1. (Eaz01) Petit théorème de Fermat.
Soit p premier et k entier tels que $0 < k < p$.
   a. Montrer que
   $$k \wedge p = 1 \Rightarrow p \text{ divise } \binom{p}{k}$$
   En déduire que
   $$\forall a \in \mathbb{N},\ (a+1)^p \equiv a^p + 1 \mod p.$$
   b. Montrer que
   $$\forall a \in \mathbb{N},\ a^p \equiv a \mod p.$$
   En déduire
   $$a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 \mod p.$$
   (petit théorème de Fermat voir en 10 une version plus générale)
2. (Eaz02) Dans tout l'exercice a, b, c, d, désignent des naturels non nuls. Cet exercice est à traiter en utilisant la décomposition en facteurs premiers. Chaque relation se démontre à partir de relations à préciser formées avec les valuations p-adiques, des max des min des sommes et des produits.
   a. Montrer que $a \wedge (b \vee a) = a$ et $a \vee (b \wedge a) = a$.
   b. Montrer que $a \wedge (bc) = a \wedge c$ et $a \vee (bc) = b(a \vee c)$ lorsque a et b sont premiers entre eux.
   c. On suppose ici que a divise b. Montrer que
   $$b \wedge c = (a \wedge c)\left[\frac{c}{a \wedge c} \wedge \frac{b}{a}\right]$$
   $$(a \vee c)\frac{b}{a} = (b \vee c)\left[\frac{c}{a \wedge c} \wedge \frac{b}{a}\right]$$
   d. Montrer que $c \vee (a \wedge b)$ divise $c \vee a$ et $c \vee b$ et que les quotients sont premiers entre eux.
   En déduire que $\vee$ est distributive sur $\wedge$:
   $$(c \vee a) \wedge (c \vee b) = c \vee (a \wedge b).$$
   e. Montrer que $\wedge$ est distributive sur $\vee$:
   $$(c \wedge a) \vee (c \wedge b) = c \wedge (a \vee b).$$
3. (Eaz03) Soit x, y, z des naturels non nuls, on pose
   $$M = x \vee y \vee z,\ m = xy \wedge yz \wedge zx$$
   Montrer que $mM = xyz$.
4. (Eaz04) Soit $p \neq 3$ un nombre premier.
Montrer que $8p^2 + 1$ est congru à 0 modulo 3. Montrer que $8p - 1$ premier entraine $8p + 1$ divisible par 3.
5. (Eaz05) Déterminer tous les couples d'entiers relatifs tels que $a + b = 182$ et $a \wedge b = 13$.
6. (Eaz06) Discuter et résoudre les systèmes
   $$\begin{cases} x \equiv 8 \mod 15 \\ x \equiv 5 \mod 6 \end{cases} \quad \begin{cases} x \equiv 5 \mod 20 \\ x \equiv 7 \mod 14 \end{cases}$$
   $$\begin{cases} x \equiv 7 \mod 15 \\ x \equiv 5 \mod 6 \end{cases}$$
7. (Eaz07) Indicatrice d'Euler.
Soit $n \geq 2$ naturel et $x \in \mathbb{Z}$, montrer
   $$(\exists y \in \mathbb{Z} \text{ tq } xy \equiv 1 \mod n) \Leftrightarrow n \wedge x = 1$$
   On note $\varphi(n)$ le nombre d'éléments de $[\![1, n]\!]$ premiers avec n. La fonction φ est appelée *l'indicatrice d'Euler*. Si p est un nombre premier, que vaut $\varphi(p)$ et $\varphi(p^n)$ pour $n \in \mathbb{N}^*$?
8. (Eaz08) Soit G un groupe commutatif fini de cardinal $n = pq$ avec p et q premier entre eux. On admet que $g^n = e$ pour tout g dans G (théorème de Lagrange al07). On note G_p (respectivement G_q) l'ensemble des g de G dont l'ordre divise p (respectivement q).
   a. Montrer que G_p et G_q sont des sous-groupes de G.
   b. Montrer que l'application
   $$\begin{cases} G_p \times G_q \to G \\ (a, b) \to ab \end{cases}$$
   est un isomorphisme de groupe. En déduire que $\sharp G_p = p$ et $\sharp G_q = q$.
9. (Eaz09) Nombre de diviseurs.
Soit n un entier supérieur ou égal à 2. On note $d(n)$ le nombre de diviseurs positifs de n. [1]
   a. Si la décomposition en facteurs premiers de n est
   $$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$
   Exprimer $d(n)$ à l'aide de $m_1, \cdots, m_k$. (valuations p-adiques de n) En déduire que d est *multiplicative* c'est à dire que
   $$a \wedge b = 1 \Rightarrow d(ab) = d(a)d(b)$$
   b. Montrer que n est un carré d'entier si et seulement si $d(n)$ est impair.
   c. Montrer que le produit de tous les diviseurs de n est $\sqrt{n^{d(n)}}$.
   d. Montrer que le nombre de couples (a, b) d'entiers tels que le ppcm de a et de b soit n est égal au nombre de diviseurs de n^2.
10. (Eaz10) Petit théorème de Fermat étendu.
Soit $n \geq 2$ naturel et $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. On note $\mathcal{M}$ l'ensemble des fonctions μ, de $\mathbb{U}_n$ dans $\mathbb{U}_n$ et vérifiant :
   $$\forall (u, u') \in \mathbb{U}_n^2,\ \mu(uu') = \mu(u)\,\mu(u')$$
   Pour μ et μ' dans $\mathcal{M}$, on définit $\mu.\mu'$ par :
   $$\forall u \in \mathbb{U}_n,\ (\mu.\mu')(u) = \mu(u)\,\mu'(u)$$
   a. Montrer que $(\mathcal{M}, ., \circ)$ est un anneau.[2]

