MATHEMATICAL.
OLYMPIAD.CH
MATHEMATIK-OLYMPIADE
OLYMPIADES DE MATHÉMATIQUES
OLIMPIADI DELLA MATEMATICA

Théorie des nombres II

Thomas Huber, Louis Hainaut

Actualisé: 4 janvier 2021
vers. 2.0.0

Table des matières

1 Congruences I

1.1 Définitions

Soient $a, b \in \mathbb{Z}$ et m un nombre naturel. Si m divise $a - b$, alors on dit que a et b sont *congruents modulo* m, et on écrit

$$a \equiv b \pmod{m}.$$

Souvent on note tout simplement $a \equiv b\ (m)$. Si a et b ne sont pas congruents, alors on écrit $a \not\equiv b \pmod{m}$. À l'aide de la division avec reste,

$$a = km + r,$$
$$b = lm + s,$$

il en découle donc immédiatement que a et b sont congruents modulo m si et seulement si $r = s$. En particulier on a $a \equiv 0\ (m)$ si et seulement si $m \mid a$. Lors du calcul de congruences, il n'y a que le reste d'un nombre après division par m qui compte. Ensuite on forme l'ensemble de tous les nombres qui ont le même reste après division par m cet ensemble est appelé *classe d'équivalence* modulo m. Il existe donc exactement m classes d'équivalence modulo m, qu'on peut *représenter* par les nombres $0, 1, \ldots, m-1$. Par exemple les nombres $17, -8$ et 2 sont tous les trois dans la même classe d'équivalence modulo 5, mais dans trois classes d'équivalence différentes modulo 7.
Tout comme les nombres usuels, on peut additionner et multiplier les congruences.

Proposition 11. *Soient a, b, c, d des entiers avec $a \equiv c$ et $b \equiv d\ (m)$. Alors on a*

$$a \pm b \equiv c \pm d \pmod{m},$$
$$ab \equiv cd \pmod{m}.$$

Preuve. Selon les hypothèses il existe des entiers k, l avec $a - c = km, b - d = lm$. Ainsi

$$(a + b) - (c + d) = (a - c) + (b - d) = km + lm = (k + l)m,$$

d'après la définition cela veut dire que $a + b \equiv c + d\ (m)$. De la même façon, on montre que $a - b \equiv c - d\ (m)$. De plus, on a

$$ab - cd = a(b - d) + d(a - c) = a(lm) + d(km) = (al + dk)m,$$

d'où $ab \equiv cd\ (m)$. □

Une conséquence directe est la règle de calcul suivante:

$$a \equiv b \pmod{m} \quad \Longrightarrow \quad a^k \equiv b^k \pmod{m}, \qquad k \geq 0.$$

Toutefois on insiste sur le fait qu'une règle similaire pour les exposants n'est **pas** valable:

$$k \equiv l \pmod{m} \quad \not\Longrightarrow \quad a^k \equiv a^l \pmod{m}$$

Par exemple on a $1 \equiv 4 \pmod{3}$, mais $2^1 \not\equiv 2^4 \pmod{3}$! Ce phénomène va être le sujet du prochain paragraphe.
Une autre difficulté est que la division, comme pour les nombres entiers, n'est pas toujours applicable. On va revenir sur ce point plus tard. Nous donnons ici juste une règle importante de simplification qui suffit dans la majorité des cas.

Proposition 12. *Si c et m n'ont pas de diviseur commun, alors on peut simplifier les congruences en divisant par c :*

$$ca \equiv cb \pmod{m} \quad \Longrightarrow \quad a \equiv b \pmod{m}.$$

Preuve. On a supposé que m divise $ca - cb = c(a - b)$. Puisque m et c n'ont pas de diviseur commun, on a même $m \mid a - b$, donc $a \equiv b$. □

Exemple 1. *Parmi 5 entiers, on en trouve toujours 3 dont la somme est divisible par* 3.

Solution. Tout nombre est congruent à $0, 1$ ou 2 modulo 3. Si il existe trois nombres a, b, c avec $a \equiv 0$, $b \equiv 1$ et $c \equiv 2 \pmod{3}$. Alors $a + b + c \equiv 0 + 1 + 2 \equiv 0 \pmod{3}$, leur somme est donc divisible par 3. Si de tels nombres n'existent pas, alors il y a, d'après le principe des tiroirs, trois nombres congruents modulo 3, donc leur somme est divisible par 3. □

Exemple 2. *(Angleterre 2000) Montrer que pour tout naturel n,*

$$121^n - 25^n + 1900^n - (-4)^n \tag{1}$$

est divisible par 2000.

Solution. On montre que (1) est divisible par 16 et par 125, ce qui prouve l'énoncé. Pour faire ceci, on calcule l'expression modulo 16. On a $121 \equiv 25 \ (\equiv 9) \pmod{16}$, donc aussi $121^n \equiv 25^n \pmod{16}$. De même $1900 \equiv -4 \pmod{16}$, donc $1900^n \equiv (-4)^n \pmod{16}$. Tout ça nous donne

$$(121^n - 25^n) + (1900^n - (-4)^n) \equiv 0 + 0 = 0 \pmod{16}.$$

On procède d'une manière similaire modulo 125 car on a $121 \equiv -4 \pmod{125}$, donc $121^n \equiv (-4)^n \pmod{125}$ et $1900 \equiv 25 \pmod{125}$, ce qui entraîne $1900^n \equiv 25^n \pmod{125}$. Ceci nous donne finalement

$$(121^n - (-4)^n) + (1900^n - 25^n) \equiv 0 + 0 = 0 \pmod{125}.$$

□

Exemple 3. *Soit n un nombre naturel qui n'est divisible ni par 2 ni par 5. Montrer qu'il existe un multiple de n de la forme $111\ldots11$.*

Solution. Considérons les nombres

$$\begin{matrix} 1 \\ 11 \\ 111 \\ \vdots \\ \underbrace{111\ldots11}_{n+1} \end{matrix} \qquad (\mathrm{mod}\ n)$$

D'après le principe des tiroirs, deux de ces nombres doivent appartenir à la même classe d'équivalence modulo n. Donc leur différence est divisible par n et de la forme $111\ldots11000\ldots00 = 10^r \cdot \underbrace{111\ldots11}_{s}$. Puisque n et 10 n'ont pas de diviseur commun, n divise même $\underbrace{111\ldots11}_{s}$. □

Exemple 4. *(Irlande 96) Soit p un nombre premier et a, n deux entiers positifs qui satisfont l'équation*

$$2^p + 3^p = a^n.$$

Montrer qu'on a $n = 1$.

