Introduction à l'arithmétique (Solutions)

Dans ce document, on se propose de donner un tour d'horizon des fondamentaux de l'arithmétique élémentaire des nombres entiers usuels. Il n'y a que peu de prérequis:

- Connaître le principe de récurrence.
- Pour les partie XI et XV uniquement: connaître le signe somme $\sum$ et savoir le manipuler.
- Pour la partie X uniquement: avoir quelques notions de géométrie du plan (pente d'une droite, équation d'un cercle).
- Pour la partie XIII uniquement: savoir ce qu'est un polynôme et son degré.

Toutes les autres notions abordées sont introduites au fil du problème. Les parties ne sont pas indépendantes. En revanche, il est parfaitement possible d'aborder une nouvelle partie en admettant les résultats des précédentes. Les parties sont numérotées en ordre grossièrement croissant de difficulté.

À propos des solutions. Les solutions présentes dans ce document donnent les idées mathématiques essentielles pour répondre à chacune des questions. Il ne s'agit aucunement d'un modèle de rédaction!

Table des matières

Partie I — Divisibilité des entiers

On que l'entier $n \neq 0$ divise l'entier m lorsque $\frac{m}{n}$ est un entier (autrement dit, s'il existe $k \in \mathbb{Z}$ tel que $m = kn$). On note alors $n \mid m$. On dit aussi que n est un diviseur de m.

(1) Pour chacune des propriétés suivantes, dire si elle est vraie ou fausse, en donner une preuve si elle est vraie, et un contre-exemple si elle est fausse.

(a) Si $n \mid m$ et $m \mid \ell$ alors $n \mid \ell$
(b) Si $n \mid m$ alors pour tout $k \in \mathbb{Z}$, $n \mid km$.
(c) Si $n \mid m$ et $\ell \mid m$ alors $n\ell \mid m$
(d) $n > 1$ admet au moins deux diviseurs.
(e) Si $n \mid m$ et $n \mid \ell$ alors $n \mid m + \ell$.
(f) Si $n, m > 0$, $n \mid m$ et $m \mid n$ alors $n = m$

(a) Vrai. On a $\ell = km$ et $m = k'n$ donc $\ell = kk'n$ et $kk' \in \mathbb{Z}$.

(b) Vrai. On a $m = qn$ donc $km = kqn$ et $kq \in \mathbb{Z}$.
(c) Faux. $2 \mid 12$ et $4 \mid 12$ mais $2 \times 4 = 8$ ne divise pas 12.
(d) Vrai. n est divisible par 1 et par n, au moins.
(e) Vrai. $m = kn$, $\ell = k'n$, alors $m + \ell = (k + k')n$ et $k + k' \in \mathbb{Z}$.
(f) Vrai. Comme $n, m > 0$, $n \mid m$ entraine $n \leq m$. Par symétrie, $n \geq m$ donc $n = m$.

(2) On appelle *plus grand commun diviseur (PGCD)* de deux entiers naturels n et m non simultanément nuls le plus grand entier $k \geq 1$ tel que $k \mid n$ et $k \mid m$. On le note $n \wedge m$
(a) Montrer que si $n, m > 0$, alors $n \wedge m \leq n$ et $n \wedge m \leq m$.

$n \wedge m$ divise n et m, d'où le résultat.
(b) Si $n \mid m$, que vaut $n \wedge m$? En déduire la valeur de $n \wedge 0$ pour $n > 0$.

Si $n \mid m$ alors $n \wedge m = n$ (n est bien diviseur des deux membres, et c'est bien le plus grand, car n n'admet pas de diviseur plus grand). Comme pour tout $n > 0$, $n \mid 0$, on a $n \wedge 0 = n$.
(c) Montrer que si n, m sont des entiers, alors

$$\frac{n}{n \wedge m} \wedge \frac{m}{n \wedge m} = 1$$

Notons $d = n \wedge m$ et soit $e > 0$ un diviseur commun de $\frac{n}{d}$ et $\frac{m}{d}$ de sorte qu'il existe u, v des entiers tels que

$$\frac{n}{d} = eu, \quad \frac{m}{d} = ev.$$

Alors, $n = deu$ et $m = dev$ donc de est un diviseur commun de n et m. Comme d est le plus grand diviseur commun, $de \leq d$ donc $e \leq 1$ donc $e = 1$. Ainsi, le seul diviseur commun de $\frac{n}{d}$ et $\frac{m}{d}$ est 1.

(3) On dit que deux entiers n et m sont *premiers entre eux* lorsque $n \wedge m = 1$.
(a) Les entiers 12 et 15 sont ils premiers entre eux ? Et les entiers 9 et 11 ?

3 divise 12 et 15 donc $12 \wedge 15 \geq 3$, donc 12 et 15 ne sont pas premiers entre eux. Les diviseurs de 9 sont $1, 3, 9$, seul 1 divise également 11, donc 9 et 11 sont premiers entre eux.
(b) Montrer que pour tout $n > 1$, n et $n - 1$ sont premiers entre eux.

Soit d un entier ≥ 1 divisant n et $n - 1$. Alors, d divise $n - (n - 1) = 1$, donc $d = 1$. Donc $n \wedge (n - 1) = 1$.
(c) (Lemme de Gauss) Montrer que si $k \mid \ell m$ et $k \wedge \ell = 1$ alors $k \mid m$.

$k \mid \ell m$ et $k \mid km$ donc $k \mid \ell m \wedge km = m(\ell \wedge k) = m$

Partie II — Nombres premiers

(1) On dit qu'un entier $p > 1$ est *premier* si ses seuls diviseurs positifs sont 1 et p.
(a) Lesquels des nombres suivants sont premiers ? $7, 9, 14, 17, 19, 21, 57$.

Sont premiers: $7, 17, 19$.
(b) Montrer que p est premier si et seulement si pour tout $m > 1$ qui n'est pas un multiple de p, on a $p \wedge m = 1$

Si p est premier, et $m > 1$ n'est pas multiple de p, alors $p \wedge m$ est un diviseur de p, qui vaut donc soit 1 soit p. Comme p ne divise pas m, il reste $p \wedge m = 1$. Supposons maintenant que pour tout $m > 1$ non multiple de p, $p \wedge m = 1$. Si p admet un diviseur d qui n'est pas multiple de p, alors $p \wedge d = d = 1$ donc p a pour seul diviseur 1 (autre que p), il est donc premier.

(c) Montrer que p est premier si et seulement si pour tout $a, b \in \mathbb{Z}$ tels que p divise ab, p divise a ou p divise b.

Supposons que p est premier et qu'il divise ab. Si $p \wedge b \neq 1$ alors $p \wedge b = p$ et p est un diviseur de b. Sinon, $p \wedge b = 1$ et le lemme de Gausse donne $p \mid a$.

Supposons désormais que p n'est pas premier. Alors il s'écrit $p = uv$ avec $u, v \neq 1$. On prend $a = u$ et $b = v$ pour trouver que p divise uv mais ne divise ni u ni v.

(d) Soit $n > 1$. Montrer que le plus petit diviseur $d > 1$ de n est premier.

Soit $n > 1$ et d son plus petit diviseur strictement supérieur à 1. Si d n'est pas premier, il a un diviseur $1 < d' < d$ et $d' \mid d$ donc $d' \mid n$, ce qui contredit la minimalité de d.

(e) Soient p, q deux nombres premiers distincts. Montrer que $p \wedge q = 1$.

On applique (b): p est premier et q n'est pas multiple de p (car sinon $p \mid q$ ce qui est absurde car q est premier).

(f) Donner la valeur de $p^n \wedge p^m$ lorsque p est premier et $1 \leq n < m$.

Lorsque p est premier, et $1 \leq n < m$, on a $p^n \wedge p^m = p^n$ car les diviseurs de p^m sont exactement les p^k pour $0 \leq k \leq m$ de sorte que le plus grand de ces diviseurs divisant p^n est p^n.

(2) Supposons qu'il y a un nombre fini de nombres premiers, que l'on note $p_1, \cdots, p_n$. En considérant le nombre

$$p_1 p_2 \cdots p_n + 1,$$

montrer qu'il existe un nombre premier p ne figurant pas dans la liste $p_1, \cdots, p_n$. En déduire qu'il y a un nombre infini de nombres premiers.

Le plus petit diviseur strict de $p_1 \cdots p_n + 1$ est un nombre premier que l'on note p. Comme les p_i énumèrent tous les nombres premiers, on a nécessairement $p = p_k$ pour un k, de sorte que

$$p \mid (p_1 \cdots p_n + 1) \wedge (p_1 \cdots p_n) = 1$$

ce qui est absurde. Il y a donc un nombre infini de nombres premiers (car il n'existe pas d'énumération finie complète des nombres premiers).

(3) Soit $n > 1$. Montrer par récurrence forte[1] que n s'écrit comme un produit $p_1 \cdots p_k$ de nombres premiers, éventuellement répétés. Indication: exploiter le résultat de la question (4.c). En déduire que tous les entiers $n > 1$ s'écrivent sous la forme

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

où $k \geq 1, p_1, \cdots, p_k$ sont des nombres premiers deux à deux distincts, $a_1, \cdots, a_k \geq 1$ sont des entiers (k et les p_i, a_i dépendent de n). On dit que c'est une *décomposition de n en facteurs premiers.*

Initialisation: 2 est le produit d'un seul nombre premier : 2.

Hérédité: Soit $n > 2$. On suppose la propriété vraie pour tout $k < n$. Le plus petit diviseur strict de n est premier, on le note p_0. Par hypothèse de récurrence,

$$\frac{n}{p_0} = p_1 \cdots p_r$$

donc

[1] Dans une récurrence forte, au lieu de supposer dans l'hérédité la propriété vraie au rang précédent, on suppose la propriété vraie à tous les rangs précédents ($\mathcal{P}_k$ vraie pour tout $k < n$). Le principe de récurrence forte est équivalent au principe de récurrence (il n'y a donc rien à vérifier « en plus » d'une récurrence classique).

$$n = p_0 \cdots p_r$$

donc la propriété est vraie au rang n.

Conclusion: par le principe de récurrence forte, tous les entiers se décomposent en un produit de facteurs premiers.

En réunissant les premiers répétés, on trouve immédiatement la seconde écriture de l'énoncé.

(4) Supposons que n admet les deux décompositions en facteurs premiers suivantes:

$$n = p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_r^{b_r}.$$

On suppose par ailleurs que les p_i et les q_i sont triés en ordre croissant. Montrer que $r = k$ et que pour tout $1 \leq i \leq k$, $p_i = q_i$ et $a_i = b_i$. On en déduit que chaque entier naturel $n \geq 1$ admet une *unique* décomposition en facteurs premiers.

Indication: Calculer $p_i \wedge n$ et $p_i^{a_i} \wedge n$.

Avec les notations de l'énoncé, on a $p_1 \wedge n = p_1$ donc p_1 divise $q_1^{b_1} \cdots q_r^{b_r}$. Par le lemme de Gauss, l'un des q_i vaut p_1. En appliquant le même raisonnement à tous les p_i, et vice versa avec les q_i, on trouve que $p_i = q_i$ pour tout i et $r = k$. Puis,

$$p_i^{a_i} \wedge n = p_i^{a_i} = q_i^{\min(a_i, b_i)} = q_i^{b_i} = q_i^{b_i} \wedge n,$$

donc $p_i^{a_i} = q_i^{b_i} = p_i^{b_i}$ et $a_i = b_i$. Ainsi, l'écriture est unique.

Partie III — Division euclidienne et algorithme d'Euclide

(1) Soient $n \geq 1$ et $q > 1$ deux entiers. Montrer qu'il existe un entier k et un *unique* entier r tel que $0 \leq r < q$ et $n = qk + r$. On parle de *division euclidienne de n par q*. On appelle r le *reste* et k le *quotient dans la division euclidienne.*

Indication: Commencer par montrer que r existe (par exemple, par récurrence). Montrer ensuite l'unicité en supposant que r_1 et r_2 conviennent (déduire $r_1 = r_2$).

Soit $q > 1$ un entier. On va montrer par récurrence forte sur n que r existe.

- Initialisation: $n = 1$. Le reste $r = 1$ convient ($1 = 0 \times q + 1$)
- Hérédité: On suppose que pour tout $\ell < n$, ℓ admet un reste dans la division euclidienne par q. Si $q > n$, alors $r = n$ convient ($n = 0 \times q + n$), et si $q = n$ alors $n = 1 \times q + 0$ donc $r = 0$ convient. Sinon, $1 \leq n - q < n$ donc par hypothèse de récurrence, $n - q = kq + r$ et $n = (k + 1)q + r$.
- Conclusion: tous les entiers $n \geq 1$ ont un reste dans la division euclidienne par q.

Supposons que n admet les deux restes r_1 et r_2 dans la division euclidienne par q. Alors,

$$n - n = (k_1 - k_2)q + r_1 - r_2 = 0.$$

Comme $0 \leq r_1, r_2 < q$, on a $|r_1 - r_2| \leq q - 1$. Si $k_1 \neq k_2$, on a $|(k_1 - k_2)q| \geq q > q - 1$. La somme de ces deux termes ne peut donc pas valoir 0. Ainsi, $k_1 = k_2$ donc $r_1 - r_2 = 0$ et $r_1 = r_2$.