[1] On donnera deux solutions pour les questions b. et c. : une utilisant la paramétrisation de l'ensemble des diviseurs sous-jacente à la question a., l'autre le regroupement des diviseurs par paires $\{d, d'\}$ telles que $dd' = n$.

[2] On remarquera que l'opération additive de cet anneau est la multiplication fonctionnelle !

b. Montrer que, pour tout $\mu \in \mathcal{M}$, il existe un unique $m \in [\![0, n-1]\!]$ tel que

$$\forall u \in \mathbb{U}_n,\ \mu(u) = u^m$$

En déduire le nombre d'éléments de $\mathcal{M}$.

c. Montrer que le groupe des inversibles de l'anneau $\mathcal{M}$ contient $\varphi(n)$ éléments (exercice 7 az07 indicatrice d'Euler).

d. En utilisant le théorème de Lagrange dans le cas commutatif (exercice al05 de la feuille Groupes, anneaux, corps), montrer le petit théorème de Fermat étendu.
Pour m et n entiers supérieurs à 2 :

$$m^{\varphi(n)} \equiv 1 \mod (n)$$

voir en 1 une version plus simple.

11. (Eaz11) Calculer le reste de la division de $2^{65} - 3$ par 65.

12. (Eaz12) Pour n naturel non nul, soit $p_1, \cdots, p_n$ les n premiers nombres premiers. On note aussi

$$q_n = p_1 p_2 \cdots p_n = 2 \times 3 \times 5 \times \cdots \times p_n$$

On note $\mathcal{P}$ l'ensemble des nombres premiers et, pour $0 < a < b$, on note $\mathcal{P}_a(b)$ l'ensemble des nombres premiers congrus à b modulo a.

a. Montrer que $[\![n! + 2, n! + n]\!]$ et $[\![q_n + 2, q_n + p_n]\!]$ ne contiennent aucun nombre premier.

b. Montrer que $\mathcal{P} \setminus \{2\} = \mathcal{P}_4(1) \cup \mathcal{P}_4(3)$. En considérant $2\frac{q_n}{3} + 3$, montrer que $\mathcal{P}_4(3)$ est infini.

c. Montrer que $\mathcal{P} \setminus \{2, 3\} = \mathcal{P}_6(1) \cup \mathcal{P}_6(5)$. En considérant $\frac{q_n}{5} + 5$, montrer que $\mathcal{P}_6(5)$ est infini.