Solution. Pour $p = 2$ on a $2^p + 3^p = 13$, donc $n = 1$. Soit alors $p > 2$, donc en particulier impair. Le côté gauche de l'équation se factorise comme $(2+3)(2^{p-1} - 2^{p-2} \cdot 3 + \ldots - 2 \cdot 3^{p-2} + 3^{p-1})$ et est ainsi divisible par 5. Ceci est donc aussi le cas pour le côté droit, donc a est divisible par 5. Si on suppose maintenant $n > 1$, le côté droit est même divisible par 25, et alors le côté gauche aussi. Mais alors $(2^{p-1} - 2^{p-2} \cdot 3 + \ldots - 2 \cdot 3^{p-2} + 3^{p-1})$ doit être divisible par 5. On calcule cette expression modulo 5 en utilisant la congruence $3 \equiv -2\ (5)$:

$$2^{p-1} - 2^{p-2} \cdot 3 + \ldots - 2 \cdot 3^{p-2} + 3^{p-1} \equiv 2^{p-1} - 2^{p-2}(-2) + \ldots - 2(-2)^{p-2} + (-2)^{p-1} = p2^{p-1} \quad (5).$$

Puisque 2 et 5 n'ont pas de diviseur commun, il suit $p \equiv 0\ (5)$, donc $p = 5$, car p est premier. Mais pour $p = 5$ on obtient $2^p + 3^p = 5^2 \cdot 11$ et c'est en contradiction avec $n > 1$. □

1.2 La fonction φ et le théorème d'Euler-Fermat

Comme nous l'avons mentionné précédemment, il est généralement faux que si $a \equiv b\ (m)$ alors $n^a \equiv n^b\ (m)$. Cependant pour n'importe quel nombre entier n, par le principe des tiroirs on peut trouver deux nombres entiers positifs c et d tels $n^c \equiv n^d\ (m)$. De plus nous avons alors

$$n^{c+1} = n \cdot n^c \equiv n \cdot n^d = n^{d+1} \quad (m).$$

Il s'ensuit donc que pour des valeurs de a suffisamment grandes la suite de congruences $n^a \ (m)$ doit être périodique. Nous allons étudier plus tard la périodicité exacte de cette suite, et en particulier nous constaterons que la période dépend du nombre n. Dans ce paragraphe nous allons voir une technique qui permet de simplifier le calcul de puissances élevées modulo m. Notre outil principal sera une fonction arithmétique qu'on va définir maintenant.

Définition 1.1. Pour un naturel m la *fonction φ d'*EULER est définie par

$$\varphi(m) = \#\{a \in \mathbb{Z} \mid 1 \leq a \leq m \ , \ \mathrm{pgcd}(a, m) = 1\}.$$

Cette fonction compte le nombre d'entiers positifs inférieurs à m qui n'ont aucun diviseur commun avec m.

Proposition 13. *La fonction φ possède les propriétés suivantes:*

(i) La fonction φ est multiplicative, c'est-à-dire

$$(m, n) = 1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

(ii) Si m se décompose en facteurs premiers $m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, alors on a

$$\begin{aligned} \varphi(m) &= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\ &= p_1^{n_1-1} p_2^{n_2-1} \cdots p_r^{n_r-1}(p_1 - 1)(p_2 - 1)\cdots(p_r - 1). \end{aligned}$$

Preuve. On va montrer seulement (ii). Pour $m = p^n$, a est sans diviseur commun avec m si a n'est pas divisible par p. Il existe exactement $p^n/p = p^{n-1}$ nombre a qui sont divisibles par p avec $1 \leq a \leq m$, donc on a $\varphi(m) = p^n - p^{n-1} = p^{n-1}(p-1)$. La formule donnée découle de (i) si on applique ce calcul à tous les premiers p_k. □

Le résultat important de ce paragraphe est le théorème suivant, qui facilite les calculs de puissances modulo m.

Proposition 14 (Euler-Fermat)**.** *Soit m un nombre naturel et a un nombre entier tel que $(a, m) = 1$. Alors on a*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Preuve. Dans ce qui suit, on va simplifier les congruences sans mention explicite. Soient $a_1, a_2, \ldots, a_{\varphi(m)}$ les naturels inférieurs à m, qui n'ont pas de diviseur commun avec m. Considérons les nombres $aa_1, aa_2, \ldots, aa_{\varphi(m)}$. On prétend qu'ils forment une permutation des nombres$a_1, a_2, \ldots, a_{\varphi(m)}$ modulo m. Puisque a et a_k n'ont pas de diviseur commun avec m, ceci est aussi valable pour aa_k. Supposons que $aa_k \equiv aa_l \ (m)$, alors on a $a_k \equiv$

a_l par 12, et donc $a_k = a_l$ car $1 \leq a_k, a_l \leq m$. Par conséquent, les aa_k représentent effectivement une permutation des a_k, d'où

$$\begin{aligned} a_1 a_2 \cdots a_{\varphi(m)} &\equiv (aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \\ &\equiv a^{\varphi(m)}(a_1 a_2 \cdots a_{\varphi(m)}) \\ \Longrightarrow \quad 1 &\equiv a^{\varphi(m)} \pmod{m}, \end{aligned}$$

où l'on a de nouveau utilisé 12 pour la dernière implication. □

Puisque pour tout nombre premier p on a $\varphi(p) = p - 1$, il en découle immédiatement le cas particulier suivant:

Corollaire 15 (Petit théorème de Fermat)**.** *Soit p un premier et a pas divisible par p. Alors on a*

$$a^{p-1} \equiv 1 \pmod{p}.$$

En plus, pour tout a (y compris si a est divisible par p), la congruence suivante est valable:

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

Avant de voir comment appliquer ce résultat dans des exemples, nous allons d'abord brièvement discuter de la division modulo m.

Remarque. *Soit m un entier positif et a un nombre entier tel que $(a, m) = 1$. Le nombre $b = a^{\varphi(m)-1}$ satisfait les égalités $ab \equiv 1 \pmod{m}$ et $ba \equiv 1 \pmod{m}$. Autrement dit c'est un inverse multiplicatif pour a modulo m, et nous écrirons généralement $b = a^{-1}$.*

La multiplication par b permet donc de définir la division par a modulo m. Il est également possible de définir b par l'identité de Bézout: puisque $(a, m) = 1$, il existe des nombres entiers b, k tels que $ab + km = 1$, autrement dit $ab \equiv 1 \pmod{m}$.

En particulier il est intéressant de noter que si $m = p$ est un nombre premier, alors a admet un facteur commun avec p si et seulement si $a \equiv 0 \ (p)$, et ainsi les congruences modulo p forment un corps

Notons que jusque là nous avons seulement parlé de division lorsque a est premier avec m. Cette restriction est en fait indispensable: si a n'est pas premier avec m, alors l'équation $ax \equiv b \ (m)$ n'admet jamais une solution unique. Selon la valeur de b il y a soit aucune solution, soit strictement plus qu'une solution.

Exemple 5. *Montrer que* $7 \mid 2222^{5555} + 5555^{2222}$

Solution. On calcule les deux nombres modulo 7 et on obtient $2222 \equiv 3$ et $5555 \equiv 4 \ (7)$. De plus $\varphi(7) = 6$ et la division avec reste nous donne $2222 = 370 \cdot 6 + 2$ et $5555 = 925 \cdot 6 + 5$.

D'après Fermat, on a alors modulo 7

$$2222^{5555} \equiv 3^{5555} = 3^{925\cdot 6+5} = (3^6)^{925} \cdot 3^5 \equiv 1^{925} \cdot 243 \equiv 5$$
$$5555^{2222} \equiv 4^{2222} = 4^{370\cdot 6+2} = (4^6)^{370} \cdot 4^2 \equiv 1^{370} \cdot 16 \equiv 2.$$

On additionne les deux congruences pour obtenir le résultat désiré. □

Exemple 6. *Soient a, b premiers entre eux. Montrer qu'il existe deux nombres naturels m, n avec*

$$a^m + b^n \equiv 1 \pmod{ab}.$$

Solution. Soit $m = \varphi(b),\ n = \varphi(a)$. Par Euler-Fermat on obtient $a^m + b^n \equiv a^{\varphi(b)} + 0 \equiv 1$ (b), puisque a et b n'ont pas de diviseur commun. De même on a $a^m + b^n \equiv 0 + b^{\varphi(a)} \equiv 1$ (a). Par conséquent,$a^m + b^n - 1$ est congruent à 0 modulo a et b, donc divisible par a et b, et aussi par ab (a et b premiers entre eux), ce qui était l'affirmation à démontrer. □

Le théorème d'Euler-Fermat montre que lorsque $(a, m) = 1$, la suite $1 = a^0, a, a^2, \ldots$ se répète avec une période de $\varphi(m)$. Il arrive souvent que la période d'une telle suite soit plus petite que $\varphi(m)$ (cette période est toujours un diviseur de $\varphi(m)$). Nous allons donner ici quelques exemples pour illustrer ce qu'on peut prouver grâce à la périodicité de la suite $a^n\ (m)$, et nous reviendrons plus en détail sur cette périodicité lorsque nous discuterons *l'ordre* d'un nombre modulo m.