(2) Soient $n > 1$ et $m > 1$ deux entiers. On suppose que $n > m$.

(a) On note $n = qm + r$ la division euclidienne de n par m. Montrer que $n \wedge m = m \wedge r$

Soit d un diviseur de n et m. Alors, d divise aussi $n - qm = r$ donc d est un diviseur de r. Soit maintenant d un diviseur de m et $n - qm$. Alors, d divise $n - qm + qm = n$ donc d divise n et m. Ainsi, les diviseurs simultanés de n et m sont les mêmes que les diviseurs simultanés de m et r, ce qui prouve le résultat.

(b) On définit une suite (r_k) de la manière suivante:
- $r_0 = n$
- $r_1 = m$
- r_{k+1} est le reste de la division de r_{k-1} par r_k, lorsque $r_k \neq 0$. Si $r_k = 0$, alors la suite s'arrête.

Montrer que la suite (r_k) est strictement décroissante. En déduire que c'est une suite finie (elle atteint 0), et en déduire que le dernier terme non-nul vaut $n \wedge m$.

On appelle cette méthode de calcul du PGCD l'*algorithme d'Euclide*.

Comme r_{k+1} est le reste dans une division euclidienne par r_k, on a nécessairement $r_{k+1} < r_k$, ce qui donne la décroissance stricte de (r_k). Puis, la suite ne prend que des valeurs entières postives ou nulles. La stricte décroissance des valeurs entières implique que la suite atteint 0 à un certain rang, où elle s'arrête.

Par la question précédente, on a $n \wedge m = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{k-1} \wedge r_k$ et le dernier PGCD dans cette liste est du type $r_{k-1} \wedge 0 = r_{k-1}$.

(c) Appliquer l'algorithme d'Euclide pour calculer $33 \wedge 12$.

Pour calculer $33 \wedge 12$:

$$\begin{aligned} 33 &= 2 \times 12 + 9 \\ 12 &= 1 \times 9 + \boxed{3} \\ 9 &= 3 \times 3 + 0 \end{aligned}$$

donc $33 \wedge 12 = 3$.

(3) Avec un raisonnement par récurrence, montrer que r_k s'écrit $a_k n + b_k m$ pour des entiers a_k, b_k. En déduire qu'il existe $u, v \in \mathbb{Z}$ tels que

$$n \wedge m = un + vm.$$

On appelle cette relation la *relation de Bézout*.

Initialisation: r_0 et r_1 s'écrivent bien comme combinaisons linéaires de m et n.

Hérédité: On suppose la propriété vraie aux rangs $k < \ell$. On a

$$\begin{aligned} r_\ell &= r_{\ell-2} - q r_{\ell-1} \\ &= a_{\ell-2} n + b_{\ell-2} m - q(a_{\ell-1} n + b_{\ell-1} m) \\ &= (a_{\ell-2} - q a_{\ell-1}) n + (b_{\ell-2} - q b_{\ell-1}) m. \end{aligned}$$

Conclusion: La propriété est vraie à tous les rangs. En particulier, si ℓ est le dernier indice de la suite (r_k), alors $r_{\ell-1}$ donne des valeurs de u et v qui conviennent.

(4) (a) Montrer que $k \mid n, m$ si et seulement si $k \mid n \wedge m$.

Par la relation de Bézout, $n \wedge m = un + vm$ pour des entiers u, v. Ainsi, si k divise n et m, alors $k \mid un + vm = n \wedge m$. La réciproque est immédiate

(b) Soient n, m, ℓ trois entiers, $\ell \neq 0$. Montrer que $n\ell \wedge m\ell = \ell(n \wedge m)$

ℓ divise $n\ell$ et $m\ell$ donc $n\ell \wedge m\ell = \ell d$ pour un entier d. Alors,

$$\forall k \in \mathbb{Z}, \quad k \mid n, m \iff k\ell \mid n\ell, m\ell \iff k\ell \mid n\ell \wedge m\ell \iff k \mid d$$

donc $n \wedge m = d$.

(5) Soit $d \geq 1$ tel qu'il existe $u, v \in \mathbb{Z}$ satisfaisant $d = un + vm$. Montrer que $n \wedge m \mid d$.

$n \wedge m$ divise un et vm donc $n \wedge m \mid d = un + vm$.

Partie IV — Congruences des entiers relatifs

On définit la relation de congruence $\equiv$ modulo n sur $\mathbb{Z}$ de la manière suivante. Soit $n > 1$ un entier. Alors pour tous $a, b \in \mathbb{Z}$,

$$a \equiv b \pmod{n} \iff n \mid a - b$$

(1) Montrer que $n \mid m$ si et seulement si $m \equiv 0 \pmod{n}$.

C'est précisément la définition de $m \equiv 0 \pmod{n}$.

(2) Montrer que si $a_1 \equiv a_2 \pmod{n}$ et $b_1 \equiv b_2 \pmod{n}$ alors $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$. Ainsi, la relation de congruence est compatible avec l'addition

Avec les notations de la question, $a_1 + b_1 - a_2 - b_2 = (a_1 - a_2) + (b_1 - b_2)$ qui est donc un multiple de n, ce qui conclut.

(3) Montrer que si $a_1 \equiv a_2 \pmod{n}$ et $b_1 \equiv b_2 \pmod{n}$ alors $a_1 b_1 \equiv a_2 b_2 \pmod{n}$. Ainsi, la relation de congruence est compatible avec la multiplication. Un travail similaire montre (on l'admettra donc) que la relation de congruence est compatible avec toutes les propriétés des opérations usuelles sur les entiers (distributivité, soustraction, etc).

Encore avec les mêmes notations,

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 + a_2 b_2 = a_1 (b_1 - b_2) + (a_1 - a_2) b_2$$

qui est encore un multiple de n.

(4) Soit $n > 1$ et $m \in \mathbb{Z}$. Montrer qu'il existe un unique entier $0 \leq k < n$ tel que $m \equiv k \pmod{n}$. On dit que k est le *résidu* de m modulo n. Donner les résidus de $-1, 10$ et -4 modulo 5.

k est exactement le reste dans la division euclidienne de m par n. On a déjà étudié son unicité. Les résidus respectifs de $-1, 10, -4$ modulo 5 sont $4, 0, 1$.

(5) Soient n et m deux nombres entiers positifs premiers entre eux. Montrer qu'il existe k tel que

$$mk \equiv 1 \pmod{n}.$$

On dit alors que m est *inversible* modulo n, et k est son *inverse modulaire*.

Si n et m sont premiers entre eux, alors il existe u, v tels que $un + vm = 1$ (relation de Bézout). Comme $un \equiv 0 \pmod{n}$, on trouve $vm = 1 \pmod{n}$.

(6) Montrer que m est inversible modulo n si et seulement si m et n sont premiers entre eux.

La question précédente montre que si m et n sont premiers entre eux, alors m est inversible modulo n. Supposons maintenant que m est inversible modulo n. Alors, il existe k tel que $mk \equiv 1 \pmod{n}$, donc $n \mid mk - 1$ et il existe q tel que $mk - 1 = nq$. On en déduit

$$-qn + mk = 1$$

donc $n \wedge m \mid 1$, ce qui implique $n \wedge m = 1$.

Partie V — Congruences modulo un nombre premier

Dans toute cette partie, p est un nombre premier impair.

(1) Montrer que tous les entiers non multiples de p sont inversibles modulo p.

Si k est un entier non multiple de p, alors $k \wedge p = 1$ donc k est inversible modulo p.

(2) Soit a non multiple de p.

(a) Soient u, v des entiers compris entre 0 et $p-1$ (bornes incluses). Montrer que

$$ua \equiv va \pmod{p} \iff u = v$$

Le sens ($\Longleftarrow$) est immédiat. Supposons $ua \equiv va \pmod{p}$, en reprenant les notations de la question. Alors

$$p \mid (u-v)a,$$

et comme $p \wedge a = 1$, le lemme de Gauss donne

$$p \mid u - v$$

de sorte que $u \equiv v \pmod{p}$. Comme u et v sont compris entre 0 et $p-1$, ils sont leurs propres résidus. Par unicité du résidu, $u = v$.

(b) En déduire que la liste des résidus de $a, 2a, 3a, \cdots, (p-1)a$ est une permutation de la liste $(1, \cdots, p-1)$.

Les nombres $a, 2a, 3a, \cdots, (p-1)a$ sont deux à deux distincts modulo p par la question précédente, de sorte que les résidus sont également deux à deux distincts. Puis, il y en a exactement le bon nombre $(p-1)$, donc il s'agit forcément d'une permutation de $(1, \cdots, p-1)$.

(c) Montrer que

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

On fait le produit $a \times 2a \times 3a \times \cdots \times (p-1)a$ pour obtenir

$$a^{p-1}(p-1)!$$

en regroupant tous les a et en regroupant les facteurs $1, \cdots, p-1$ dans la factorielle. Vu la question précédente, ce produit vaut également $(p-1)!$ modulo p.

(3) (Petit théorème de Fermat) Déduire de ce qui précède que pour tout entier $n \in \mathbb{Z}$,

$$n^p \equiv n \pmod{p}.$$

Indication: Séparer les cas $n \equiv 0 \pmod{p}$ et $n \not\equiv 0 \pmod{p}$. Dans le second cas, montrer $a^{p-1} \equiv 1 \pmod{p}$.

On se place dans le cadre de la question précédente. Comme $(p-1)!$ est un produit de termes inversibles (chacun des entier du produit n'est pas un multiple de p), on en déduit que $(p-1)!$ est inversible d'inverse q. Alors

$$\begin{aligned} & a^{p-1}(p-1)!q \equiv (p-1)!q \pmod{p} \\ \implies & a^{p-1} \equiv 1 \pmod{p} \end{aligned}$$

On a donc bien trouvé le bon résultat lorsque $a \not\equiv 0 \pmod{p}$. Si $a \equiv 0 \pmod{p}$, il n'y a rien à faire car $a^{p-1} \equiv 0 \equiv a$.

Partie VI — Théorème de Wilson

Dans cette partie, on veut montrer le théorème de Wilson: p est premier si et seulement si

$$(p-1)! \equiv -1 \pmod{p}.$$

(1) Montrer que le théorème est vérifié pour $p = 2$.

Pour $p = 2$, $(p-1)! = 1! = 1$ et $1 \equiv -1 \pmod{2}$ donc le théorème est vérifié.

(2) Supposons que $(p-1)! \equiv -1 \pmod p$. Montrer que tous les entiers non multiples de p sont inversibles, et en déduire que p est premier.

Supposons que $(p-1)! = -1 \pmod p$. Soit k un entier non multiple de p. On sait que k est inversible si et seulement si son résidu est inversible. On suppose donc $0 \leq k < p-1$. On sait par ailleurs que $k \neq 0$ car 0 est un multiple de p. Ainsi,

$$-(p-1)! = -1 \times 2 \times 3 \times \cdots \times (k-1) \times k \times (k+1) \cdots \times (p-1) = 1 \pmod p,$$

de sorte que k soit inversible d'inverse

$$-1 \times 2 \times \cdots \times (k-1) \times (k+1) \times \cdots \times (p-1) = -\frac{(p-1)!}{k} \in \mathbb{Z}.$$

(3) Supposons maintenant que p est un nombre premier impair.

(a) Montrer que seuls -1 et 1 sont leur propre inverse modulaire.

Supposons que $k \in \mathbb{Z}$ est son propre inverse. Alors, $k^2 \equiv 1 \pmod p$ donc

$$p \mid k^2 - 1 = (k-1)(k+1).$$

Alors, comme p est premier et $p > 2$, on a soit $p \wedge (k-1) = 1$ soit $p \wedge (k+1) = 1$. Donc, p divise soit $(k+1)$ soit $k-1$. Dans les deux cas, on trouve que $k \equiv \pm 1 \pmod p$.

(b) Conclure.

Dans le produit $(p-1)! = 1 \times \cdots \times (p-1)$, les facteurs 1 et $(p-1) \equiv -1$ sont leur propre inverse et ne sont donc pas inversés (ils n'apparaissent qu'une fois). Le produit de ces deux termes vaut -1 modulo p. Chacun des autres termes du produit est accompagné de son inverse ailleurs dans le produit (les termes sont donc couplés en groupes de deux nombres inverses l'un de l'autre). Le produit de tous ces termes vaut donc 1. Finalement, $(p-1)! \equiv -1 \pmod p$.

(4) On donne $10! = 3\ 628\ 800$. D'après le théorème, 11 est-il premier ?

$10! \equiv 10 \equiv -1 \pmod{11}$ donc 11 est premier.

Partie VII — Valuations p-adiques

Soit p un nombre premier. On appelle *valuation p-adique* d'un entier $n \neq 0$ le plus grand entier k tel que $p^k \mid n$. On la note $v_p(n)$. On prend la convention $v_p(0) = +\infty$.

(1) Montrer que $v_p(ab) = v_p(a) + v_p(b)$ pour tous $a, b > 0$.

$p^{v_p(a)} \mid a$ et $p^{v_p(b)} \mid b$ donc $p^{v_p(a)+v_p(b)} \mid ab$ donc $v_p(ab) \geq v_p(a) + v_p(b)$. Puis, si $p^{v_p(a)+v_p(b)+1} \mid ab$, alors

$$p \mid \frac{a}{p^{v_p(a)}} \times \frac{b}{p^{v_p(b)}}$$

ce qui est absurde car les deux fractions sont des entiers premiers avec p. Ainsi, $v_p(ab) < v_p(a) + v_p(b) + 1$ ce qui conclut.