13. (Eaz13) Résoudre les systèmes de congruence :

$$\text{modulo } 7 \quad \begin{cases} 3x + 2y \equiv 1 \\ 2x + 5y \equiv 6 \end{cases}, \quad \begin{cases} x - 3y \equiv 4 \\ 3x + 6y \equiv 6 \end{cases}, \quad \begin{cases} 4x + 3y \equiv 2 \\ 3x + 5y \equiv -3 \end{cases}, \quad (1)$$

$$\text{modulo } 4 \quad \begin{cases} 2x + 3y \equiv 1 \\ x + y \equiv 2 \end{cases}, \quad \begin{cases} 2x - 2y \equiv 2 \\ x + 3y \equiv 1 \end{cases} \quad (2)$$

14. (Eaz14)

a. Montrer que le carré d'un nombre impair est congru à 1 modulo 8.

b. Montrer que le cube d'un entier est congru à 0 ou 1 ou -1 modulo 7.

c. Soit p un nombre premier supérieur ou égal à 5. Montrer que 24 divise $p^2 - 1$.

15. (Eaz15) Soit p, n, m naturels tels que $0 < p$, $0 < n < m$ et r le reste de la division de m par n. Montrer que le reste de la division de $p^m - 1$ par $p^n - 1$ est $p^r - 1$.
Que peut-on en déduire pour $(p^m - 1) \wedge (p^n - 1)$?
Un *nombre de Mersenne* est de la forme

$$M_n = 2^n - 1.$$

Montrer que M_n premier entraine n premier. Montrer que M_{11} n'est pas premier.

16. (Eaz16) Soit a et b entiers non nuls. Montrer que

$$(a + b) \wedge (ab) = 1 \Leftrightarrow a \wedge b = 1.$$

En déduire $a \wedge b = (a + b) \wedge (a \vee b)$.

17. (Eaz17) Soit x et y non nuls dans z et a, b, c, d dans $\mathbb{Z}$ tels que $\delta = ad - bc \neq 0$. On définit u et v :

$$\begin{cases} u = ax + by \\ v = cx + dy \end{cases}.$$

a. Montrer que $x \wedge y$ divise $u \wedge v$.

b. Montrer que $u \wedge v$ divise $\delta(x \wedge y)$.

c. Montrer que

$$\delta = \pm 1 \Rightarrow u \wedge v = x \wedge y.$$

d. Montrer que si $\delta = p$ est premier $u \wedge v = x \wedge y$ ou $p(x \wedge y)$.

1. (Caz01)

   a. D'après l'expression des coefficients du binôme avec des produits :

   $$\binom{p}{n} = \frac{p}{n}\binom{p-1}{n-1}$$
   $$\Rightarrow p \text{ divise } n\binom{p}{n} \Rightarrow p \text{ divise } \binom{p}{n}$$

   lorsque $n \wedge p = 1$ d'après le théorème de Gauss.
   En développant $(a+1)^p$ avec la formule du binôme, tous les coefficients sauf les deux extrêmes disparaissement modulo p. On en déduit la formule demandée.

   b. On raisonne par récurrence sur a. La formule est évidente pour $a = 0$ ou 1. On passe de a à $a+1$ avec la première question.
   Lorsque $a \wedge p = 1$, il existe b (théorème de Bezout) tel que $ab \equiv 1 \mod p$. Il suffit de multiplier la relation précédente par b pour obtenir le petit théorème de Fermat.

2. (Caz02) Pour $a, b, \cdots$ naturels non nuls, on notera α, β les valuations p-adiques c'est à dire que, pour tout nombre premier p, l'exposant de p dans la décomposition de a en facteurs premiers est $\alpha(p)$. Celui de b est $\beta(p)$. Le résultat fondamental utilisé ici est
   – la valuation p-adique de $a \wedge b$ est $\min(\alpha(p), \beta(p))$,
   – la valuation p-adique de $a \vee b$ est $\max(\alpha(p), \beta(p)$.
   Les formules demandées reposent sur des relations simples entre des entiers. On note ici $x = \alpha(p), y = \beta(p), \cdots$.
   Pour les questions a. et b, on présente dans des tableaux les résultats prouvant les relations demandées.

   a.