Exemple 7. *Soit n un naturel impair. Montrer que la représentation décimale de $2^{2n}(2^{2n+1} - 1)$ se termine par 28.*

Solution. Les deux derniers chiffres d'un nombre sont congruents à ce nombre modulo 100 $A = 2^{2n}(2^{2n+1} - 1) - 28$ est divisible par 100 pour tout n. On a que 2^{2n} est toujours divisible par 4 pour $n \geq 1$, donc c'est aussi le cas pour A. Il suffit alors de montrer la divisibilité par 25. Puisque n est impair, on peut substituer $n = 2k + 1$ et on obtient $A = 4 \cdot 16^k(8 \cdot 16^k - 1) - 28$. On calcule maintenant les puissances de 16 modulo 25:

$$16^0 \equiv 1,\ 16^1 \equiv 16,\ 16^2 \equiv 6,\ 16^3 \equiv 21,\ 16^4 \equiv 11,\ 16^5 \equiv 1 \pmod{25}$$

Elles sont périodiques avec période 5, c'est-à-dire qu'il suffit de considérer les cas $k = 0, 1, 2, 3, 4$:

$$\begin{aligned}
k = 0: &\quad A \equiv 4(8 - 1) - 28 &&\equiv 0\\
k = 1: &\quad A \equiv 4 \cdot 16(8 \cdot 16 - 1) - 28 \equiv 14 \cdot 2 - 28 &&\equiv 0\\
k = 2: &\quad A \equiv 4 \cdot 6(8 \cdot 6 - 1) - 28 \equiv (-1) \cdot (-3) - 28 &&\equiv 0\\
k = 3: &\quad A \equiv 4 \cdot 21(8 \cdot 21 - 1) - 28 \equiv 9 \cdot 17 - 28 &&\equiv 0\\
k = 4: &\quad A \equiv 4 \cdot 11(8 \cdot 11 - 1) - 28 \equiv 19 \cdot 12 - 28 &&\equiv 0
\end{aligned}$$

Dans chaque cas, A est divisible par 25 et ceci termine la preuve. □

Exemple 8. *Trouver tous les nombres naturels x, y qui satisfont $3^x - 2^y = 7$.*

Solution. Supposons d'abord $y \geq 3$. Alors $3^x \equiv 7 \pmod 8$. Mais un petit calcul nous montre que 3^x est toujours congruent à 1 ou à 3 (mod 8), donc on n'a pas de solutions dans ce cas. Si on a $y = 1$, alors $x = 2$. Pour $y = 2$ l'équation n'a pas de solution. Donc la seule solution est $(2, 1)$. □

Souvent on peut montrer qu'une expression ne peut pas prendre certaines valeurs en la regardant modulo un nombre approprié. C'est l'idée de l'exercice suivant:

Exemple 9. *Soient m, n deux naturels. Trouver le plus petit nombre A qui peut s'écrire comme $|36^m - 5^n|$.*

Solution. Pour $m = 1$ et $n = 2$, on trouve $A = 11$. On va montrer que ceci est la plus petite valeur possible. Puisque 5 et 36 n'ont pas de diviseur commun, A ne peut pas être divisible par $2, 3$ ou 5, donc $A \neq 0, 2, 3, 4, 5, 6, 8, 9, 10$. Il reste a exclure les cas $A = 1$ et $A = 7$. Si $A = 1$ ou $A = 7$, on a $36^m - 5^n = 1, -1, 7, -7$. Modulo 10 on trouve $36^m \equiv 6$ et $5^n \equiv 5$ pour tout $m, n \geq 1$. Donc $36^m - 5^n \equiv 6 - 5 \equiv 1 \pmod{10}$ et par conséquent $36^m - 5^n \neq -1, 7, -7$. Modulo 4 on obtient $36^m - 5^n \equiv 0 - 1^n \equiv 3$, donc $36^m - 5^n = 1$ n'est pas possible non plus. Ceci termine la preuve. □

1.3 Restes quadratiques et puissances élevées.

Un des faits les plus importants en théorie des nombres est que les carrés ne peuvent pas prendre n'importe quelle valeur modulo m. Voici quelques exemples pour illustrer ceci:

Exemple 10. *Trouver toutes les solutions non négatives entières de l'équation*

$$x^2 + y^2 = 2^n + 3.$$

Solution. L'idée est de considérer l'équation modulo 4. Le fait important est que pas tous les nombres ne sont des carrés modulo 4. Si $x \equiv 0$ ou $\equiv 2$ (4) est pair, alors on a $x^2 \equiv 0$ (4). Si $x \equiv 1$ ou $\equiv 3$ (4) est impair, alors $x^2 \equiv 1$ (4). Donc un carré est toujours $\equiv 0$ ou 1 (4). Par conséquent, le côté gauche de l'équation ne prend que les valeurs $0, 1$ ou 2. En supposant que $n \geq 2$, le côté droit vaut 3 (4) et l'équation n'est pas satisfaite. Les cas restants nous donnent $(x, y, n) = (2, 0, 0), (0, 2, 0), (2, 1, 1)$ et $(1, 2, 1)$. □

Voici une liste des restes quadratique pour quelques modules importants:

(mod 3)

n	0	1	2
n^2	0	1	1

(mod 4)

n	0	1	2	3
n^2	0	1	0	1

(mod 5)

n	0	1	2	3	4
n^2	0	1	4	4	1

(mod 8)

n	0	1	2	3	4	5	6	7
n^2	0	1	4	1	0	1	4	1

(mod 16)

n	0	1	2	3	4	5	6	7	8
n^2	0	1	4	9	0	9	4	1	0

L'exercice suivant vient des Olympiades d'Australie et très peu de participants on trouvé la solution. Il est effectivement très difficile de trouver la solution uniquement avec des calculs algébriques. Cependant si on considère le problème modulo 16, il devient presque trivial.

Exemple 11 (Australie 01)**.** *Montrer qu'il n'existe pas des entiers x, y, z, w avec*

$$x^2 = 10w - 1$$
$$y^2 = 13w - 1$$
$$z^2 = 85w - 1$$

Solution. Supposons que de tels nombres existent. Les carrés sont alors congruents à $0, 1, 4, 9$ modulo 16. Si $w \equiv 0, 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15 \ (16)$, alors d'après la première équation $x^2 \equiv 15, 3, 13, 7, 11, 5, 15, 3, 13, 7, 11, 5 \ (16)$, contradiction. Si $w \equiv 1, 13 \ (16)$, alors $y^2 \equiv 12, 8 \ (16)$, ce qui n'est pas possible non plus. $w \equiv 5, 9 \ (16)$, alors $z^2 \equiv 8, 12 \ (16)$, contradiction. Donc de tels nombres n'existent pas. □

On a vu l'efficacité de la réduction d'un problème modulo m. Puisque toutes les classes d'équivalence modulo m ne sont pas des carrés, on peut en tirer beaucoup d'informations. Tout cela n'est pas seulement valable pour des carrés mais aussi pour des k-èmes puissances. Dans ces cas, peut appliquer la règle suivante:

S'il s'agit de k-ème puissances, alors choisir m comme puissance de 2 ou tel que $k \mid \varphi(m)$.