(2) Montrer que si $b \mid a$, alors $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$

On utilise la question 1: $v_p(a) = v_p\left(\frac{a}{b}\right) + v_p(b)$.

(3) Montrer que $v_p(a+b) \geq \min\big(v_p(a), v_p(b)\big)$

Soit $k = \min\big(v_p(a), v_p(b)\big)$. Alors $p^k \mid a$, $p^k \mid b$ donc $p^k \mid a+b$, d'où $v_p(a+b) \geq k$.

(4) Soient a_1, b_1, a_2, b_2 des entiers, b_1 et b_2 non nuls, tels que $a_1 b_2 = a_2 b_1$. Montrer que

$$v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2).$$

En déduire que si $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ pour $a, b \in \mathbb{Z} \setminus \{0\}$, on peut définir $v_p(x) = v_p(a) - v_p(b)$ sans que cette définition ne dépende du choix de a et b. Ainsi, la valuation p-adique est définie sur $\mathbb{Q}$.

Supposons que $x = \frac{a_1}{b_1} = \frac{a_2}{b_2}$ sont deux écritures du même rationnel $x \in \mathbb{Q} \setminus \{0\}$. C'est équivalent à $a_1 b_2 = a_2 b_1$. On applique le résultat de la question (1) pour trouver

$$v_p(a_1) + v_p(b_2) = v_p(a_2) + v_p(b_1)$$

ce qui est équivalent à l'identité recherchée (en réarrangeant l'égalité). Ainsi, la définition proposée pour $v_p(x)$ ne dépend pas du choix d'entiers a, b pour l'écriture fractionnaire.

On appelle *partie entière* du réel $x \in \mathbb{R}$ l'unique entier $k \in \mathbb{N}$ tel que

$$x - 1 < k \leq x.$$

On la note $\lfloor x \rfloor$. On souhaite montrer la *formule de Legendre*, valable pour tout p premier et pour tout entier naturel non nul n:

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

(5) Montrer qu'il s'agit d'une somme finie: à partir d'un certain rang, tous les termes sont nuls.

Si p est premier, alors $p > 1$ de sorte qu'il existe $k \geq 1$ tel que $p^k > n$. Dans ce cas, $0 \leq \frac{n}{p^k} < 1$ et $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$, ce qui reste vrai pour tous les termes suivants. Ainsi, la somme n'a qu'un nombre fini de termes non nuls.

(6) Montrer qu'il y a $\left\lfloor \frac{n}{p} \right\rfloor$ multiples de p dans l'ensemble $\{1, 2, \cdots, n\}$. Combien y a-t-il de multiples de p^2 ?

$k \in \{1, 2, \cdots, n\}$ est multiple de p s'il s'écrit pq pour un $q \in \mathbb{N}$ tel que $pq \leq n$, autrement dit $q \leq \frac{n}{p}$. Le plus grand entier q inférieur à $\frac{n}{p}$ est (par définition) $\left\lfloor \frac{n}{p} \right\rfloor$.

Pour compter les multiples de p^2, on fait la même chose: il faut $pq^2 \leq n$ donc $q \leq \frac{n}{p^2}$ et il y a $\left\lfloor \frac{n}{p^2} \right\rfloor$ valeurs possibles.

(7) En utilisant $n! = 1 \times \cdots \times n$, montrer la formule de Legendre.

On a $v_p(n!) = v_p(1) + \cdots + v_p(n)$. Chaque multiple de p entre 1 et n apporte donc une contribution d'un facteur p dans $n!$. Chaque multiple de p^2 apporte une seconde contribution d'un facteur p dans le produit, etc pour tous les p^k.

Partie VIII — Équations diophantiennes linéaires

On appelle équation diophantienne toute équation donc on ne cherche que des solutions entières. Une équation diophantienne linéaire à n variables $x_1, \cdots, x_n$ est une équation du type

$$a_1 x_1 + \cdots + a_n x_n = c$$

où $a_1, \cdots, a_n, c$ sont des entiers et pour laquelle on cherche des solutions $x_1, \cdots, x_n \in \mathbb{Z}$.

(1) Dans cette question, on note (E) l'équation

$$ax + by = c,$$

où a, b, c sont des entiers, a et b sont non nuls. On note (E_h) l'équation $\frac{a}{d}x + \frac{b}{d}y = 0$ avec $d = a \wedge b$, que l'on appelle équation *homogène réduite* associée à (E).

(a) Montrer que (E) admet une solution si et seulement si $a \wedge b$ divise c.

Si (E) admet une solution, alors $a \wedge b \mid ax + by = c$. Réciproquement, si $a \wedge b \mid c$, alors $c = (a \wedge b)k$ pour un $k \in \mathbb{Z}$. Il existe u, v tels que $au + bv = a \wedge b$ donc (uk, vk) est solution.

(b) On suppose désormais que l'on connait une solution de (E) notée (x_0, y_0). Montrer que $(x + x_0, y + y_0)$ est solution de (E) si et seulement si (x, y) est solution de (E_h).

Si (x, y) est solution de (E_h), alors

$$a(x + x_0) + b(y + y_0) = (ax + by) + ax_0 + by_0 = d \times 0 + c = c$$

Réciproquement, supposons que $(x + x_0, y + y_0)$ soit solution de (E), alors

$$\begin{aligned}\frac{a}{d}x + \frac{b}{d}y &= \frac{a}{d}(x + x_0 - x_0) + \frac{b}{d}(y + y_0 - y_0) \\ &= \frac{1}{d}(a(x + x_0) + b(y + y_0)) - \frac{1}{d}(ax_0 + bx_0) \\ &= \frac{1}{d} \times c - \frac{1}{d} \times c = 0.\end{aligned}$$

(c) Supposons que (x, y) est solution de (E_h). Montrer que $\frac{b}{d}$ divise x et $\frac{a}{d}$ divise y. En déduire qu'il existe k tel que

$$x = \frac{b}{d}k, \quad y = -\frac{a}{d}k.$$

$$\frac{b}{d}y = -\frac{a}{d}x$$

donc $\frac{b}{d}$ divise $-\frac{a}{d}x$ or $\frac{b}{d} \wedge \frac{a}{d} = 1$ donc $\frac{b}{d}$ divise x (lemme de Gauss), et $x = \frac{b}{d}k$. En injectant cette écriture dans l'équation, on trouve

$$\frac{b}{d}y = -\frac{a}{d}\frac{b}{d}k$$

donc $y = -\frac{a}{d}k$.

(d) Montrer que pour tout $k \in \mathbb{Z}$.

$$x = \frac{b}{d}k, \quad y = -\frac{a}{d}k$$

est solution de (E_h).

On injecte dans l'équation, le calcul est immédiat.

(e) En déduire que les solutions de (E) sont exactement les couples de la forme

$$\left(\frac{b}{d}k + x_0, -\frac{a}{d}k + y_0\right), \quad k \in \mathbb{Z}.$$

Les solutions de (E_h) sont entièrement décrites dans les deux questions précédentes, et on a vu que pour obtenir les solutions de (E), il suffit d'ajouter (x_0, y_0) aux solutions de (E_h). On trouve la description de l'énoncé.

(2) Résoudre $-12x + 16y = 20$.

$-12 \wedge 16 = 4 \mid 20$ donc des solutions existent. Une solutions particulière est $x_0 = y_0 = 5$. Les solutions sont donc les

$$(4k + 5, 3k + 5), \quad k \in \mathbb{Z}$$

Partie IX — Descente infinie dans une équation diophantienne

Soit p un nombre premier et $n \geq 3$. On s'intéresse à l'équation diophantienne suivante:

$$x^n + py^n = p^2 z^n$$

(1) Montrer que $(0,0,0)$ est solution. On note $N(x,y,z) = |x| + |y| + |z|$. Montrer que si $(x,y,z) \neq (0,0,0)$, alors $N(x,y,z) > 0$.

Si $(x,y,z) \neq 0$ alors par exemple $x \neq 0$ donc $|x| > 0$, et comme $|y| \geq 0, |z| \geq 0$ on trouve bien $N(x,y,z) > 0$.

(2) On suppose qu'il existe une solution différente de $(0,0,0)$. Montrer qu'il existe une solution $(x,y,z) \neq (0,0,0)$ telle que $N(x',y',z') \geq N(x,y,z)$ pour toute solution non nulle (x',y',z'). Dans la suite, (x,y,z) désigne une telle solution.

Notons (a,b,c) la solution non nulle connue, et $k = N(a,b,c)$. Alors, il y a un nombre fini de triplets (x,y,z) tels que $0 < N(x,y,z) \leq k$, donc un nombre fini de solutions (x,y,z) tels que $0 < N(x,y,z) \leq k$. Par ailleurs, cet ensemble n'est pas vide puisqu'il contient (a,b,c). Ainsi, on peut en choisir un élément minimal pour N.

(3) Montrer que p divise x^n. En déduire qu'il existe x' tel que

$$p^{n-1}x'^n + y^n = pz^n.$$

$x^n = p(pz^n - y^n)$ donc $p \mid x^n$ donc $p \mid x$ et $x = px'$. On trouve immédiatement l'égalité recherchée.

(4) Montrer que p divise y puis que p divise z. En déduire qu'il existe une solution (x',y',z') telle que $N(x',y',z') < N(x,y,z)$.

$y^n = p(z^n - p^{n-2}x'^n)$ donc $p \mid y$ (car $n-2 > 0$ puisque $n \geq 3$). Il existe donc y' tel que

$$p^{n-1}x'^n + p^n y'^n = pz^n$$

soit encore $p^{n-2}x'^n + p^{n-1}y'^n = z^n$ donc $p \mid z$ et on trouve ainsi une solution (x',y',z').

Cette solution satisfait bien $N(x',y',z') < N(x,y,z)$ car $|x'| = |\frac{x}{p}| \leq |x|$, idem pour les autres coordonnées, avec l'inégalité stricte pour chaque coordonnée non nulle (c'est à dire au moins l'une des trois puisque $(x,y,z) \neq 0$.

(5) Conclure que l'équation n'a qu'une seule solution.

On a montré que si (x,y,z) est une solution non nulle minimale pour N, alors on peut construire une solution (x',y',z') strictement plus petite pour N et encore non nulle. C'est absurde, donc il n'existe pas de solutions non nulles de l'équation. La seule solution est la solution nulle.

Partie X — Triplets pythagoriciens

On appelle *triplet pythagoricien* toute solution entière (x,y,z) de l'équation diophantienne

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

On dit qu'un triplet pythagoricien (x,y,z) est *primitif* lorsque $x \wedge y \wedge z = 1$.

(1) Soit (x,y,z) un triplet pythagoricien et $d = x \wedge y \wedge z$. Montrer que $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ est un triplet pythagoricien primitif.

C'est encore un triplet pythagoricien (l'équation est homogène: on peut multiplier un triplet pythagoricien par n'importe quelle constante pour obtenir un autre triplet pythagoricien). Il est

primitif car $d = x \wedge y \wedge z = \left(d\frac{x}{d}\right) \wedge \left(d\frac{y}{d}\right) \wedge \left(d\frac{z}{d}\right) = d\left(\left(\frac{x}{d}\right) \wedge \left(\frac{y}{d}\right) \wedge \left(\frac{z}{d}\right)\right)$ donc en divisant par d on trouve que le PGCD des trois termes vaut 1.

(2) (a) Soit (x, y, z) un triplet pythagoricien primitif. Montrer que $x \wedge y = y \wedge z = x \wedge z = 1$.

Indication: Montrer que si un premier p divise deux termes, alors il divise le troisième.

Supposons que p est un nombre premier qui divise x et y. Alors, p divise $x^2 + y^2$ donc $p \mid z^2$ et comme p est premier, $p \mid z$. Donc, $p \mid x \wedge y \wedge z = 1$ ce qui est absurde. Donc, $x \wedge y$ n'a aucun diviseur premier: il vaut 1. C'est le même raisonnement pour les deux autres PGCD.

(b) Soit (x, y, z) un triplet pythagoricien primitif. Montrer que x et y ont des parités différentes[2].

Indication: Montrer que si x et y sont impairs, alors $z^2 \equiv 2 \pmod 4$. Est-il possible pour un carré de valoir 2 modulo 4 ?

Supposons que x et y sont pairs. Alors $z^2 = x^2 + y^2$ est pair, donc z est pair et le triplet n'est pas primitif. On en déduit que x et y ne sont pas tous les deux pairs.

Supposons maintenant que x et y sont impairs. Les nombres impairs sont congrus à 1 ou 3 modulo 4, et $1^2 \equiv 1 \pmod 4$, $3^2 \equiv 9 \equiv 1 \pmod 4$, donc le carré d'un nombre impair sera toujours congru à 1 modulo 4. Ainsi, $z^2 \equiv x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$.

Il reste à vérifier que 2 n'est pas un carré modulo 4. La liste exhaustive des résidus qui sont des carrés est donnée par $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 0, 3^2 \equiv 1 \pmod 4$. Donc, les résidus qui sont des carrés sont 0 et 1. Ainsi, il est impossible d'avoir $z^2 \equiv 2 \pmod 4$, ce qui montre que x et y ne peuvent pas être tous les deux impairs.