$\min(x, \max(y, x)) = x$	$a \wedge (b \vee a) = a$
$\max(x, \min(y, x)) = x$	$a \vee (b \wedge a) = a$

   b.

$xy = 0$	$a \wedge b = 1$
$\min(x, y+z) = \min(x, z)$	$a \wedge (bc) = a \wedge c$
$\max(x, y+z) = y + \max(x, z)$	$a \vee (bc) = a \vee c$

   c. On suppose que a divise b. Par linéarité puis associativité du pgcd :

   $$(a \wedge c)\left[\frac{c}{a \wedge c} \wedge \frac{b}{a}\right] = c \wedge \left((a \wedge c)\frac{b}{a}\right)$$
   $$= c \wedge \left(b \wedge \frac{bc}{a}\right) = \left(c \wedge \frac{b}{a}c\right) \wedge b = c \wedge b.$$

   Utilisons la propriété $(u \wedge v)(u \vee v) = uv$.
   On déduit de la relation précédente

   $$\frac{ac}{a \vee c}\left[\frac{c}{a \wedge c} \wedge \frac{b}{a}\right] = \frac{cb}{c \vee b}$$
   $$\Rightarrow (c \vee b)\left[\frac{c}{a \wedge c} \wedge \frac{b}{a}\right] = \frac{cb}{ac}(a \vee c) = \frac{b}{a}(a \vee c).$$

   d. On utilise encore le produit du pgcd et du ppcm.

   $$\mathbb{Z} \ni \frac{c \vee a}{c \vee (a \wedge b)} = \frac{ca(a \wedge b \wedge c)}{(c \wedge a)c(a \wedge b)} = \frac{\frac{a}{a \wedge b}}{\frac{a \wedge c}{a \wedge b \wedge c}}$$
   $$\Rightarrow \frac{c \vee a}{c \vee (a \wedge b)} \text{ divise } \frac{a}{a \wedge b}.$$

   De même

   $$\frac{c \vee b}{c \vee (a \wedge b)} = \frac{\frac{b}{a \wedge b}}{\frac{b \wedge c}{a \wedge b \wedge c}} \Rightarrow \frac{c \vee b}{c \vee (a \wedge b)} \text{ divise } \frac{b}{a \wedge b}.$$

   Comme $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux, leurs diviseurs aussi.
   En multipliant par $c \vee (a \wedge b)$ et par linéarité du pgcd :

   $$\left(\frac{c \vee a}{c \vee (a \wedge b)}\right) \wedge \left(\frac{c \vee b}{c \vee (a \wedge b)}\right) = 1$$
   $$\Rightarrow (c \vee a) \wedge (c \vee b) = c \vee (a \wedge b).$$

   e. On utilise les relations précédentes

   $$(c \wedge a) \vee (c \wedge b) = [(c \wedge a) \vee c] \wedge [(c \wedge a) \vee b] \text{ (distr.)}$$
   $$= c \wedge [(c \vee b) \wedge (a \vee b)] \text{ (distr.)}$$
   $$= [c \wedge (c \vee b)] \wedge (a \vee b) = c \wedge (a \vee b).$$

   f.

3. (Caz03) Soit p un nombre premier. Alors

   $$v_p(m) = \min(v_p(xy), v_p(yz), v_p(zx))$$
   $$= \min(v_p(xyz) - v_p(z), v_p(zyz) - v_p(x), v_p(xyz) - v_p(y))$$
   $$= v_p(xyz) - \max(v_p(x), v_p(y), v_p(z))$$

   On en déduit $mM = xyz$.

4. (Caz04) Parmi trois nombres consécutifs, un est forcément divisible par 3. Si $8p-1$ est premier, il n'est pas divisible par 3, le nombre $8p$ ne l'est pas non plus donc $8p+1$ doit l'être. Un nombre premier qui n'est pas 3 est congru à 1 ou -1 modulo 3 donc $8p^2+1$ est congru à9 modulo 3 donc divisible par 3.
5. pas de correction pour Eaz05.tex
6. pas de correction pour Eaz06.tex
7. pas de correction pour Eaz07.tex
8. pas de correction pour Eaz08.tex
9. (Caz09)

