fait intervenir v_2 et v_5 car il s'agit de la plus grande puissance de 10 qui divise ce nombre

Ex 15 Somme et produit des diviseurs
Soit $n \in \mathbb{N}^*$, on note $d(n)$ le nombre de diviseurs positifs de n et $\sigma(n)$ la somme des diviseurs de n. On suppose $n = \prod_{p\in\mathscr{P}} p^{v_p(n)}$.
Montrer que

$$d(n) = \prod_{p\in\mathscr{P}} (v_p(n)+1) \quad \text{et} \quad \sigma(n) = \prod_{p\in\mathscr{P}} \left(\frac{p^{v_p(n)+1}-1}{p-1} \right)$$

Montrer que $\mathcal{D}(n) = \left\{ 2^{\alpha_2}\times 3^{\alpha_3}\times\ldots\times p_r^{\alpha_{p_r}}, 0\leq\alpha_2\leq v_2(n), 0\leq\alpha_3\leq v_3(n), \ldots, 0\leq\alpha_{p_r}\leq v_{p_r}(n) \right\}$

Congruences

Ex 16 Critères de divisibilité par 7 et 11
Soit n un entier naturel non nul.

1. On pose a_{i-1} le i-ème chiffre de n. Si on suppose que n est un nombre à p chiffres, exprimer n en fonction de la suite $(a_i)_{i\in[\![0,p-1]\!]}$.
2. Montrer que n est divisible par 11 ssi la différence entre les sommes de ses chiffres de rang pair et de rang impair est un multiple de 11.
3. Montrer que n est divisible par 7 ssi la différence entre le nombre de dizaines de n et le double du chiffre des unités est un multiple de 7.
4. Lequel des nombres suivants sont multiples de 7 ou 11 ? 15326 2816 759114

Ex 17 **Périodicité des restes**

1. Déterminer le reste de la division euclidienne de 19^{52} par 8. Le même que $3^52 = (3^2)^26 = 9^26$ or $9 \equiv 1[3]$
2. Déterminer le reste de la division euclidienne de $1234^{4321} + 4321^{1234}$ par 7.
3. Résoudre l'équation diophantienne : $x^2 = 4k+3$.
4. Résoudre l'équation diophantienne : $x^2 = y^5 - 4$ (Indication : On pourra étudier l'équation modulo 11)

Ex 18 **Théorème chinois**

1. Soient N_1 et N_2 deux entiers premiers entre eux et a_1 et a_2 des entiers relatifs. On considère le système congruent suivant

$$(S) \begin{cases} x \equiv a_1 [N_1] \\ x \equiv a_2 [N_2] \end{cases}$$

   Montrer qu'il existe $a \in \mathbb{Z}$ tel que $(S) \iff x \equiv a [N_1 N_2]$.
   Généraliser le résultat à un système congruent de k équations de la forme $x \equiv a_i [N_i]$ où les N_i sont premiers entre eux deux à deux. Utiliser les coefficients de Bézout
2. Application 1 : Résoudre le système congruent suivant $\begin{cases} x \equiv 2 [10] \\ x \equiv 5 [13] \end{cases}$
3. Application 2 : Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui-ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment; le cuisinier reçoit 4 pièces. Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces. Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Ex 19 **Probabilités et indicatrice d'Euler**

On choisit au hasard un des nombres entiers 1, 2, ... n, tous les choix étant équiprobables. Soit p un entier non nul, $p \leqslant n$. On note A_p l'événement « le nombre choisi est divisible par p ».

1. Calculer $\mathrm{P}(A_p)$ lorsque p divise n. Seuls $p, 2p, 3p, ...$ et $\frac{n}{p}p$ sont divisibles par p et l'on est en situation d'équiprobabilité
2. Montrer que si $p_1, p_2, \dots p_k$ sont des diviseurs premiers de n distincts 2 à 2 alors les événements $A_{p_1}, A_{p_2}, \dots A_{p_k}$ sont indépendants.
3. On appelle **fonction indicatrice d'Euler** la fonction φ définie sur les entiers naturels dont la valeur $\varphi(n)$ est égale au nombre d'entiers non nuls inférieurs à n et premiers avec n. Montrer que

$$\varphi(n) = n \prod_{p \in \mathscr{P}, p \mid n} \left(1 - \frac{1}{p}\right)$$