L'idée derrière la règle énoncée ci-dessus devrait être plus claire après la lecture du chapitre suivant.
Si on considère des 3-èmes puissances, on doit choisir m tel que $3 \mid \varphi(m)$. La solution la plus petite est $m = 7$. Effectivement, une comparaison entre $m = 7$ et $m = 11$ nous montre clairement la différence:

n	0	1	2	3	4	5	6
n^3	0	1	1	6	1	6	6

(mod 7)

n	0	1	2	3	4	5	6	7	8	9	10
n^3	0	1	8	5	9	4	7	2	6	3	10

(mod 11)

L'exemple suivant était le problème le plus difficile des Olympiades des Balkans 98:

Exemple 12 (BalkMO 98)**.** *Montrer que l'équation*

$$y^2 = x^5 - 4.$$

n'a pas de solution entière.

Solution. Il y a des 2-ème et 5-ème puissances, donc on cherche un m avec $2 \mid \varphi(m)$ et $5 \mid \varphi(m)$ pour ensuite considérer l'équation modulo m. Le choix le plus simple est $m = 11$. Un petit calcul montre que les carrés sont $\equiv 0, 1, 3, 4, 5, 9 \ (11)$ et les 5-èmes puissances $\equiv 0, 1, 10 \ (11)$. Supposons que l'équation ait une solution (x, y). Alors le côté gauche de

l'équation vaut $\equiv 0, 1, 3, 4, 5, 9$ (11) et le côté droit $\equiv 6, 7, 8$ (11), contradiction. Donc l'équation n'a pas de solution entière. □

1.4 Ordres modulo m

Comme nous l'avons déjà vu, lorsque $(a, m) = 1$, la suite $1 = a^0, a, a^2, a^3, \ldots$ est périodique modulo m. Le théorème d'Euler-Fermat nous dit que pour tous les entiers a premiers avec m cette suite se répète avec une période de $\varphi(m)$. Cependant en général la période de cette suite (à savoir le plus petit entier positif d tel que $a^n \equiv a^{n+d}$ (m) pour tout n) est inférieur à $\varphi(m)$. Par exemple pour $a = 16$ et $m = 25$ nous avons vu que la période vaut 5 et non $\varphi(25) = 20$.

Définition 1.2. Soit m un entier positif et a un entier premier avec m. On définit *l'ordre* de a modulo m comme le plus petit entier strictement positif d tel que $a^{n+d} \equiv a^n$ (m) pour tout entier n.

Une propriété très utile est que l'ordre d'un nombre modulo m est toujours un diviseur de $\varphi(m)$.

Proposition 16. *Soient a, d et m comme ci-dessus. Si n est un nombre entier tel que $a^n \equiv 1$ (m), alors on a $d \mid n$.*

Démonstration. On effectue la division avec reste et on obtient $n = kd + r$ avec $0 \leq r \leq d - 1$. De plus, les propriétés des congruences nous donne

$$1 \equiv a^{\varphi(m)} \equiv a^{kd+r} \equiv (a^d)^k \cdot a^r \equiv 1^k \cdot a^r \equiv a^r \quad (m)$$

donc r satisfait la condition $a^r \equiv 1$ (m). Cependant d est défini comme le plus petit entier strictement positif avec cette propriété et r est strictement plus petit que d. On doit donc nécessairement avoir $r = 0$, ce qui signifie que d divise n. □

En particulier on a donc $d \mid \varphi(m)$. Dans certain cas on peut également prouver que d est un diviseur d'un nombre qui est presque premier avec $\varphi(m)$, ce qui implique que d doit être petit. Nous allons tout de suite voir comment cette idée peut être utilisée pour avancer dans la résolution d'un ancien exercice d'IMO:

Exemple 13 (IMO 90)**.** *Trouver tous les entiers naturels n tels que la fraction*

$$\frac{2^n + 1}{n^2}$$

est un nombre entier.

solution. Clairement $n = 1$ est solution. Nous pouvons donc considérer $n > 1$ pour le reste de la solution et nous allons montrer que dans ce cas le plus petit facteur premier de n est $p = 3$.

Puisque $n > 1$ le numérateur est toujours impair, donc le dénominateur doit également être impair et donc n n'est pas divisible par 2. Soit p le plus petit facteur premier de n et soit d l'ordre de 2 modulo p. Nous avons d'une part que d divise $\varphi(p) = p-1$. D'autre part, p doit diviser $2^n + 1$, donc $2^n \equiv -1 \ (p)$, et ainsi $2^{2n} \equiv 1 \ (p)$, ce qui signifie que d divise également $2n$. Il s'ensuit donc que d divise $(p-1, 2n)$. Puisque p a été choisi comme le plus petit facteur premier de n, cela signifie que $p-1$ est premier avec n, et donc puisque p est impair nous avons $(p-1, 2n) = (p-1, 2) = 2$, donc $d = 1, 2$. Si $d = 1$ on aurait alors $2^1 \equiv 1 \ (p)$, ce qui est impossible, donc on a $d = 2$ et $2^2 \equiv 1 \ (p)$, ce qui est possible uniquement si $p = 3$. □

Cette idée de considérer le plus petit facteur premier d'un nombre est très importante et peut souvent amener à progresser dans la résolution d'un exercice. La solution ci-dessus fonctionne car p est un diviseur de n mais également de $2^n + 1$, ce qui fournit deux conditions de divisibilité pour n quasiment incompatibles.

On peut terminer la solution de la manière suivante: en utilisant une technique enseignée seulement après le tour final, on arrive à prouver que n n'est pas divisible par 9. On peut donc écrire $n = 3m$ avec m un nombre qui n'est pas divisible par 3. On termine la solution en prouvant de la même manière que ci-dessus que si $m > 1$, le plus petit facteur premier de m est 7, ce qui mène rapidement à une contradiction.

Une application très importante des ordres est le résultat suivant, qui est assez surprenant à première vue:

Exemple 14. *Soit p un nombre premier impair et soit a, b deux nombres entiers qui ne sont pas divisibles par p. Si p divise $a^{2^n} + b^{2^n}$, alors $p \equiv 1 \pmod{2^{n+1}}$*

Solution. Puisque p ne divise pas b, ce nombre admet un inverse b^{-1} modulo p. En multipliant l'expression $a^{2^n} + b^{2^n}$ par $(b^{-1})^{2^n}$ on obtient alors que p divise $c^{2^n} + 1$ avec $c = ab^{-1}$. Autrement dit on obtient les deux congruences

$$c^{2^n} \equiv -1 \pmod{p} \quad c^{2^{n+1}} \equiv 1 \pmod{p}.$$

Soit d l'ordre de c modulo p. On obtient donc $d \mid 2^{n+1}$ d'une part, et $d \nmid 2^n$ puisque $c^{2^n} \equiv -1 \not\equiv 1 \pmod{p}$ d'autre part, donc la seule solution est $d = 2^{n+1}$. En utilisant la relation de divisibilité $d \mid \varphi(p) = p-1$ on obtient la congruence $p \equiv 1 \pmod{2^{n+1}}$. □

Cette affirmation paraît assez technique. Elle admet cependant comme cas particulier les résultats suivants, qui peuvent être très utile dans la résolution d'exercices d'olympiades:

- Si a et b sont premiers entre eux, alors tout facteur premier impair de $a^{2^n} + b^{2^n}$ est congruent à $1 \pmod{2^{n+1}}$! C'est en particulier le cas lorsque $b = 1$.
- Un cas encore plus spécifique de l'exemple précédent est lorsque $a = 2, b = 1$. On obtient alors les *nombres de Fermat* $F_n = 2^{2^n} + 1$, à propos desquels Fermat a supposé à tort qu'ils étaient tous premiers. Par exemple F_5 est divisible par

641. Cependant tous les facteurs premiers de F_n sont vraiment grands, car ils sont congruents à 1 $\pmod{2^{n+1}}$, donc en particulier ils ne sont pas plus petits que $2^{n+1}+1$. C'est la raison pourquoi les nombres de Fermat sont très difficiles à factoriser.