(c) Montrer que deux entiers naturels premiers entre eux dont le produit est un carré parfait (c'est à dire k^2 pour un entier k) sont eux-même des carrés parfaits.

Indication: Montrer que dans les décompositions en facteurs premiers, les exposants sont pairs.

Soient r, s deux entiers tels que $rs = k^2$ avec $r \wedge s = 1$. On écrit les décompositions en facteurs premiers:

$$r = p_1^{a_1} \cdots p_n^{a_n}$$
$$s = q_1^{b_1} \cdots q_m^{b_m}$$

Comme $r \wedge s = 1$, on en déduit que les $\{p_1, \cdots, p_n\}$ et les $\{q_1, \cdots q_m\}$ sont disjoints (i.e. on n'a jamais $p_i = q_j$ car sinon $p_i \mid r \wedge s = 1$). On en conclut que

$$k^2 = p_1^{a_1} \cdots p_n^{a_n} q_1^{b_1} \cdots q_m^{b_m}$$

est la décomposition en facteurs premiers de k^2. Comme c'est un carré parfait, chacun des exposants $a_1, \cdots, b_m$ doit être pair (pour le voir: faire la décomposition en facteurs premiers de k et la mettre au carré: tous les exposants sont pairs et on sait que la décomposition est unique).

Ainsi, tous les a_i sont pairs et tous les b_i sont pairs, donc r et s sont chacun des carrés parfaits.

(3) On va montrer que l'ensemble des triplets primitifs positifs S pour lesquels y est pair est donné par

$$(x, y, z) \in S \iff \exists m, n \in \mathbb{N}, m > n, m \wedge n = 1, m \not\equiv n \pmod 2, \begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases}$$

Soit (x, y, z) un triplet primitif positif avec y pair.

[2] Parités différentes: l'un est pair, l'autre impair.

(a) Montrer que $z+x$ et $z-x$ sont pairs. En déduire que $r=\frac{z+x}{2}$ et $s=\frac{z-x}{2}$ sont premiers entre eux, puis que ce sont des carrés parfaits. On note $r=m^2$ et $s=n^2$.

Comme x et y n'ont pas la même parité et que y est pair, x est impair, et z est impair aussi (car $z^2=x^2+y^2$ est impair). Donc, $z+x$ et $z-x$ sont pairs. Puis,

$$rs=\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)=\frac{z^2-x^2}{4}=\left(\frac{y}{2}\right)^2.$$

Si d un diviseur de r et s, alors d divise $r+s=z$ et $r-s=x$ donc p divise $x\wedge z=1$. On en déduit que $r\wedge s=1$. Par la question (2.c), r et s sont des carrés parfaits.

(b) Montrer que

$$\begin{cases} x=m^2-n^2 \\ y=2mn \\ z=m^2+n^2 \end{cases}$$

et que $m\wedge n=1$. Montrer que m et n n'ont pas la même parité.

On a $x=r-s=m^2-n^2$, $y=2\sqrt{\left(\frac{y}{2}\right)^2}=2\sqrt{rs}=2mn$, et $z=r+s=m^2+n^2$. Puis, $m\wedge n$ divise $x\wedge z=1$ donc $m\wedge n=1$.

(c) Conclure.

On a bien $r>s$ donc $m>n$. On a montré $n\wedge m=1$, on a de plus $m\not\equiv n\pmod 2$ car sinon x, y et z sont tous pairs, ce qui est faux pour un triplet pythagoricien primitif.

Réciproquement, si m et n vérifient ces conditions, alors on vérifie aisément que (x,y,z) est un élément de S, ce qui conclut la description.

On va maintenant adopter une approche géométrique pour résoudre le même problème.

(4) Montrer que (x,y,z) est un triplet pythagoricien non nul si et seulement si $\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1$. En déduire qu'il y a une correspondance entre les triplets pythagoriciens non nuls primitifs et les points rationnels[3] (x,y) du cercle unité.

Il suffit de diviser/multiplier par z^2 toute l'équation.

Pour la correspondance, il suffit d'envoyer un triplet pythagoricien non nul primitif (x,y,z) sur $\left(\frac{x}{z},\frac{y}{z}\right)$ qui est alors un point rationnel du cercle unité. Pour trouver la correspondance inverse, on remarque que pour chaque point rationnel (x,y) du cercle, il n'y a qu'un unique entier naturel non nul d tel que (xd,yd,d) est est triplet pythagoricien primitif (et d est le plus petit entier naturel non nul tel que xd et yd soient deux entiers, le PGCD $xd\wedge yd\wedge d$ valant automatiquement 1).

(5) On note désormais I le point $(-1,0)$. Montrer que si $P=(x,y)$ est un point rationnel du cercle unité, alors la droite (IP) a une pente rationnelle.

La droite (IP) a pour pente

$$\frac{x_P-x_I}{y_P-y_I}=\frac{x_P-1}{y_P}$$

qui est donc rationnelle lorsque P est un point rationnel.

(6) Pour $t\in\mathbb{Q}$, on note $\mathcal{D}_t : y=t(x+1)$.

(a) Montrer que toutes les droites de pente rationnelles passant par I s'écrivent $\mathcal{D}_t$ pour un $t\in\mathbb{Q}$.

[3] Le point (x,y) est rationnel lorsque $x,y\in\mathbb{Q}$

Si $\mathcal{D}$ est une droite de pente $t \in \mathbb{Q}$ passant par I, alors son équation est du type $y = tx + c$ avec $0 = -t + c$ donc $c = t$ et $y = t(x+1)$.

(b) Soit $P = (x, y)$ un point d'intersection de $\mathcal{D}_t$ et du cercle unité $x^2 + y^2 = 1$. Montrer que

$$(x+1)\big((x-1) + t^2(x+1)\big) = 0.$$

En déduire que

$$x = -1 \quad \text{ou} \quad x = \frac{1-t^2}{1+t^2}.$$

Montrer que si $x = -1$, alors $P = I$. Sinon, montrer que P a les coordonnées

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

Soit P comme dans l'énoncé. Alors, $y = t(x+1)$ et P est sur le cercle unité donc

$$x^2 + t^2(x+1)^2 = 1$$

soit encore,

$$x^2 - 1 + t^2(x+1)^2 = 0$$

ce qui donne

$$(x+1)\big((x-1) + t^2(x+1)\big) = 0$$

donc $x = -1$ ou bien

$$x - 1 + t^2(x+1) = 0$$

soit encore $x(1+t^2) = 1 - t^2$ donc

$$x = \frac{1-t^2}{1+t^2}.$$

Si $x = -1$, alors $y = t(x+1) = 0$ donc $P = I$. Sinon,

$$y = t(x+1) = \frac{2t}{1+t^2}.$$

(c) Montrer que pour $t \in \mathbb{Q}$, les points d'intersection de $\mathcal{D}_t$ et du cercle unité sont rationnels. En déduire que les points rationnels du cercle unité sont I et tous les points

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right), \quad t \in \mathbb{Q}.$$

Si t est rationnel, on a trouvé en question précédente les coordonnées du point P d'intersection de $\mathcal{D}_t$ et du cercle unité. Ces coordonnées sont rationnelles si t est rationnel.

Si un point P est un point rationnel du cercle, alors on a vu que la pente de (IP) est rationnelle, disons $t \in \mathbb{Q}$ de sorte que P appartient à $\mathcal{D}_t$ et P a l'expression donnée dans l'énoncé.

(d) Soit $t \in \mathbb{Q}$. Comme t est rationnel, il s'écrit $t = \frac{m}{n}$ avec $m \in \mathbb{Z}$, $n \in N^*$, $m \wedge n = 1$. Montrer que

$$(m^2 - n^2, 2mn, m^2 + n^2)$$

est un triplet pythagoricien.

On a

$$\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1$$

donc

$$\left(\frac{n^2-m^2}{n^2+m^2}\right)^2 + \left(\frac{2nm}{n^2+m^2}\right)^2 = 1$$

et

$$(n^2-m^2)^2 + (2nm)^2 = (n^2+m^2)^2$$

de sorte que $(m^2 - n^2, 2nm, n^2 + m^2)$ est un triplet pythagoricien primitif.

Partie XI — Indicatrice d'Euler

On appelle indicatrice d'Euler la fonction φ dont la définition est la suivante: pour tout $n > 0$ entier, $\varphi(n)$ est le nombre d'entiers entre 1 et $n - 1$ qui sont premiers avec n.

(1) Soit p un nombre premier.

(a) Montrer que $\varphi(p) = p - 1$

Si $1 \leq k \leq p$, alors k est permier avec p sauf si $k = p$. Il y a donc $p - 1$ choix possibles.

(b) Montrer pour tout $k > 1$, $\varphi(p^k) = (p-1)p^{k-1}$.

On compte: $p^k - \varphi(p^k)$ est le nombre d'entiers entre 1 et p^k qui ne sont **pas** premiers avec p^k. Comme p est premier, x n'est pas premier avec p^k si et seulement si x est un multiple de p. Il y a exactement p^{k-1} multiples de p compris entre 1 et p^k (ce sont les $\{p, 2p, \cdots, p^{k-1}p\}$). Donc, $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

(2) Soit p un nombre premier et n un entier premier avec p. Soit $k \geq 1$ un entier. On appelle E et E' les ensembles suivants:

$$E = \{x \in \mathbb{N}^*, \quad x \wedge p^k n = 1 \quad \text{et} \quad x \leq p^k n\}$$
$$F = \{x \in \mathbb{N}^*, x \wedge n = 1 \quad \text{et} \quad x \leq p^k n\}$$

(a) Montrer que E est inclus dans F.

Soit $x \in E$. Alors, x est premier avec $p^k n$ donc x est premier avec n. Ainsi, $x \in F$ et $E \subset F$.

(b) Montrer que F possède $p^k \varphi(n)$ éléments.

Soit x un entier naturel non nul et x' son résidu modulo n

$$\begin{aligned} x \in F &\iff x \text{ inversible mod } n \quad \text{et} \quad x \leq p^k n \\ &\iff x' \text{ inversible mod } n \quad \text{et} \quad x \leq p^k n \\ &\iff x' \wedge n = 1 \quad \text{et} \quad x \leq p^k n \end{aligned}$$

et comme les valeurs possibles de $x \leq p^k n$ associées à un résidu x' sont les $\{x', x'+n, \cdots, x'+(p^k-1)n\}$ (il y en a p^k), on a que F est composé de p^k copies de l'ensemble des résidus inversibles modulo n, lui même de taille $\varphi(n)$. Donc, F est de taille $p^k\varphi(n)$.

(c) Montrer que $F \setminus E$ possède $p^{k-1}\varphi(n)$ éléments.

Les éléments de $F \setminus E$ sont des multiples de p (car ils ne sont pas premiers avec p^k), donc de la forme ℓp. Les choix de ℓ qui conviennent sont exactement les $\ell \leq np^{k-1}$ tels que $\ell \wedge n = 1$ (car $\ell p \in F \Rightarrow \ell \wedge n = 1$ puisque $p \wedge n = 1$).

Ainsi, il y a bien exactement $\varphi(n)p^{k-1}$ choix pour ℓ, ce qui conclut.

(d) En déduire que $\varphi(p^k n) = \varphi(p^k)\varphi(n)$

E possède $\varphi(p^k n)$ éléments, et $E = F \setminus (F \setminus E)$ donc

$$\varphi(p^k n) = p^k\varphi(n) - p^{k-1}\varphi(n) = (p-1)p^{k-1}\varphi(n) = \varphi(p^k)\varphi(n)$$

(3) Soient u, v premiers entre eux. Montrer que $\varphi(uv) = \varphi(u)\varphi(v)$. On dit que φ est *multiplicative*.

On fait les décompositions en facteurs premiers puis on applique le résultat précédent.

(4) Montrer que si $n = p_1^{k_1} \cdots p_r^{k_r}$ alors

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\begin{aligned} \varphi(n) &= \varphi\left(p_1^{k_1}\right) \cdots \varphi\left(p_r^{k_r}\right) \\ &= (p_1 - 1)p_1^{k_1 - 1} \cdots (p_r - 1)\left(p_r^{k_r}\right) \\ &= p_1^{k_1 - 1} \cdots p_r^{k_r - 1}(p_1 - 1) \cdots (p_r - 1) \\ &= \frac{n}{p_1 \cdots p_r}(p_1 - 1) \cdots (p_r - 1) \\ &= n\frac{p_1 - 1}{p_1} \cdots \frac{p_r - r}{p_r} \\ &= n \times \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \end{aligned}$$

(5) Dans cette question, on souhaite montrer l'identité suivante:

$$\forall n \in \mathbb{N}^*, \quad n = \sum_{d \mid n} \varphi(d),$$

où la somme porte sur l'ensemble des diviseurs d de n.

(a) Montrer que l'identité est vérifiée pour $n = p$ avec p un nombre premier, et pour $n = p^k$ pour p premier et $k > 1$.

Les seuls diviseurs de p premier sont p et 1, et $\varphi(1) = 1, \varphi(p) = p - 1$, donc la formule est vraie pour $n = p$ premier.