   a. Dans la décomposition d'un diviseur, l'exposant de p_i est arbitraire entre 0 et m_i. Le nombre de diviseurs de n est donc

   $$d(n) = (1 + m_1) \cdots (1 + m_k).$$

   b. On introduit une relation entre les diviseurs positifs de n : d et d' sont en relation si et seulement si $dd' = n$. C'est une relation d'équivalence, les classes forment donc une partition de l'ensemble des diviseurs positifs. Or toutes les classes sont des paires sauf éventuellement le singleton $\{m\}$ si $m^2 = n$.
   On en déduit que n est un carré d'entier si et seulement si il existe une telle classe à un élement c'est àdire si et seulement si $d(n)$ est impair.

c. On remarque d'abord que si n est un carré alors $n^{d(n)}$ aussi. Si n n'est pas un carré, alors $d(n)$ est pair donc $n^{d(n)}$ est encore un carré.
Écrivons le produit des diviseurs

$$\pi = \prod_{(i_1,\cdots,i_k)\in[\![0,m_1]\!]\times\cdots\times[\![0,m_k]\!]} p_1^{i_1}\cdots p_p^{i_k}$$
$$= p_1^{\frac{m_1(m_1+1)}{2}}\cdots p_1^{\frac{m_p(m_1+1)}{2}}$$
$$\Rightarrow \pi^2 = (p_1^{m_1}\cdots p_k^{m_k})^{(m_1+1)\cdots(m_k+1)} = n^d(n).$$

d. Soit (a,b) dont le ppcm est n, notons α_k et β_k les exposants de p_k. Un doit être égal à m_k et l'autre plus petit. Attention, à ne pas compter deux fois le couple (m_k,m_k). On en déduit donc que le nombre de couples cherché est

$$(2(m_1+1)-1)\cdots(2(m_p+1)-1)$$
$$= (1+2m_1)\cdots(1+2m_p) = d(n^2)$$

10. pas de correction pour Eaz10.tex
11. pas de correction pour Eaz11.tex
12. (Caz12)
    a. On remarque que $n!+2$ est divisible par 2, $n!+3$ est divisible par 3, $\cdots$, $n!+n$ est divisible par n. De manière analogue, tout x entre $2=p_1$ et p_n admet un diviseur premier p_i avec $i\leq n$. On en déduit que q_n+x est divisible par p_i.
    b. Un nombre premier n'est pas congru à 0 mod 4 car il serait divisible par 4 ; ni congru à 2 (sauf 2) car il serait pair. On a donc

$$\mathcal{P}\setminus\{2\} = \mathcal{P}_4(1)\cup\mathcal{P}_4(3)$$

    Si p est un diviseur premier de $m=2\frac{q_n}{3}+3$ inférieur à p_n, il divise 3. Le seul possible serait 3 mais 3 ne divise pas m. Tous les diviseurs premiers de m sont donc strictement plus grands que p_n. Ils ne sont pas tous congrus à 1 modulo 4 car $2q_n+3\equiv 3 \mod 4$ (car $p_1=2$). Il existe donc un nombre premier congru à 3 modulo 4 et plus grand que n'importe quel nombre premier.
    c. Un nombre premier autre que 2 ou 3 ne peut être congru modulo 6 qu'à 1 ou 5 (sinon il serait divisible par 2 ou 3). Un diviseur premier de $m=\frac{q_n}{5}+5$ est strictement supérieur à p_n sinon il diviserait 5 et 5 n'est pas un diviseur de m. De plus $m\equiv 5 \mod 6$ car $p_1=2$ et $p_2=3$ donc les diviseurs premiers de m ne sont pas tous congrus à 1 modulo 6.
13. pas de correction pour Eaz13.tex
14. (Caz14)
    a. à compléter
    b. à compléter
    c. Le nombre premier p est impair donc $p-1$ et $p+1$ sont pairs d'où $p^2-1=(p-1)(p+1)$ est divisible par 4. Un des trois entiers consécutifs

$$p-1, p, p+1$$

est divisible par 3 et ce n'est pas p donc $(p-1)(p+1)$ est divisible par 3. Comme $2\wedge 3=1$, on a bien p^2-1 divisible par 24.