- Si $p \equiv 3$ (4) divise a^2+b^2, alors p divise a et b.

Dans tous les exemples précédents nous avons pu grâce aux ordres déduire des affirmations à propos des diviseurs premiers de différents nombres. Aucune autre méthode que nous avons apprise ne permet de déduire des affirmations aussi fortes. Pour cette raison les ordres sont une aide technique inévitable dans la résolution de problèmes de théorie des nombres.

Comme dernier exemple nous présentons encore un résultat connu et très utile à propos des facteurs premiers des suites géométriques. Nous rappelons à cet effet que pour $a \neq 1$ et tout entier naturel n, on a la formule $1 + a + \ldots + a^{n-1} = \frac{a^n-1}{a-1}$.

Exemple 15. *Soit p un nombre premier et $a \neq 1$ un nombre entier. Si q est un facteur premier de*

$$\frac{a^p-1}{a-1},$$

alors soit $q = p$, soit $q \equiv 1 \pmod{p}$. De plus le cas $q = p$ est possible uniquement si $p \mid a-1$.

Solution: Soit q un tel nombre premier et d l'ordre de a modulo q. Puisque $q \mid a^p - 1$, on a ainsi $a^p \equiv 1$ (q) et donc $d \mid p$. Il n'y a donc que deux cas possibles: soit $d = 1$, soit $d = p$. Si $d = p$, alors $p = d \mid \varphi(q) = q-1$, donc on obtient $q \equiv 1$ (p). Si $d = 1$, alors $a \equiv 1$ (q), et alors on peut écrire

$$0 \equiv a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv 1 + 1 + \ldots + 1 \equiv p \pmod{q}$$

donc q divise p, et comme p et q sont tous les deux premiers $q = p$. De plus dans ce cas on a bien $p = q \mid a-1$. □

2 Le théorème des restes chinois

Le théorème des restes chinois est un résultat qui permet de formaliser une propriété relativement intuitive des calculs modulaires. De manière informelle, le théorème des restes chinois permet de répondre à la question suivante:

Exemple 16. *Supposons que l'on ait une suite arithmétique de raison 7, combien de termes de cette suite sont divisibles par 3? Et à quelle fréquence est-ce que de tels termes apparaissent dans cette suite?*

Il convient déjà ici de mentionner le piège principal lorsque l'on souhaite appliquer le théorème des restes chinois: dans l'exemple ci-dessus il est important que les nombres

3 et 7 soient premiers entre eux. Nous reviendrons sur ce point après avoir énoncé le théorème sous sa forme générale.

Proposition 21 (Théorème des restes chinois)**.** *Soient $m_1, m_2, \ldots, m_r$ des nombre naturels deux-à-deux premiers entre eux et soient $a_1, a_2, \ldots, a_r$ arbitraires. Alors le système de congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \qquad\quad \vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

a une solution entière x. Cette solution est uniquement déterminée modulo $m_1 m_2 \cdots m_r$.

Exemple 17. *Voici un exemple concret. Soit x tel que*

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

On cherche la classe d'équivalence de x modulo 35.

Solution. La première congruence nous donne $x \equiv 3, 8, 13, 18, 23, 28$ ou 33 modulo 35. De même, on trouve par la deuxième $x \equiv 2, 9, 16, 23$ ou 30 modulo 35. La seule classe d'équivalence modulo 35 qui satisfait les deux conditions est 23. Donc $x \equiv 23 \pmod{35}$ est la seule solution du système de congruences, comme nous le confirme aussi le théorème 21 □

Comme promis plus haut, il est temps de voir ce qu'il se passe lorsque les nombres m_i ne sont pas deux-à-deux premiers entre eux. En version courte, le phénomène qui se produit devrait rappeler des souvenirs à ceux qui sont familiers avec l'algèbre linéaire: soit le système de congruences ne possède aucune solution, soit il possède plusieurs solutions.

Exemple 18. *Considérons le système de congruence*

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 11 \pmod{15}. \end{aligned}$$

Il n'existe aucun nombre x qui vérifie ces deux congruences simultanément (quelle en est la raison?).

Si l'on considère cette fois le système de congruence

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 13 \pmod{15}, \end{aligned}$$

on voit que les solutions sont $x \equiv 28, 58, 88 \pmod{90}$. *Par contre, on voit que dans cet exemple la solution est unique modulo* $30 = \text{ppcm}(6, 15)$. *Ce n'est pas une coïncidence.*

Nous allons maintenant décrire plus en détail 3 situations dans lesquelles on peut utiliser le théorème des restes chinois. Ces 3 situations peuvent être appelées respectivement "Construction", "Destruction" et "Comptage". Notez cependant que cette liste sert uniquement d'illustration et n'a pas vocation à être exhaustive de tous les usages possibles.

2.1 Construction

Ici, on utilise le théorème des restes chinois sous la forme suivante:

Proposition 22. *Soient* $m_1, \ldots, m_r$ *des naturels deux-à-deux premiers entre eux et soit* $M = m_1 m_2 \cdots m_r$. *Soient de plus* $a_1, \ldots, a_r$ *des nombres entiers quelconques. Alors il existe un nombre entier* x *qui vérifie* $x \equiv a_i \pmod{m_i}$ *pour tous les* i *simultanément. De plus, pour tout entier* k, *le nombre* $x + kM$ *satisfait également toutes ces congruences.*

Exemple 19. *(OIM 89) Pour tout* n *il existe* n *nombres consécutifs dont aucun n'est une puissance d'un nombre premier.*

Solution. Voici une solution très élégante qui utilise le théorème des restes chinois. Choisissons $2n$ premiers distincts $p_1, p_2, \ldots, p_n$ et $q_1, q_2, \ldots, q_n$. Considérons le système suivant:

$$\begin{aligned} x &\equiv -1 \pmod{p_1 q_1} \\ x &\equiv -2 \pmod{p_2 q_2} \\ &\vdots \qquad\quad \vdots \\ x &\equiv -n \pmod{p_n q_n} \end{aligned}$$

D'après le théorème des restes chinois, il possède une solution entière x et on peut supposer $x > 0$. Mais ce système est construit de telle manière que $x + k$ possède en tant que diviseurs premiers p_k et q_k pour $1 \leq k \leq n$. Les n nombres $x + 1, x + 2 \ldots, x + n$ ne peuvent donc pas être des puissances d'un nombre premier. □

Exemple 20 (USAMO 2008/1)**.** *Prouver que pour tout entier positif* n, *il existe des nombres entiers deux-à-deux premiers entre eux* $k_1, \ldots, k_n$, *tous strictement plus grands que* 1, *tels que* $k_1 \cdots k_n - 1$ *est le produit de deux nombres entiers consécutifs.*

Solution. L'idée ici est de trouver des nombres entiers t tels que $P(t) = t(t+1) + 1 = t^2 + t + 1$ est divisible par au moins n nombres premiers distincts. Si on peut trouver n nombres premiers distincts p_i et des nombres t_i tels que $P(t_i) \equiv 0 \pmod{p_i}$, alors le théorème des restes chinois garantit l'existence d'un nombre entier t tel que $t \equiv t_i \pmod{p_i}$ pour chaque i et les propriétés du calcul modulaire assurent alors que $P(t) \equiv 0 \pmod{p_i}$ pour tous les i.