Pour $k > 1$, les diviseurs de p^k sont exactement les p^ℓ pour $0 \leq \ell \leq k$ On a bien

$$\begin{aligned}\sum_{d \mid p^k} \varphi(d) &= \varphi\big(p^k\big) + \varphi\big(p^{k-1}\big) + \cdots + \varphi(1)\\ &= \big(p^k - p^{k-1}\big) + \big(p^{k-1} - p^{k-2}\big) + \cdots + 1\\ &= p^k + \big(-p^{k-1} + p^{k-1}\big) + \big(-p^{k-2} + p^{k-2}\big) + \cdots + (-1+1)\\ &= p^k + 0 + \cdots + 0 = p^k\end{aligned}$$

(b) Soient $m, n > 0$ deux entiers premiers entre eux. On suppose que la formule est vraie pour m et pour n. Montrer que

$$mn = \sum_{d \mid mn} \varphi(d).$$

Indication: Montrer que les diviseurs de mn s'écrivent de manière unique comme un produit $d_1 d_2$ où $d_1 \mid m$ et $d_2 \mid n$. Que dire de $d_1 \wedge d_2$?

L'indication découle immédiatement des décompositions en facteurs premiers respectives de m et n. On a bien sûr $d_1 \wedge d_2 = 1$.

On a

$$\begin{aligned}\sum_{d \mid mn} \varphi(d) &= \sum_{\substack{d_1 \mid m\\ d_2 \mid n}} \varphi(d_1 d_2)\\ &= \sum_{d_1 \mid m} \varphi(d_1) \times \sum_{d_2 \mid n} \varphi(d_2)\\ &= m \times n\end{aligned}$$

d'où la formule.

(c) En déduire l'identité pour tout $n \in \mathbb{N}^*$.

On décompose en facteurs premiers, et c'est immédiat vu ce qu'on a fait.

(6) Dans cette question, pour $n > 1$ fixé et x un entier, on note $\overline{x}$ le résidu de x modulo n.

(a) Montrer que l'ensemble des résidus inversibles modulo n est un ensemble $U = \{x_1, \cdots, x_k\}$ de taille $\varphi(n)$.

Inversible modulo n = premier avec n.

(b) Montrer que $xU \coloneqq \{\overline{xx_1}, \overline{xx_2}, \cdots, \overline{xx_k}\} = U$. Indication: Montrer que chacun des $\overline{xx_i}$ est inversible modulo n et que $\overline{xx_i} \neq \overline{xx_j}$ lorsque $i \neq j$.

On a clairement $xU \subseteq U$ car chacun des $\overline{xx_i}$ sont inversibles (c'est un résidu d'un produit d'inversibles). Puis, $\overline{xx_i} \neq \overline{xx_j}$ car $xx_i \equiv xx_j \pmod n \iff x_i \equiv x_j \pmod n$. Donc, il y a autant d'éléments dans xU que dans U. Donc, $xU = U$.

(c) En déduire que $x_1 \cdot x_k \equiv x^k \cdot x_1 \cdots x_k \pmod n$

$$x_1 \cdots x_k \equiv \overline{xx_1} \cdots \overline{xx_k} = \overline{x}^k \overline{x_1} \cdots \overline{x_k} \equiv x^k x_1 \cdots x_k \pmod n$$

(d) Démontrer le *Théorème d'Euler*: pour tout $n > 1$ et tout x premier avec n, $x^{\varphi(n)} \equiv 1 \pmod n$.

Dans le produit précédent, $x_1 \cdots x_k$ est inversible (produit d'inversibles). Il suffit de l'inverser pour trouver $x^k \equiv 1 \pmod n$. Par ailleurs, on avait montré $k = \varphi(n)$ en (6.a).

Partie XII — Ordre multiplicatif

Soit $n > 1$ et x un entier. On appelle *ordre multiplicatif* de x modulo n le plus petit entier $k \geq 1$ tel que $x^k \equiv 1 \pmod{n}$, lorsqu'un tel entier existe. Dans ce cas, on dit que x admet un ordre modulo n, et on note $o_n(x)$ cet ordre.

(1) Supposons que x et n sont premiers entre eux.

(a) Montrer qu'il existe $1 \leq k_1 < k_2$ deux entiers tels que $x^{k_1} \equiv x^{k_2} \pmod{n}$.

Il n'y a qu'un nombre fini de résidus possibles modulo n, mais un nombre infini de $k \geq 1$. Il y en a donc au moins deux entiers x^k qui ont le même résidu modulo n, car sinon il y aurait un nombre infini de résidus (on parle de principe des tiroirs).

(b) En déduire que $x^{k_2-k_1} \equiv 1 \pmod{n}$. Conclure que x admet un ordre modulo n.

x est inversible modulo n d'inverse y.

$$x^{k_2-k_1}x^{k_1} \equiv x^{k_2} \equiv x^{k_1} \pmod{n} \Rightarrow x^{k_2-k_1} \equiv 1 \pmod{n}$$

en multipliant chaque côté par y^{k_1}.

(2) Supposons que x et n ne sont pas premiers entre eux. Est-il possible pour x d'admettre un ordre modulo n ?

Si x admet un ordre (disons k), alors x est inversible d'inverse x^{k-1}, ce qui est impossible si x et n ne sont pas premiers entre eux.

(3) Soit x un entier premier avec n.

(a) Supposons que m est un multiple de $o_n(x)$. Montrer que $x^m \equiv 1 \pmod{n}$.

$m = o_n(x)k$ donc $x^m = \left(x^{o_n(x)}\right)^k \equiv 1^k \equiv 1 \pmod{n}$.

(b) Supposons désormais que $x^m \equiv 1 \pmod{n}$. Montrer que $o_n(x)$ divise m.

Indication: Faire la division euclidienne de m par $o_n(x)$, et exploiter la minimalité de $o_n(x)$.

On fait la division euclidienne: $m = qo_n(x) + r$ avec $0 \leq r < o_n(x)$. Donc,

$$x^m \equiv \left(x^{o_n(x)}\right)^m x^r \equiv x^r \equiv 1 \pmod{n}$$

ce qui est impossible si $0 < r < o_n(x)$ car sinon $o_n(x)$ n'est pas l'entier minimal k pour lequel $x^k \equiv 1 \pmod{n}$. Donc, $r = 0$ et $m = qo_n(x)$.

(c) Montrer que $o_n(x)$ divise $\varphi(n)$.

On a vu (théorème d'Euler) $x^{\varphi(n)} \equiv 1 \pmod{n}$. Par la question précédente, $o_n(x) \mid \varphi(n)$.

Partie XIII — Racines primitives modulo un nombre premier

On appelle *racine primitive* modulo n tout entier x admettant un ordre modulo n tel que $o_n(x) = \varphi(n)$. Dans toute cette partie, on prendra $n = p$ un nombre premier.

(1) Supposons que g est une racine primitive modulo p.

(a) Montrer que pour tout x premier avec p, il existe $0 \leq r < p-1$ tel que $g^r \equiv x \pmod{p}$.

Comme g est une racine primitive, les résidus de $g, g^2, \cdots, g^{p-1}$ sont deux à deux distincts. Il y en a exactement $p-1$, c'est à dire autant que de résidus inversibles modulo p, ils sont donc tous présents dans la liste.

(b) Soit $k > 1$. Montrer que si x admet un ordre, alors

$$o_p(x^k) = \frac{o_p(x)}{o_p(x) \wedge k}$$

Supposons que ℓ est tel que $\left(x^k\right)^\ell \equiv 1 \pmod p$. Alors, $x^{k\ell} \equiv 1 \pmod p$ et $o_p(x) \mid k\ell$. On note $d = o_p(x) \wedge k$ et $d' = \frac{k}{d}$. Ainsi, il existe $q \in \mathbb{Z}$ tel que

$$k\ell = o_p(x)q$$

ou de manière équivalente

$$\ell d' = \frac{o_p(x)}{d} q$$

donc $\frac{o_p(x)}{d} \mid \ell d'$. Par construction, $\frac{o_p(x)}{d}$ et d' sont premiers entre eux, donc par le lemme de Gauss, $\frac{o_p(x)}{d}$ divise ℓ. Réciproquement, si $\frac{o_p(x)}{d}$ divise ℓ, alors $x^{k\ell} = x^{\frac{k}{d} \times o_p(x) \times q} \equiv \left(x^{o_p(x)}\right)^{\frac{k}{d} \times q} \equiv 1 \pmod p$. Ainsi, $\left(x^k\right)^\ell \equiv 1 \pmod p$ si et seulement si $\frac{o_p(x)}{d}$ divise ℓ, ce qui montre le résultat.

(c) En déduire que $1 \leq x \leq p-1$ est générateur si et seulement si $r \wedge (p-1) = 1$ où r est tel que $g^r \equiv x \pmod p$.

Vu ce qui précède: $o_p(g^r) = o_p(g) = p-1 \iff r \wedge o_p(g) = r \wedge (p-1) = 1$.

(d) Conclure qu'il y a exactement $\varphi(p-1)$ racines primitives modulo p.

Il y a autant de générateurs que de valeurs de r entre 1 et $p-1$ telles que $r \wedge (p-1) = 1$. Ce nombre est précisément $\varphi(p-1)$.

Dans la question précédente, on a montré que s'il existe une racine primitive, alors il y en a exactement $\varphi(p-1)$. Il nous reste à montrer qu'il en existe bien une. Pour cela, on va montrer le résultat préliminaire suivant, appelé *Théorème de Lagrange*: Si $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ est un polynôme de degré $n \geq 1$ à coefficients entiers et tel que a_n n'est pas multiple de p, alors $f(X)$ admet *au plus* n racines non congrues[4] modulo p.

(2) On va montrer le théorème par récurrence sur n.

(a) Montrer que le théorème est vrai pour $n = 1$.

Si $f(X) = a_1 X + a_0$ avec a_1 non multiple de p, alors $f(x) \equiv 0 \pmod p \iff x \equiv -a_0 a_1^{-1} \pmod p$. La solution est bien unique.

(b) Supposons que le théorème est vrai au rang $n-1$, et soit $f(X)$ un polynôme comme dans l'énoncé du théorème, de degré n. Supposons que $f(X)$ admet $n+1$ racines non congrues modulo p que l'on note $c_0, \cdots, c_n$.

(i) Montrer

$$\begin{aligned} f(X) - f(c_0) = a_n(X - c_0)(X^{n-1} + X^{n-2}c_0 + \cdots + Xc_0^{n-2} + c_0^{n-1}) \\ + \quad a_{n-1}(X - c_0)(X^{n-2} + \cdots + Xc_0^{n-3} + c_0^{n-2}) \\ + \quad \vdots \\ + \quad a_1(X - c_0) \end{aligned}$$

puis en déduire qu'il existe un polynôme $g(X)$ de degré $n-1$ de coefficient dominant a_n tel que $f(X) - f(c_0) = (X - c_0)g(X)$.

Indication: utiliser l'identité $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.

[4] Autrement dit, il existe au plus n entiers $0 \leq k < p$ tels que $f(k) \equiv 0 \pmod p$.

$$f(X) - f(c_0) = a_n(X^n - c_0^n) + a_{n-1}(X^{n-1} - c_0^{n-1}) + \cdots + a_0$$

et appliquer l'identité à chaque parenthèse du membre de droite donne la forme mentionnée dans l'énoncé. Chacun des termes de la somme est multiple de $(X - c_0)$, par lequel on peut donc factoriser. Dans le second terme du produit, on y met la somme d'un polynôme de degré $n-1$ de coefficient dominant a_n, et de plusieurs polynômes de degrés $< n-1$, qui n'ont donc aucune influence sur le terme dominant. On trouve bien $g(X)$ comme voulu.

(ii) Montrer que $c_1, \cdots, c_n$ sont des racines de $g(X)$ modulo p.

Soit $1 \leq i \leq n$.

$$f(c_i) - f(c_0) \equiv \underbrace{(c_i - c_0)}_{\neq 0} g(c_i) \equiv 0 \pmod{p}$$

donc (lemme de Gauss), $g(c_i) \equiv 0 \pmod{p}$.

(iii) Conclure en montrant que l'hypothèse selon laquelle $f(X)$ admet $n+1$ racines non congrues modulo p est absurde.

La question précédente (ii) est en directe contradiction avec l'hypothèse de récurrence, selon laquelle $g(X)$ ne peut admetre qu'au plus $n-1$ racines non congrues modulo p. Ainsi, l'hypothèse de départ est absurde également, et $f(X)$ admet n ou moins racines non congrues modulo p.

(c) Conclure

Le théorème est vrai au rang 1, et vérifie la propriété d'hérédité. Il est donc vrai par le principe de récurrence.

On peut désormais montrer l'existence de racines primitives modulo p. On appelle *l'exposant* modulo p l'entier λ correspondant au maximum des valeurs de $o_p(k)$ pour $1 \leq k < p$.

(3) (a) On appelle *plus petit commun multiple*[5] *(PPCM)* de m et n des entiers non nuls la quantité

$$m \vee n = \frac{mn}{m \wedge n}.$$

Montrer que si a et b sont des entiers naturels tels que $o_p(a) = m$ et $o_p(b) = n$, alors

$$o_p(a \times b^{m \wedge n}) = m \vee n$$

Indication: On pourra exploiter la relation (1.b)

D'après la relation (1.b), on a

$$o_p(b^{m \wedge n}) = \frac{n}{(m \wedge n) \wedge n} = \frac{n}{m \wedge n} = \frac{m \vee n}{m}$$

Par ailleurs, $o_p(b^{m \wedge n}) \wedge o_p(a) = 1$ donc* $o_p(ab^{m \wedge n}) = o_p(a) o_p(b^{m \wedge n}) = m \times \frac{m \vee n}{m} = m \vee n$.