15. (Caz15) Soit $m=qn+r$ la division de m par n. Alors

$$p^m-1 = p^m-p^r+p^r-1 = p^r\left((p^m)^r-1\right)+p^r-1$$
$$= (p^m-1)p^r\left(p^{m(r-1)}+p^{m(r-2)}+\cdots+1\right)$$

Comme $0<p^r-1<p^m-1$, cette écriture est la division euclidienne de p^m-1 par p^n-1. Les suites de divisions euclidiennes de l'algorithme d'Euclide pour le calcul du pgcd de m et n ou de p^m-1 et p^n-1 sont parallèles. On en déduit

$$(p^m-1)\wedge(p^n-1) = p^{m\wedge n}-1.$$

Si n n'est pas premier, il admet un diviseur m tel que $1<m<n$. La question précédente (avec $p=2$) montre que 2^m-1 divise M_n. On en déduit

$$M_n \text{ premier } \Rightarrow n \text{ premier.}$$

Bien que $M2=3$, $M_3=7$, $M_5=31$, $M_7=127$ soient premiers, la réciproque est fausse car $M_{11}=2047$ n'est pas premier car il est divisible par 23. Ce diviseur a été trouvé à l'aide de quelques lignes de Python

```
d = 2
while 2047 % d != 0 and d*d <= 2047:
    d += 1
print(d)
```

16. (Caz16) Supposons $(a+b)\wedge(ab)=1$ et utilisons le théorème de Bezout. Il existe des entiers λ et μ tels que

$$\lambda(a+b)+\mu(ab)=1 \Rightarrow \lambda a+(\lambda+\mu a)b=1.$$

On en déduit $a\wedge b=1$.
Réciproquement, supposons $a\wedge b=1$ et considérons un diviseur premier p de ab et de $a+b$. Comme il est premier, il divise a ou b. Mais comme p divise $a+b$, s'il divise l'un il doit diviser l'autre en contradiction avec le fait que a et b sont premiers entre eux. Donc ab et $a+b$ n'ont pas de diviseur premier en commun, ils sont premiers entre eux.
Autre méthode, d'après Bezout, il existe λ et μ tels que $\lambda a+\mu b=1$. On transforme le carré pour faire apparaitre $a+b$ et ab.

$$1 = (\lambda a+\mu a)^2$$
$$= \lambda^2\left(a(a+b)-ab\right)+\mu^2\left(b(a+b)-ab\right)+2\lambda\mu ab$$
$$= \left(\lambda^2 a+\mu^2 b\right)(a+b)+\left(2\lambda\mu-\lambda^2-\mu^2\right)ab$$
$$= \left(\lambda^2 a+\mu^2 b\right)(a+b)-(\lambda-\mu)^2 ab.$$

On conclut par le théorème de Bezout. On veut montrer

$$a\wedge b = (a+b)\wedge(a\vee b).$$

C'est une conséquence immédiate de la relation précédente lorsque a et b sont premiers entre eux. Dans le cas général on utilise la linéarité avec les notations habituelles $d=a\wedge b$, $a=da',\ldots$.

$$(a+b)\wedge(a\vee b) = d(a'+b')\wedge(a'\vee b')$$
$$= d(a'+b')\wedge(a'b') = d = a\wedge b.$$

17. (Caz17)

a. D'après Bezout, il existe λ, μ tels que

$$\begin{aligned} u \wedge v &= \lambda u + \mu v \\ &= (\lambda a + \mu c)x + (\lambda b + \mu d)y \in \mathcal{M}(x \wedge y). \end{aligned}$$

b. En combinant les lignes, on obtient

$$\begin{cases} \delta x = du - bv \\ \delta y = -cu + av \end{cases}$$

D'après la première question,

$$u \wedge v \text{ divise } (\delta x) \wedge (\delta y) = \delta(x \wedge y).$$

c. Notons λ et μ les entiers tels que

$$u \wedge v = \lambda(x \wedge y), \qquad \delta(x \wedge y) = \mu(u \wedge v).$$

On en tire $\lambda\mu = \delta$. Si δ est un nombre premier p, λ est 1 ou p donc $u \wedge v$ est $x \wedge y$ ou $p(x \wedge y)$.