Tout ce qu'il reste à faire pour conclure est donc de prouver qu'il existe de tels nombres premiers $p_1, \ldots, p_n$. Pour cela on peut adapter la preuve d'Euclide de l'infinité des nombres premiers: on sait que $3 = P(1)$, et si on a déjà trouvé des nombres distincts $p_1, \ldots, p_n$, on choisit pour p_{n+1} un facteur premier de $P(p_1 \cdots p_n)$, et par construction p_{n+1} n'est aucun des nombres $p_1, \ldots, p_n$. □

2.2 Destruction

Cet exemple est probablement le moins intéressant de la liste, mais également le plus susceptible d'apparaître dans les problèmes d'olympiades. Le motto ici est que dans certains cas "les puissances de nombres premiers suffisent". De manière un peu plus formelle, on peut formuler de la manière suivante:

Proposition 23. *Soient $m_1, \ldots, m_r$ des nombres entiers deux-à-deux premiers entre eux et soit $M = m_1 \cdots m_r$. Afin de comprendre un nombre x modulo M, il suffit de comprendre x modulo chacun des m_i.*

Comme ce cas d'utilisation est probablement toujours un peu obscur voyons tout de suite un exemple d'application:

Exemple 21 (CH TST 2019, 7)**.** *Prouver que pour tout nombre entier $n > 1$ il existe deux nombres entiers a, b tels que n divise $4a^2 + 9b^2 - 1$.*

Solution. On étudie d'abord le cas où n est une puissance d'un nombre premier, $n = p^k$.

- Si $p = 2$, on peut choisir $a \equiv 0$ et $b \equiv \frac{4^k - 1}{3}$ modulo 2^k.
- Si $p \neq 2$, on peut choisir $a \equiv \frac{p^k + 1}{2}$ et $b \equiv 0$ modulo p^k.

Maintenant pour le cas général, si $n = p_1^{k_1} \cdots p_r^{k_r}$, le théorème des restes chinois nous assure de l'existence de nombres a, b modulo n qui satisfont toutes les relations de congruence modulo $p_i^{k_i}$ simultanément, et donc pour ces nombres a et b on a bien que $4a^2 + 9b^2 - 1 = 0$. □

Cet exemple peut paraître un peu magique à première vue. Cependant, avec l'habitude cela deviendra quelque chose de parfaitement naturel à faire, et il est tout à fait acceptable de se contenter d'écrire "par le théorème des restes chinois il suffit de résoudre le problème dans le cas $n = p^k$ uniquement" et de faire la distinction de cas comme ci-dessus. Dans un premier temps je conseille toutefois d'écrire explicitement le système de congruences auquel on applique le théorème des restes chinois.

2.3 Comptage

Dans les exemples précédents, on a à chaque fois utilisé le fait que le théorème des restes chinois assure l'existence d'un nombre qui satisfait toutes les relations de congruence simultanément, mais on n'a pas encore utilisé le fait que cette solution est unique. C'est

précisément ce que nous allons faire ici. L'idée est que si l'on veut compter le nombre de solutions on peut découper le problème en morceaux plus simples et ensuite multiplier le nombre de solutions pour chacun de ces morceaux pour obtenir le nombre total de solutions.

Exemple 22. *Il a déjà été mentionné précédemment que la fonction φ de Fermat vérifie une certaine propriété de multiplicativité, à savoir que si n_1, n_2 sont deux nombres entiers premiers entre eux, alors $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$.*

Solution. On va utiliser le théorème des restes chinois, bien que d'autres preuves soient également possibles. L'idée est que si un nombre m est premier avec $n = n_1 n_2$, alors il est aussi premier avec n_1 et n_2 puisque tout facteur premier commun de m et l'un de ces deux nombres serait aussi un facteur premier commun de m et n. Inversement si un nombre m est premier avec n_1 et n_2, alors il est également premier avec n puisque tout facteur premier commun de m et n devrait diviser soit n_1 soit n_2, en contradiction avec l'hypothèse que m est premier avec n_1 et n_2.

Maintenant nous savons par le théorème des restes chinois qu'il existe une bijection entre les classes de congruences m modulo n et les paires de classes de congruence (m_1, m_2) modulo n_1 resp. n_2. De plus on déduit de la discussion ci-dessus que m est premier avec n si et seulement si dans la paire correspondante (m_1, m_2) on a que m_1 est premier avec n_1 et m_2 est premier avec n_2 (car $m_i \equiv m \pmod{n_i}$). On conclut donc que $\varphi(n) = \varphi(n_1)\varphi(n_2)$. □

Il existe encore une autre possibilité d'application du théorème des restes chinois que nous n'allons pas développer ici, mais que je vais rapidement présenter pour la complétude. On peut nommer cette situation le *lifting*, et l'idée est que si un nombre admet le même reste modulo différents nombres premiers entre eux, alors il admet le même reste modulo leur produit. Plus formellement on peut formuler de la manière suivante:

Proposition 24. *Soient $m_1, \ldots, m_r$ des nombres entiers premiers entre eux et soit $M = m_1 \cdots m_r$. Si un nombre x satisfait $x \equiv a \pmod{m_i}$ pour chaque i avec a un nombre entier qui est le même pour chacun des m_i, alors x satisfait $x \equiv a \pmod{M}$.*

Ce résultat semble encore plus évident que les exemples d'application vu précédemment, mais l'intérêt réside dans le fait que M peut être un nombre immense alors que les m_i ont une taille plus raisonnable, et donc dans les cas favorables ce résultat nous permet d'estimer la taille de x.

3 Divers

3.1 Factorisations

Un élément important de la théorie des nombres, et en particulier pour l'OIM, sont les factorisations. On collecte ainsi des informations utiles sur la divisibilité, les congruences,

etc. des facteurs. Il s'agit en général d'expressions polynomiales en une ou plusieurs variables que l'on aimerait factoriser. Il existe beaucoup de manières de procéder, mais cela fait plutôt partie de la théorie des polynômes. Nous allons donc nous borner ici aux applications se rapportant à la théorie des nombres. Elles sont essentiellement composées de quelques faits simples qui, appliqués correctement, peuvent avoir un effet important.

Quelques faits à garder en mémoire:

- $a \mid bc$ et $(a, b) = 1 \Longrightarrow a \mid c$
- Si a et b sont premiers entre eux et $ab = x^k$ est une k-ième puissance, alors a et b sont eux-mêmes des k-ièmes puissance.
- Si p est un nombre premier et $ab = p^k$ une puissance de p alors a et b sont également des puissances de p.
- Si p est premier et $ab = p$, alors un des facteurs vaut 1.
- $a, b \in \mathbb{N},\ a \mid b \quad \Longrightarrow \quad a \leq b$

Dans ce qui suit, nous allons présenter un aperçu des formules binomiales. Souvent elles suffisent pour trouver une factorisation appropriée. La formule binomiale classique est bien sûr

$$\boxed{(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}$$

où x, y sont des nombres réels arbitraires et $n \geq 0$ un entier. On peut prouver cette formule par la combinatoire (interprétation des coefficients binomiaux) ou par induction. Les identités ci-dessous vont plus dans le sens de la factorisation d'une expression (en l'occurrence du côté gauche). La première vaut pour **tout** n naturel:

$$\boxed{x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})}$$

Ceci seulement si n est **impair**:

$$\boxed{x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + - \ldots - xy^{n-2} + y^{n-1})}$$

Et ceci uniquement si n est un nombre **pair**:

$$\boxed{x^n - y^n = (x+y)(x^{n-1} - x^{n-2}y + - \ldots + xy^{n-2} - y^{n-1})}$$

Voici encore une fois le cas spécial avec l'exposant qui vaut 2:

$$\boxed{\begin{array}{rcl} (x+y)^2 & = & x^2 + 2xy + y^2 \\ (x-y)^2 & = & x^2 - 2xy + y^2 \\ x^2 - y^2 & = & (x+y)(x-y) \end{array}}$$

En particulier, la différence de deux carrés est toujours factorisable. Ce fait important ne s'étend malheureusement pas à la somme de deux carrés. Toutefois, x^2+y^2 est également factorisable si $2xy$ est un carré. Dans le cas le plus simple, on obtient ainsi l'importante **identité de Sophie Germain**:

$$\boxed{x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)}$$

Il est facile de voir que cette identité est correcte. Toutefois, il serait beaucoup plus intéressant de se demander comment on trouve une telle formule. Voici un développement dont il faudrait se souvenir:

$$\begin{aligned} x^4 + 4y^4 &= (x^4 + 4x^2y^2 + 4y^4) - 4x^2y^2 = (x^2 + 2y^2)^2 - (2xy)^2 \\ &= (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2) \end{aligned}$$

Il est maintenant temps de voir quelques exemples.