*Si x, y sont d'ordres respectifs m, n modulo p, et si $m \wedge n = 1$. Supposons que $x^r \equiv y^s \pmod{p}$ pour r, s des entiers. Alors,

$$(x^r)^m \equiv (x^m)^r \equiv 1 \pmod{p}$$

donc $o_p(x^r) \mid m$, et

[5] On l'admettra: comme son nom l'indique, il désigne bien le plus petit entier multiple à la fois de n et de m.

$$(x^r)^n \equiv (y^s)^n \equiv 1 \pmod p$$

donc $o_p(x^r) \mid n$, donc $o_p(x^r) \mid m \wedge n = 1$ et $x^r = 1$.

Puis,

$$(xy)^\ell \equiv 1 \pmod p \Longrightarrow x^\ell \equiv y^{-\ell} \pmod p$$

donc $x^\ell \equiv 1 \pmod p$ ce qui donne $m \mid \ell$ et de même, $y^{-\ell} \equiv 1 \pmod p$ donc $y^\ell \equiv \left(y^{-\ell}\right)^{-1} \equiv 1 \pmod p$ ce qui donne $n \mid \ell$. Le plus petit multiple commun de m et n est mn puisque $m \wedge n = 1$.

(b) Montrer que λ vaut $o_p(1) \vee o_p(2) \vee \cdots \vee o_p(p-1)$ (on admet que l'ordre n'a pas d'importance dans le calcul du PPCM). En déduire qu'il existe g un entier naturel tel que $o_p(g) = \lambda$, et donc que $\lambda \leq \varphi(p)$.

On a vu que le PPCM de plusieurs ordres est lui même l'ordre d'un élément. Ainsi, le PPCM de tous les ordres est lui même un ordre, il est supérieur ou égal à chacun des autres ordres (puisque c'en est un multiple), et ainsi c'est l'ordre maximal. Il existe donc un élément g d'ordre λ. Puis, on sait que $o_p(g) \mid \varphi(p)$ donc $\lambda \leq \varphi(p)$.

(c) Montrer que le polynôme $f(X) = X^\lambda - 1$ admet $p-1$ racines non congrues modulo p. En déduire $\lambda \geq p-1$.

Le polynôme $f(X)$ admet pour racines modulo p toutes les valeurs de $1 \leq k \leq p-1$, car pour chaque tel k, on a $k^\lambda \equiv 1 \pmod p$ (puisque λ est multiple de $o_p(k)$). Il s'agit bien de $p-1$ racines non congrues modulo p. Par le théorème de Lagrange, on a donc bien $\lambda \geq p-1$.

(d) Conclure que g est d'ordre $\varphi(p)$.

On a trouvé $\lambda \leq \varphi(p)$ et $\lambda \geq p-1 = \varphi(p)$, donc $\lambda = \varphi(p)$. Ainsi, g (qui a pour ordre λ), est bien d'ordre $\varphi(p)$. C'est une racine primitive modulo p.

(4) Conclure sur le nombre de racines primitives modulo p.

On a montré que s'il existe une racine primitive, alors il y en a exactement $\varphi(p-1)$. On a montré qu'une racine primitive existe, il y en a donc exactement $\varphi(p-1)$.

Partie XIV — Racines primitives modulo une puissance d'un nombre premier

On a montré l'existence de racines primitives modulo un nombre premier p. On va montrer que pour $k > 1$, il existe une racine primitive modulo p^k.

(1) (Prérequis sur les polynômes[6]) Montrer que pour tout $N > 1$, il existe un polynôme $Q(X)$ à coefficients entiers tel que

$$(1+X)^N = 1 + NX + X^2 Q(X)$$

Par récurrence sur N. Pour $N = 1$, c'est évident avec $Q(X) = 0$. Puis,

$$\begin{aligned}(1+X)^{N+1} &= (1 + NX + X^2 Q_N(X))(1+X) \\ &= 1 + NX + X^2 Q_N(X) + X + NX^2 + X^3 Q_N(X) \\ &= 1 + (N+1)X + X^2(N + Q_N(X) + XQ_N(X))\end{aligned}$$

donc $Q_{N+1}(X) = N + Q_N(X) + XQ_N(X)$ convient et est bien à coefficients entiers.

[6]Le lecteur ayant connaissance de la formule du binôme de Newton reconnaîtra immédiatement qu'il s'agit ici d'un énoncé plus faible de celle ci.

(2) Montrer que pour tout $n \in \mathbb{N}$,

$$(1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}.$$

Indication: procéder par récurrence sur n.

On procède par récurrence:
- Pour $n = 0$, c'est immédiat.
- On suppose que

$$(1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}.$$

On a

$$\begin{aligned}(1+p)^{p^{n+1}} &= \left((1+p)^{p^n}\right)^p \\ &= \left(1+p^{n+1}+qp^{n+2}\right)^p \\ &= \left(1+\underbrace{p^{n+1}(1+pq)}_{X}\right)^p \\ &= 1 + p^{n+2}(1+pq) + p^{2(n+1)}(1+pq)^2 Q\left(p^{n+2}(1+pq)\right) \\ &\equiv 1 + p^{n+2} \pmod{p^{n+3}}.\end{aligned}$$

puisque $p^{2(n+1)} \equiv 0 \pmod{p^{n+3}}$ pour $n \geq 1$.

(3) On rappelle que $\varphi\left(p^k\right) = (p-1)p^{k-1}$ (voir Partie XI).

(b) Montrer que $1+p$ est d'ordre p^{k-1} modulo p^k. Indication: Calculer $(1+p)^{p^{k-2}}$ et $(1+p)^{p^{k-1}}$ modulo p^k.

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \pmod{p^k}$$

$$(1+p)^{p^{k-1}} \equiv 1 + p^k \equiv 1 \pmod{p^k}$$

Donc, d'après (XII.3.a) et (XII.3.b), on a $o_{p^k}(1+p) \mid p^{k-1}$ mais $o_{p^k}(1+p) \nmid p^{k-2}$. Les seuls diviseurs de p^{k-1} sont les p^ℓ pour $\ell \leq k-1$, et le seul d'entre eux qui ne divise pas p^{k-2} est p^{k-1} donc $o_{p^k}(1+p) = p^{k-1}$.

(c) Soit g une racine primitive modulo p. Montrer que pour tout $0 < \ell < p-1$, $p^k \nmid g^\ell - 1$, et que $p \mid g^{p-1} - 1$. En déduire qu'il existe ℓ tel que g^ℓ est d'ordre $p-1$ modulo p^k.

On a $o_p(g) = p-1$ donc

$$\forall 0 < \ell < p-1, p \nmid g^\ell - 1$$

ce qui implique automatiquement $p^k \nmid g^\ell - 1$ pour $0 < \ell < p-1$. Puis, $g^{p-1} \equiv 1 \pmod{p}$ donc $p \mid g^{p-1} - 1$. Par ailleurs, $o_{p^k}(g) \mid \varphi\left(p^k\right) = (p-1)p^{k-1}$. Ainsi, il existe $d \mid p-1$ et $k' < k$ tel que $o_{p^k}(g) = dp^{k'}$. On a

$$p^k \mid g^{dp^{k'}} - 1$$

donc $g^{dp^{k'}} \equiv 1 \pmod{p}$ or $g^{dp^{k'}} \equiv \left(g^d\right)^{p^{k'}} \equiv g^d \pmod{p}$ (petit théorème de Fermat) donc $g^d \equiv 1 \pmod{p}$ d'où l'on tire $d = p-1$ et $o_{p^k}(g) = (p-1)p^{k'}$. On prend $\ell = p^{k'}$ pour trouver l'élément g^ℓ d'ordre $p-1$.

(d) Montrer que $(p-1) \wedge p^{k-1} = 1$. En déduire qu'il existe une racine primitive modulo p^k.

Si q est un nombre premier divisant p^{k-1} et $p-1$ alors $q=p$, or $p \wedge p-1 = 1$ (car $p-(p-1)=1$ donc q ne peut pas diviser $p-1$. Ainsi, aucun nombre premier ne divise $p-1$ et p^{k-1}, d'où $(p-1)\wedge p^{k-1}=1$. On a vu en (XIII.3.a) que l'on peut trouver un élément qui a pour ordre le PPCM de deux autres ordres. Ici, le PPCM de $(p-1)$ et p^{k-1} est $\varphi\big(p^k\big)$, ce qui conclut.

Partie XV — Convolutions et inversion de Möbius

On appelle *fonction arithmétique* toute fonction $f : \mathbb{N}^* \longrightarrow \mathbb{R}$. Si f et g sont des fonctions arithmétiques, on définit leur convolution de la manière suivante:

$$\forall n \in \mathbb{N}^*, \quad (f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

(1) Montrer que si f et g sont des fonctions arithmétiques, $f \star g = g \star f$.

Soit $n \in \mathbb{N}^*$. Alors $d \mid n$ si et seulement si $\frac{n}{d}$ est un entier, auquel cas $n = d\frac{n}{d}$ et $\frac{n}{d}$ divise n. Ainsi, les diviseurs d de n sont exactement les $\frac{n}{d}$ pour d divisant n. Les sommes suivantes sont donc bien égales:

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) = (g \star f)(n)$$

(2) On note δ_1 la fonction arithmétique telle que $\delta_1(1) = 1$ et $\delta_1(n) = 0$ pour tout $n > 1$. Soit f une fonction arithmétique. Montrer que $f \star \delta_1 = f$.

On sait que $f \star \delta_1 = \delta_1 \star f$. Regardons plutôt cette deuxième forme. Pour $n \in \mathbb{N}^*$, la somme porte sur $d \mid n$. Si $d > 1$, alors $\delta_1(d) = 0$, ce qui laisse comme unique terme restant dans la somme le terme pour $d = 1$ (qui est bien un diviseur de n). Il reste donc

$$(\delta_1 \star f)(n) = \delta_1(1) f\left(\frac{n}{1}\right) = f(n).$$

(3) On note $\mathbb{1}$ la fonction arithmétique constante égale à 1 et μ la fonction arithmétique appellée *fonction de Möbius* définie par

$$\forall n \in \mathbb{N}^*, \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré parfait différent de 1} \\ 1 & \text{si } n \text{ est produit d'un nombre pair de nombres premiers distincts} \\ -1 & \text{si } n \text{ est produit d'un nombre impair de nombres premiers distincts.} \end{cases}$$

(a) Si E est un ensemble fini, on note $\mathrm{card}(E)$ sa cardinalité (sa taille). Montrer que si $P = \{p_1, ..., p_r\}$ est un ensemble fini de nombres premiers deux à deux distincts, alors

$$\mu(p_1 \cdots p_r) = (-1)^{\mathrm{card}(P)}.$$

Le terme $(-1)^k$ vaut 1 lorsque k est pair, -1 sinon. On trouve donc bien exactement $\mu(p_1 \cdots p_r) = (-1)^r$ si les $p_1, \cdots, p_r$ sont deux à deux distincts. Dans ce cas, $r = \mathrm{card}(P)$.

(b) Soit $n > 1$ un entier dont la décomposition en facteurs premiers est $p_1^{k_1} \cdots p_s^{k_s}$. Montrer que les diviseurs d de n tels que $\mu(d) \neq 0$ sont exactement les produits $p'_1 \cdots p'_r$ avec $\{p'_1, \cdots, p'_r\}$ un sous ensemble de $\{p_1, \cdots, p_s\}$.

Les diviseurs de n sont les entiers de la forme $d = p_1^{k'_1} \cdots p_s^{k'_s}$ avec $0 \leq k'_i \leq k_i$ pour tout $1 \leq i \leq s$. Si $k'_i \geq 2$, alors d est divisible par p_i^2 et automatiquement $\mu(d) = 0$. Il reste $k'_i \leq 1$ pour tout i, ce qui correspond exactement aux produits décrits dans l'énoncé.

(c) Notons P l'ensemble des nombres premiers divisant $n > 2$. Montrer que

$$\sum_{d|n} \mu(d) = \sum_{D \subset P} (-1)^{\mathrm{card}(D)}$$

La réécriture découle immédiatement des deux questions précédentes.

(d) En déduire que

$$\sum_{d|n} \mu(d) = k - \ell$$

où k est le nombre de sous-ensembles de P de cardinal pair et ℓ est le nombre de sous-ensenbles de P de cardinal impair.

On peut séparer la somme de la manière suivante:

$$\sum_{D \subset P} (-1)^{\mathrm{card}(D)} = \sum_{\substack{D \subset P \\ \mathrm{card}(D) \text{ pair}}} \underbrace{(-1)^{\mathrm{card}(D)}}_{=1} + \sum_{\substack{D \subset P \\ \mathrm{card}(D) \text{ impair}}} \underbrace{(-1)^{\mathrm{card}(D)}}_{=-1} = k - \ell$$

(e) Soit $p \in P$ fixé. On forme des couples $(S, S \cup \{p\})$ de sous-ensembles de P, avec S un sous ensemble de P ne contenant pas p. Montrer que chaque sous-ensemble de P figure dans l'un des couples et uniquement dans celui ci, et que chaque couple contient un ensemble de cardinal pair et un ensemble de cardinal impair.

En déduire que $k = \ell$.

Soit $D \subset P$. Si D contient p alors le couple correspondant est $(D \setminus \{p\}, D)$, sinon le couple est $(D, D \cup \{p\})$. Puis, chaque couple (S, S') contient un ensemble de cardinal $\mathrm{card}(S)$ et un ensemble de cardinal $\mathrm{card}(S') = \mathrm{card}(S) + 1$ donc l'un est pair et l'autre impair. On en déduit immédiatement que les sous ensembles de cardinal pair peuvent être couplés aux sous-ensembles de cardinal impair, de sorte que $k = \ell$ et $k - \ell = 0$.

(f) Montrer que $\mu \star \mathbb{1} = \delta_1$.

Soit $n > 1$. On a

$$(\mu \star \mathbb{1})(n) = \sum_{d \mid n} \mu(d) = k - \ell = 0 = \delta_1(1),$$

et $(\mu \star \mathbb{1})(1) = \mu(1) = 1 = \delta_1(1)$ donc $\mu \star \mathbb{1} = \delta_1$.

(4) Soient f, g, h trois fonctions arithmétiques. Montrer que $(f \star g) \star h = f \star (g \star h)$.

Réécrivons la condition de divisibilité sous forme de condition sur des produits. Soit $n \in \mathbb{N}^*$

$$\begin{aligned}
((f \star g) \star h)(n) &= \sum_{d|n} (f \star g)(d) h\left(\frac{n}{d}\right) = \sum_{ab=n} (f \star g)(a) h(b) = \sum_{ab=n} \sum_{cd=a} f(c) g(d) h(b) \\
&= \sum_{cdb=n} f(c) g(d) h(b) \\
&= \sum_{acd=n} f(a) g(c) h(d) \\
&= \sum_{ab=n} \sum_{cd=b} f(a) g(c) h(d) = \sum_{ab=n} f(a) \sum_{cd=b} g(c) h(d) = \sum_{ab=n} f(a) (g \star h)(b) \\
&= (f \star (g \star h))(n)
\end{aligned}$$

(5) En déduire la formule d'inversion de Möbius:

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d) \iff \forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

La première condition s'écrit $g = f \star \mathbb{1}$, la seconde s'écrit $f = \mu \star g (= g \star \mu)$. On a montré que $\mu \star 1 = \delta_1$ donc si $g = f \star \mathbb{1}$, alors $g \star \mu = f \star \mathbb{1} \star \mu = f \star (\mu \star \mathbb{1}) = f \star \delta_1 = f$. Réciproquement, si $f = g \star \mu$, alors $f \star \mathbb{1} = g \star (\mu \star \mathbb{1}) = g \star \delta_1 = g$.

(6) Montrer l'identité

$$\forall n \in \mathbb{N}^*, \quad \varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

On a montré (voir Partie XI) que $\mathrm{id} = \varphi \star \mathbb{1}$ où $\mathrm{id} : n \mapsto n$. La formule découle immédiatement de l'inversion de Möbius

Partie XVI — Résidus quadratiques et symbole de Legendre

On appelle résidu quadratique modulo $n > 1$ les entiers $0 \leq k < n$ tels qu'il existe $x \in \mathbb{N}$ satisfaisant $x^2 \equiv k \pmod{n}$. On dit que x est une racine carrée de k modulo p.

Dans toute la suite, p et q sont des nombre premier **impairs**.

(1) Montrer que pour tout a, b entiers,

$$ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p} \quad \text{ou} \quad b \equiv 0 \pmod{p}.$$

$ab \equiv 0 \pmod{p} \iff p \mid ab \iff p \mid a \quad \text{ou} \quad p \mid b$ car p est premier.

(2) En déduire que pour $k \in \mathbb{N}$, $x^2 \equiv k \pmod{p}$ admet au plus deux solutions dans l'ensemble $\{0, \cdots, p-1\}$.

Si l'équation n'admet pas de solution, il n'y a rien à faire. Supposons qu'il existe une solution que l'on note a. Alors, $a^2 \equiv k \pmod{p}$ de sorte que l'équation est équivalente à

$$(x-a)(x+a) \equiv 0 \pmod{p}.$$

Par la question précédente, les solutions x satisfont $x \equiv a \pmod{p}$ ou $x \equiv -a \pmod{p}$ de sorte que dans l'ensemble $\{0, \cdots, p-1\}$, les seules solutions sont a et $p - a$.

(3) Soit g une racine primitive modulo p.

(a) Montrer que le résidu modulo p de g^{2m} est un résidu quadratique modulo p pour tout $m \geq 0$. Combien il y a-t-il de résidus de cette forme ?

$g^{2m} \equiv (g^m)^2 \pmod{p}$ donc le résidu de g^m est une racine carrée du résidu de g^{2m} modulo p.

Comme g est une racine primitive, l'ensemble des résidus non nuls modulo p est exactement l'ensemble des résidus de $1, g, g^2, \cdots, g^{p-2}$. Ici, comme p est impair, on a pris en compte $1, g^2, g^4, \cdots, g^{p-3}$ ce qui donne $\frac{p-1}{2}$ résidus.

(b) Montrer que le résidu modulo p de g^{2m+1} n'est pas un résidu quadratique modulo p, pour tout $m \geq 0$. Combien y a-t-il de résidus de cette forme ?

Supposons que $g^{2m+1} \equiv x^2 \pmod{p}$. Alors, il existe ℓ tel que $x \equiv g^\ell$ (car x n'est pas nul modulo p). On trouve:

$$g^{2m+1} \equiv g^{2\ell} \pmod{p}$$

soit encore $g^{2m+1-2\ell} \equiv 1 \pmod{p}$ donc $o_p(g) = p - 1 \mid 2m + 1 - 2\ell$ ce qui est impossible car $p - 1$ est pair et $2m + 1 - 2\ell$ est impair. Donc, le résidu de g^{2m+1} n'est pas un résidu quadratique.

Comme à la question précédente, on a listé les $\frac{p-1}{2}$ résidus non nuls restants.

(c) En déduire qu'il y a exactement $\frac{p-1}{2}$ résidus quadratiques.

On a vu que k est un résidu quadratique si et seulement si il peut s'écrire $k \equiv g^{2m} \pmod p$, et on a vu que cela constitue exactement $\frac{p-1}{2}$ résidus.

(d) Montrer que pour un résidu non nul k, on a

$$k^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p \text{ si } k \text{ est un résidu quadratique modulo } p \\ -1 \pmod p \text{ si } k \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Indication: Montrer que $g^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Si k est un résidu quadratique, on note x une racine carrée de k modulo p et

$$k^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

par le petit théorème de Fermat.

Si k n'est pas un résidu quadratique, alors il s'écrit $k \equiv g^{2m+1} \pmod p$ et

$$k^{\frac{p-1}{2}} \equiv g^{(2m+1)\frac{p-1}{2}} \equiv g^{m(p-1)+\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod p$$

Puis, $g^{\frac{p-1}{2}}$ est solution de $x^{p-1} \equiv 1 \pmod p$ (petit théorème de Fermat), et cette équation s'écrit

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

donc $g^{\frac{p-1}{2}}$ vaut soit 1 soit -1 modulo p. Comme g est une racine primitive, $o_p(g) = p-1$ donc $g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ ce qui montre le résultat.

Lorsque p est un nombre premier impair, et k un entier non multiple de p, on appelle *symbole de Legendre* l'entier défini par

$$\left(\frac{k}{p}\right) = \begin{cases} 1 \text{ si le résidu de } k \text{ est un résidu quadratique modulo } p \\ -1 \text{ si le résidu de } k \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

(4) Montrer les relations suivantes:

(a) Pour a, b non nuls modulo p,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

Et le résultat découle car les seules valeurs possibles du symbole de Legendre sont ± 1.

(b)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \pmod 4 \\ -1 \text{ si } p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod p$$

donc le symbole vaut 1 si et seulement si $\frac{p-1}{2}$ est pair, c'est à dire si $4 \mid p-1$ ce qui équivaut à $p \equiv 1 \pmod 4$. Si $p \not\equiv 1 \pmod 4$ alors comme p est impair, $p \equiv 3 \pmod 4$.

(5) On va montrer le *lemme de Gauss* pour les symboles de Legendre: Si a est un entier non multiple de p et si s est le nombre de résidus modulo p des entiers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ qui sont strictement supérieurs à $\frac{p}{2}$, alors

$$\left(\frac{a}{p}\right) = (-1)^s.$$

On note $u_1, \cdots, u_s$ les résidus des entiers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ qui sont supérieurs (strictement) à $\frac{p}{2}$. On note $v_1, \cdots, v_t$ les résidus restants.

(a) Montrer que les u_i, v_i sont inversibles modulo p, puis que les u_i sont deux à deux distincts, de même que les v_i sont deux à deux distincts.

Les u_i, v_i sont inversibles car résidus d'entiers de la forme ja avec j inversible et a inversible. Puis, clairement $u_i = u_j$ est impossible de même que $v_i = v_j$ car sinon on a une relation du type $na \equiv ma \pmod p$ avec $n \not\equiv m \pmod p$ et a inversible.

(b) Montrer qu'il n'existe pas de couple (i, j) tel que $p - u_i \equiv v_j \pmod p$. En déduire que les entiers $p - u_1, \cdots, p - u_s, v_1, \cdots, v_s$ sont exactement les entiers $1, 2, \cdots, \frac{p-1}{2}$ (éventuellement dans le désordre).

$p - u_i \equiv v_j \pmod p$ donne une relation du type $-na \equiv ma \pmod p$ avec $n \not\equiv m \pmod p$ et a inversible, ce qui est impossible car n et m sont dans l'ensemble $1, 2, \cdots, \frac{p-1}{2}$.

On a donc $\frac{p-1}{2}$ résidus tous inférieurs ou égaux à $\frac{p-1}{2}$ et deux à deux distincts. On a donc exactement $1, 2, \cdots, \frac{p-1}{2}$.

(c) Montrer que

$$(-1)^s u_1 u_2 \cdots u_s v_1 v_2 \cdots, v_t \equiv \left(\frac{p-1}{2}\right)! \pmod p.$$

$$(p - u_1) \cdots (p - u_s) v_1 \cdots v_t = \left(\frac{p-1}{2}\right)!$$

vu ce qui précède et $p - u_i \equiv -u_i \pmod p$ donc on trouve l'égalité demandée en passant au modulo p.

(d) Montrer que

$$u_1 \cdots u_s v_1 \cdots v_t \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

On a choisi les u_i, v_i précisément pour énumérer les $a, 2a, \cdots, \frac{p-1}{2}a$ modulo p. On en tire donc immédiatement

$$u_1 \cdots u_s v_1 \cdots v_t \equiv a \cdot 2a \cdots \frac{p-1}{2}a \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

(e) Conclure.

Vu ce qui précède:

$$(-1)^s a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod p$$

donc

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

et

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod p$$

ce qui conclut car

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

(6) Nous allons montrer que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-8}{2}}.$$

(a) Montrer que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}-\lfloor\frac{p}{4}\rfloor}.$$

Indication: Utiliser le lemme de Gauss.

Par le lemme de Gauss, il suffit de montrer qu'il y a $\frac{p-1}{2} - \lfloor\frac{p}{4}\rfloor$ résidus supérieurs à $\frac{p}{2}$ parmi ceux des entiers $2, 4, \cdots, (p-1)$. Comme ces entiers sont leurs propres résidus, il suffit de compter ceux qui sont supérieurs à $\frac{p}{2}$.

Il y a $\frac{p-1}{2}$ entiers dans la liste $2, 4, \cdots, (p-1)$, auxquels il faut enlever ceux qui sont $< \frac{p}{2}$. Ils s'écrivent $2 \leq 2k < \frac{p}{2}$ soit encore $1 \leq k < \frac{p}{4}$ et comme $\frac{p}{4}$ n'est pas entier (p est impair), $k < \frac{p}{4}$ est équivalent à $k \leq \lfloor\frac{p}{4}\rfloor$. Il y a donc exactement $\lfloor\frac{p}{4}\rfloor$ entiers k qui conviennent entre 1 et $\lfloor\frac{p}{4}\rfloor$, ce qui donne

$$\frac{p-1}{2} - \left\lfloor\frac{p}{4}\right\rfloor$$

résidus supérieurs à $\frac{p}{2}$.

(b) Montrer que nour tout entier n,

$$\frac{n-1}{2} - \left\lfloor\frac{n}{4}\right\rfloor = \frac{n^2-1}{8} \pmod 2 \iff \frac{(n+8)-1}{2} - \left\lfloor\frac{n+8}{4}\right\rfloor \equiv \frac{(n+8)^2-1}{8} \pmod 2.$$

$$\begin{aligned}\frac{(n+8)-1}{2} - \left\lfloor\frac{n+8}{4}\right\rfloor &= \frac{n-1}{2} + 4 - \left\lfloor\frac{n}{4}+2\right\rfloor = \frac{n-1}{2} + \left\lfloor\frac{n}{4}\right\rfloor + 2 \\ &\equiv \frac{n-1}{2} + \left\lfloor\frac{n}{4}\right\rfloor \pmod 2\end{aligned}$$

et

$$\frac{(n+8)^2-1}{8} = \frac{n^2+16n+8^2-1}{8} = \frac{n^2-1}{8} + 2n + 8 \equiv \frac{n^2-1}{8} \pmod 2$$

Donc les deux équations modulo 2 sont bien équivalentes.