Exemple 23 (Grèce 95)**.** *Trouver tous les nombres naturels n tels que $2^4 + 2^7 + 2^n$ est un carré.*

Solution. Nous cherchons en fait tous les n tels que $2^n = m^2 - 2^4 - 2^7 = m^2 - 144$ pour un naturel m. Cela peut être factorisé comme $2^n = (m + 12)(m - 12)$, donc $m + 12$ et $m - 12$ sont deux puissances de 2 dont la différence vaut 24. Les seules puissances de 2 remplissant cette condition sont $8 = 2^3$ et $32 = 2^5$, par conséquent $m = 20$ et $n = 8$. □

Exemple 24. *Montrer que le produit de quatre nombres naturels consécutifs n'est jamais un carré.*

Solution. Nous avons

$$\begin{aligned} n(n+1)(n+2)(n+3) &= n^4 + 6n^3 + 11n^2 + 6n \\ &= n^2(n^2 + 3n + 1) + 3n(n^2 + 3n + 1) + (n^2 + 3n + 1) - 1 \\ &= (n^2 + 3n + 1)^2 - 1. \end{aligned}$$

autrement dit ce produit est toujours plus petit de 1 qu'un carré. Les deux seuls carrés dont la différence vaut 1 sont 0 et 1. Comme $n(n + 1)(n + 2)(n + 3) \geq 24$ ceci ne peut jamais être un carré. □

Exemple 25. *Trouver tous les nombres premiers de la forme $n^n + 1$ qui sont plus petit que 10^{19}.*

Solution. Si $n = 1$, nous obtenons le nombre premier 2. Si n est impair, alors $n^n + 1$ est pair, donc pas premier. Ensuite, si $n > 1$ est pair, nous pouvons l'écrire comme $n = 2^t u$ avec $t \geq 1$ et u impair. Si $u > 1$, nous pouvons alors appliques la formule binomiale et factoriser comme suit:

$$n^n + 1 = \left(n^{2^t}\right)^u + 1^u = (n^{2^t} + 1)(\ldots),$$

où tous les facteurs sont plus grands que 1, le nombre n'est donc pas premier. il ensuit que $n = 2^t$. Pour $t = 1$, nous obtenons le nombre premier 5. Soit maintenant $t > 1$. Nous pouvons de nouveau l'écrire comme $t = 2^s v$ avec v impair. Si $v > 1$, la formule binomiale nous assure que

$$n^n + 1 = \left(2^{2^s n}\right)^v + 1^v = (2^{2^s n} + 1)(\ldots),$$

où les deux facteurs sont plus grands que 1. Ainsi, $v = 1$ et $n = 2^{2^s}$. Pour $s = 1$, nous trouvons $4^4+1 = 257$, un nombre premier. De plus, si $s \geq 2$, alors $n^n+1 \geq 16^{16}+1 > 10^{19}$. Les seuls nombres premiers satisfaisant cette condition sont donc 2, 5 et 257. □

Exemple 26 (Kürschak 78)**.** *Montrer que $n^4 + 4^n$ n'est jamais un nombre premier pour $n > 1$.*

Solution. Si n est pair, alors $n^4 + 4^n$ l'est également et vaut plus que 2, donc ce n'est pas un nombre premier. Si n est impair, nous pouvons alors écrire $n = 2k + 1$ avec $k \geq 1$. Par Sophie Germain, nous avons

$$\begin{aligned} n^4 + 4^n &= n^4 + 4^{2k+1} = n^4 + 4(2^k)^4 \\ &= (n^2 + 2 \cdot n \cdot 2^k + 2(2^k)^2)(n^2 - 2 \cdot n \cdot 2^k + 2(2^k)^2) \\ &= (n^2 + 2^{k+1}n + 2^n)(n^2 - 2^{k+1}n + 2^n). \end{aligned}$$

Le premier facteur est toujours plus grand que 1. Avec $2^n - 2^{k+1}n = 2^{k+1}(2^k - 2k - 1)$ et une estimation triviale, on trouve que, pour $k \geq 1$, le deuxième facteur est également plus grand que 1. Par conséquent, $n^4 + 4^n$ n'est jamais un nombre premier. □

L'exemple suivant montre comment on peut appliquer le calcul des modulos pour cueillir des informations à propos des exposants, ce qui peut mener à une factorisation appropriée.

Exemple 27. *Trouver tous les nombres naturels x, y, z, tels que*

$$2^x + 3^y = z^2.$$

Solution. Nous allons considérer l'équation modulo 3. Le côté droit est $\equiv 0, 1$, d'autre part nous avons $2^x \equiv 1$ si x est pair et $2^x \equiv 2$ si x est impair. Il s'ensuit que x doit être pair, donc en particulier que $x \geq 2$. Nous considérons maintenant l'équation modulo 3. Comme z est impair, le côté droit est $\equiv 1 \pmod 4$, par conséquent $3^y \equiv 1$. C'est le cas seulement si $y = 2s$ est pair. Nous pouvons maintenant factoriser:

$$2^x = (z - 3^s)(z + 3^s).$$

Les deux facteurs de droite sont des puissances de deux ≥ 2. Leur plus grand diviseur commun doit de surcroît diviser $2 \cdot 3^s$, il vaut donc 3. Ainsi, $z - 3^s = 2$ et $z + 3^s = 2^{x-1}$. En soustrayant la première équation à la deuxième et en divisant par 2, on obtient $3^s + 1 = 2^{x-2}$ et par conséquent $x > 2$. Pour $x = 4$, nous avons la solution $y = 2$ et $z = 5$. Si $x \geq 6$, alors $3^s + 1$ doit être divisible par 16. Cependant, un calcul rapide nous montre que $3^s \equiv 1, 3, 9, 11 \pmod{16}$, contradiction, L'unique solution est donc $(x, y, z) = (4, 2, 5)$. □

Exemple 28. *Montrer que pour tous les nombres naturels $n > 1$ et a, b, on a*

$$\text{pgcd}(n^a - 1, n^b - 1) = n^{\text{pgcd}(a,b)} - 1.$$

Solution. Soit $d = \text{pgcd}(a, b)$ et écrivons $a = dk$ et $b = dl$. Or il s'ensuit de la formule binomiale que $n^a - 1 = (n^d)^k - 1^k = (n^d - 1)(n^{d(k-1)} + n^{d(k-2)} + \ldots + n^d + 1)$, donc $n^d - 1 \mid n^a - 1$. Le calcul analogue pour b nous donne $n^d - 1 \mid \text{pgcd}(n^a - 1, n^b - 1)$. Inversement, par Bézout il existe deux entiers x, y avec $ax - by = d$. Nous avons alors $(n^a - 1) \mid (n^{ax} - 1)$ et $(n^b - 1) \mid (n^{by} - 1)$ ou encore

$$(n^{ax} - 1) - (n^{by} - 1) = n^{by}(n^d - 1).$$

Ainsi, $\text{pgcd}(n^a - 1, n^b - 1)$ divise le côte gauche de l'équation, donc également le côté droit. Comme $\text{pgcd}(n^{by}, n^b - 1) = 1$, il divise en particulier $n^d - 1$. Au final, il s'ensuit que $\text{pgcd}(n^a - 1, n^b - 1) = n^{\text{pgcd}(a,b)} - 1$. □