(c) En déduire que pour tout entier impair n,

$$\frac{n-1}{2} - \left\lfloor\frac{n}{4}\right\rfloor = \frac{n^2-1}{8} \pmod 2.$$

Si l'équation est vraie pour un entier impair n, elle est vraie pour $n+8$. Il sera donc suffisant de vérifier pour $n = -3, -1, 1, 3$. Pour $n = -3$ on a

$$\frac{n-1}{2} - \left\lfloor \frac{n}{4} \right\rfloor = -\frac{4}{2} - (-1) = -1$$

et

$$\frac{n^2-1}{8} = \frac{8}{8} = 1$$

et $1 \equiv -1 \pmod 2$. Même principe pour les trois autres valeurs.

(d) Conclure.

On sait

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}$$

et la valeurs de $(-1)^t$ ne dépend que de la valeur de t modulo 2. Ainsi, il est suffisant de montrer que

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{n^2-1}{8} \pmod 2,$$

ce qu'on vient de faire à la question précédente.

Partie XVII — Loi de réciprocité quadratique

Dans toute cette partie, p et q désignent des premiers impairs distincts. L'objectif est de montrer le résultat suivant, connu sous le nom de *loi de réciprocité quadratique*:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

(1) (*Lemme préliminaire*) Dans cette question, a est un entier **impair** non divisible par p. On va montrer

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)},$$

avec

$$T(a,b) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor.$$

On reprend les notations utilisées pour le lemme de Gauss (question (XVI.5)): on note $u_1, \cdots, u_s$ (resp. $v_1, \cdots, v_t$) les résidus modulo p des entiers $a, 2a, \cdots, \frac{p-1}{2}a$ supérieurs à $\frac{p}{2}$ (resp. inférieurs à $\frac{p}{2}$).

(a) Montrer que

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

Indication: Faire la division euclidienne de ja par $\left\lfloor \frac{ja}{p} \right\rfloor$, pour chaque j.

On applique l'indication: chaque division euclidienne donne une équation de la forme

$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + r_j$$

avec $ja \equiv r_j \pmod p$ et $0 \leq r_j < p$ donc r_j est un résidu congru à un ja, donc de la forme u_i ou v_i, et chaque u_i ou v_i apparaît comme r_j exactement une fois. On fait la somme pour $1 \leq j < \frac{p-1}{2}$ pour obtenir exactement l'égalité demandée.

(b) Montrer

$$\sum_{j=1}^{\frac{p-1}{2}} j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j$$

On sait que l'ensemble des $1 \leq j < \frac{p-1}{2}$ est exactement l'ensemble des $p - u_1, \cdots, p - u_s, v_1, \cdots, v_t$ de sorte que

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} (p - u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{\frac{p-1}{2}} u_j + \sum_{j=1}^{\frac{p-1}{2}} v_j$$

(c) En déduire que

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} j = pT(a,p) - ps + 2\sum_{k=1}^{s} u_j$$

On soustrait les égalités que l'on vient de trouver:

$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - ps + \sum_{j=1}^{\frac{p-1}{2}} u_j + \sum_{j=1}^{\frac{p-1}{2}} u_j + \sum_{j=1}^{\frac{p-1}{2}} v_j + \sum_{j=1}^{\frac{p-1}{2}} v_j$$

ce qui après simplification donne

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\underbrace{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor}_{=T(a,p)} - ps + 2\sum_{j=1}^{\frac{p-1}{2}} u_j$$

(d) Conclure en montrant que $T(a,p) \equiv s \pmod 2$.

On reprend l'égalité précédente modulo 2. On sait que $p \equiv 1 \pmod 2$ (p est impair) et $a \equiv 1 \pmod p$. Il reste:

$$0 \equiv 1 \cdot T(a,p) - 1 \cdot s + 0 \pmod 2$$

donc $T(a,b) \equiv s \pmod 2$.

(2) (*Preuve de la loi de réciprocité quadratique*) Soient p, q deux premiers impairs distincts

(a) Montrer qu'il y a $\frac{p-1}{2} \cdot \frac{q-1}{2}$ paires d'entiers (x,y) telles que $1 \leq x \leq \frac{p-1}{2}$ et $1 \leq y \leq \frac{q-1}{2}$.

Pour le premier entier, il y a $\frac{p-1}{2}$ choix, pour le second il y en a $\frac{q-1}{2}$. Il y a donc au total $\frac{p-1}{2} \cdot \frac{q-1}{2}$ choix.

(b) Montrer que pour de telles paires, on a jamais $qx = py$.

Si $qx = py$ alors $q \mid py$ donc $q \mid p$ ou $q \mid y$. On sait que q ne divise pas p car ce sont des premiers distincts, et $q \mid y$ est absurde car $1 \leq y < q$.

(c) Montrer qu'il y a $T(q,p)$ paires telles que $qx > py$.

Soit $1 \leq x \leq \frac{p-1}{2}$. On va compter le nombre de valeurs de $1 \leq y \leq \frac{p-1}{2}$ telles que $qx > py$. Cette dernière condition impose $y < \frac{qx}{p}$ soit encore $y \leq \left\lfloor \frac{qx}{p} \right\rfloor$ car $\frac{qx}{p}$ n'est pas un entier (q est premier avec p et x est premier avec p donc qx est premier avec p qui n'en est donc pas un diviseur). Il y a donc $\left\lfloor \frac{qx}{p} \right\rfloor$ valeurs possibles de y à x fixé.

On prends pour x toutes les valeurs $j = 1, \cdots, \frac{p-1}{2}$ et on obtient:

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor = T(q,p)$$

(d) En déduire que

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

L'ensemble des paires (x,y) avec $1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}$ est au nombre de $\frac{p-1}{2} \cdot \frac{q-1}{2}$. On a vu que pour de telles paires on n'a jamais $py = qx$ donc on a toujours $qx > py$ ou $qx < py$. Il y a $T(q,p)$ paires telles que $qx > py$, et avec le même raisonnement, il y a $T(p,q)$ paires telles que $qx < py$.

(e) Conclure.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(p,q)}(-1)^{T(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

(3) Montrer que $103x + 78 = y^2$ n'a pas de solutions entières (x,y). On admettra que 103 est un nombre premier.

Si (x,y) est solution alors $y^2 \equiv 78 \pmod{103}$, et réciproquement. Il faut donc montrer que $\left(\frac{78}{103}\right) = -1$. La décomposition en facteurs premiers de 78 est $2 \times 3 \times 13$ donc

$$\left(\frac{78}{103}\right) = \left(\frac{2}{103}\right) \times \left(\frac{3}{103}\right) \times \left(\frac{13}{103}\right).$$

On sait que

$$\left(\frac{2}{103}\right) = (-1)^{\frac{103^2-1}{8}} = 1$$

et

$$\left(\frac{3}{103}\right) \times \left(\frac{13}{103}\right) = -\left(\frac{103}{3}\right)\left(\frac{103}{13}\right) = -\left(\frac{1}{3}\right)\left(-\frac{1}{13}\right) = -1(-1)^{\frac{13-1}{2}} = -1$$

donc $\left(\frac{78}{103}\right) = -1$, ce qui conclut.

Partie XVIII — Lifting the exponent

On appelle *Lifting the exponent lemma* ou *lemme LTE* le résultat suivant: si p est un premier impair divisant $a - b$ mais ne divisant ni a ni b, alors

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

On rappelle l'identité suivante: pour tous a, b et tout $n > 0$,

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

(1) Donner une justification rapide de l'identité rappelée.

On développe le membre de droite: on a

$$a^n + a^{n-1}b + \cdots + a \cdot b^{n-1} - ba^{n-1} - b^2a^{n-2} - \cdots - b^n$$

et chacuns des binomes $a^x b^y$ avec $x, y > 0$ apparaît deux fois avec deux signes différents, donc tous les termes s'annulent sauf a^n et $-b^n$.

(2) Dans cette question, $p \nmid n$, et satisfait les conditions du lemme LTE. Montrer que

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv na^{n-1} \pmod{p}.$$

En déduire que p ne divise pas $a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$, et conclure que le lemme LTE est vrai lorsque p ne divise pas n.

On a $p \mid x - y$ donc $x \equiv y \pmod{p}$ ce qui donne

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv a^{n-1} + a^{n-2} \cdot a + \cdots + a^{n-1} \equiv na^{n-1} \pmod{p}$$

or n est inversible modulo p et a aussi, donc $na^{n-1} \not\equiv 0 \pmod{p}$. Ainsi,

$$v_p(a^n - b^n) = v_p(a-b) + v_p(a^{n-1} + \cdots + b^{n-1}) = v_p(a-b) = v_p(a-b) + v_p(n).$$

ce qui conclut.

(3) Soit p un premier impair divisant $a - b$ mais ne divisant ni a ni b.

(a) Montrer que p divise $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$.

Le terme vaut $pa^{p-2} \equiv 0 \pmod{p}$ (voir question précédente).

(b) Notons $k = \frac{b-a}{p}$ (c'est un entier). Montrer que pour $1 \leq t < p$, on a

$$b^t a^{p-1-t} \equiv a^{p-1} + tkpa^{p-2} \pmod{p^2}.$$

Indication: Utiliser la question (XIV.1) avec $X = \frac{kp}{a}$

La question (XIV.1) donne

$$(1+X)^N = 1 + NX + X^2Q(X)$$

avec $Q(X)$ un polynôme à coefficients entiers. On prend $X = \frac{y}{x}$ pour obtenir

$$x^N\left(1 + \frac{y}{x}\right)^N = (x+y)^N = x^N + Nx^{N-1}y + x^{N-2}y^2Q\left(\frac{y}{x}\right)$$

et Q est de degré au plus $N-2$ car $(1+X)^N$ est de degré N. On en déduit que

$$R(y) = x^{N-1}Q\left(\frac{y}{x}\right)$$

est une expression polynomiale en y à coefficients entiers lorsque x est entier.

On prend $N = t$, $y = kp$ et $x = a$ pour trouver

$$b^t a^{p-1-t} = (a+kp)^t a^{p-1-t} = a^{p-1} + a^{p-1-t}ta^{t-1}kp + a^{p-1-t}k^2p^2\underbrace{a^{t-2}Q\left(\frac{kp}{a}\right)}_{\in\mathbb{Z}}$$

$$\equiv a^{p-1} + tkpa^{p-2} \pmod{p^2}$$

(c) En déduire que

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \not\equiv 0 \pmod{p^2}$$

puis que le lemme LTE est vrai pour $n = p$.

Indication: On pourra utiliser librement que $1 + 2 + \cdots + (p-1) = \frac{p(p-1)}{2}$.

On utilise le résultat précédent:

$$\begin{aligned} & a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-2} \\ \equiv\ & a^{p-1} + (a^{p-1} + kpa^{p-2}) + (a^{p-1} + 2kpa^{p-2}) + \cdots + (a^{p-1} + (p-1)kpa^{p-2}) \\ \equiv\ & pa^{p-1} + (1 + 2 + \cdots + (p-1))kpa^{p-2} \\ \equiv\ & pa^{p-1} + \frac{p-1}{2}kp^2a^{p-2} \equiv pa^{p-1} \not\equiv 0 \pmod{p^2}. \end{aligned}$$

On a donc montré que $v_p(a^{p-1} + a^{p-2}b + \cdots + b^{p-2}) = 1$ ce qui montre bien le lemme pour $n = p$ car dans ce cas $v_p(n) = 1$.

(d) Notons $\alpha = v_p(n)$. Montrer que

$$v_p(a^n - b^n) = v_p(a^{p^\alpha} - b^{p^\alpha}).$$

En déduire que le lemme LTE est vrai pour tout n.

L'égalité demandée provient de la question (2): $n = p^\alpha m$ avec $p \nmid m$ donc

$$v_p(a^n - b^n) = v_p\big((a^{p^\alpha})^m - (b^{p^\alpha})^m\big) = v_p(a^{p^\alpha} - b^{p^\alpha})$$

car si p divise $a - b$ alors p divise $a^{p^\alpha} - b^{p^\alpha}$ (par l'identité rappelée), et bien sûr $p \nmid a^{p^\alpha}, b^{p^\alpha}$.

Il est donc suffisant de montrer le lemme pour $n = p^\alpha$ (car $v_p(n) = \alpha = v_p(p^\alpha)$). Vu ce qui précède,

$$v_p(a^{p^\alpha} - b^{p^\alpha}) = v_p\Big(\big(a^{p^{\alpha-1}}\big)^p - \big(b^{p^{\alpha-1}}\big)^p\Big) = v_p\big(a^{p^{\alpha-1}} - b^{p^{\alpha-1}}\big) + 1$$

En continuant le raisonnement, on trouve

$$v_p(a^{p^\alpha} - b^{p^\alpha}) = v_p\big(a^{p^{\alpha-1}} - b^{p^{\alpha-1}}\big) + 1 = \cdots = v_p(a - b) + \alpha.$$