3.2 La valuation p-adique

Comme vous l'avez probablement constaté presque toute la théorie des nombres faite jusqu'à présent repose d'une manière ou d'une autre sur des questions de divisibilité. Nous avons lors du tour précédent étudié des problèmes qui peuvent être résolus uniquement par des considérations de divisibilité. Les techniques présentées au cours de ce tour ont jusqu'à présent reposé sur la congruence, qui permet d'étudier toutes les classes de congruence et pas uniquement celle de 0. Nous allons ici présenter une autre généralisation, où l'on ne s'intéresse pas seulement à savoir qu'un certain nombre est divisible par un nombre premier p, mais à la plus grande puissance de p qui divise ce nombre.

Définition 3.1. Soit p un nombre premier et a un nombre entier. On définit la *valuation p-adique* de a, notée $v_p(a)$, comme le nombre entier non-négatif α tel que $p^\alpha \mid a$ mais $p^{\alpha+1} \nmid a$. De manière informelle on peut dire que $v_p(a)$ compte combien de fois a est divisible par p.

On voit facilement avec la définition que si $a = p_1^{\alpha_1} \cdot p_k^{\alpha_k}$, alors $v_{p_i}(a) = \alpha_i$ pour tout $1 \leq i \leq k$. Pour $r = \frac{a}{b}$ un nombre rationnel, on peut définir sa valuation p-adique par $v_p(r) = v_p(a) - v_p(b)$. Il est facile de vérifier que cette définition ne dépend pas du choix de la fraction choisie pour représenter r.

Avant de voir comment utiliser la valuation pour des problèmes d'olympiade nous avons besoin de prouver certaines de ses propriétés.

Proposition 31. *Soit p un nombre premier et a, b deux nombres entiers. La valuation p-adique interagit avec l'addition et la multiplication de la manière suivante:*

- $v_p(ab) = v_p(a) + v_p(b)$
- $v_p(a + b) \geq \min(v_p(a), v_p(b))$. *De plus, nous avons égalité lorsque $v_p(a) \neq v_p(b)$.*

Démonstration. Soit $\alpha = v_p(a)$ et $\beta = v_p(b)$. On peut écrire $a = p^\alpha k$ et $b = p^\beta l$ avec k, l deux nombres entiers qui ne sont pas divisibles par p. On obtient alors $ab = p^{\alpha+\beta}kl$ et p ne divise pas kl, donc $v_p(ab) = \alpha + \beta$.

Pour la deuxième identité on peut supposer sans perte de généralité que $\alpha \leq \beta$. On peut alors écrire

$$a + b = p^\alpha(k + p^{\beta-\alpha}l),$$

ce qui suffit déjà à prouver que $v_p(a + b) \geq \alpha = \min(v_p(a), v_p(b))$. De plus, si $\alpha \neq \beta$, alors $\beta - \alpha > 0$ donc $k + p^{\beta-\alpha}l \equiv k \not\equiv 0 \pmod{p}$ donc $v_p(a + b) = \alpha$. Il est cependant important de noter qu'il est possible d'avoir égalité également dans le cas où $\alpha = \beta$. □

Le résultat précédent est également vrai lorsque a et b sont des nombres rationnels quelconques et pas uniquement des nombres entiers. La preuve dans ce cas est essentiellement la même que lorsque a, b sont entiers.

Nous allons voir un exemple où l'on utilise la valuation p-adique.

Exemple 29 (IMO 2018, P5)**.** *Soit $a_1, a_2, \ldots$ une suite infinie d'entiers strictement positifs. On suppose qu'il existe un entier $N > 1$ tel que, pour tout $n \geq N$, le nombre*

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \ldots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

soit un entier. Montrer qu'il existe un entier strictement positif M tel que $a_m = a_{m+1}$ pour tout $m \geq M$.

Solution. Dénotons la somme ci-dessus s_n. Une observation importante pour cet exercice est que s_n et s_{n+1} ont beaucoup de termes en commun. Il est donc probablement intéressant de prendre la différence et on obtient que

$$s_{n+1} - s_n = \frac{a_n}{a_{n+1}} + \frac{a_{n+1}}{a_1} - \frac{a_n}{a_1}$$

est un entier. En multipliant par a_1, il s'ensuit que $\frac{a_1 a_n}{a_{n+1}}$ est également un entier, et donc que $a_{n+1} \mid a_1 a_n$ pour tout $n \geq N$. En utilisant cette relation de manière répétée, on trouve que $a_n \mid a_1^{n-k} a_k$ et donc tous les facteurs premiers de a_n pour $n \geq k$ sont parmi ceux de $a_1 a_k$. En particulier il y a seulement un nombre fini de tels nombres premiers, donc il suffit de montrer que pour chacun d'eux, l'exposant dans la décomposition en facteur premier de a_n est constant à partir d'un certain point.

Soit p un facteur premier de $a_1 a_k$. Nous dirons qu'un indice $n \geq k$ est *large* si il satisfait $v_p(a_n) \geq v_p(a_1)$. Nous avons deux cas à traiter:

- Il existe un indice n large:

  Si $v_p(a_{n+1}) < v_p(a_1)$ alors $v_p(a_n/a_{n+1}) > 0$ et $v_p(a_n/a_1) \geq 0$ alors que d'un autre côté $v_p(a_{n+1}/a_1) < 0$, donc en utilisant les règles pour la valuation d'une somme

on obtient alors $v_p(s_{n+1} - s_n) < 0$, ce qui contredit le fait que ce nombre est entier. Autrement dit, on a nécessairement que $n+1$ est également un indice large.

Nous voulons de plus prouver que $v_p(a_{n+1}) \leq v_p(a_n)$. Cela suffit à conclure puisqu'on a alors que la suite $v_p(a_n), v_p(a_{n+1}), \ldots$ est une suite décroissante d'entiers bornée par en-dessous par $v_p(a_1)$, donc elle doit être constante à partir d'un certain point.

Supposons donc que $v_p(a_{n+1}) > v_p(a_n)$. On a alors $v_p(a_n/a_{n+1}) < 0$ alors que $v_p(a_{n+1}/a_1) > 0$ et $v_p(a_n/a_1) \geq 0$, donc de nouveau les règles pour la valuation d'une somme donnent $v_p(s_{n+1} - s_n) < 0$, contredisant le fait que ce nombre est entier.

- Il n'existe aucun indice large:

  Dans ce cas nous avons $v_p(a_1) > v_p(a_n)$ pour tout $n \geq k$. Si il existait un indice $n \geq k$ tel que $v_p(a_{n+1}) < v_p(a_n)$, alors nous aurions

  $$v_p(a_{n+1}/a_1) < v_p(a_n/a_1) < 0 < v_p(a_n/a_{n+1})$$

  et de la même manière que précédemment on obtient ainsi une contradiction avec le fait que $s_{n+1} - s_n$ est entier. Autrement dit dans ce cas la suite $v_p(a_k), v_p(a_{k+1}), \ldots$ est une suite croissante de nombres entiers bornée par $v_p(a_1)$, donc elle est constante à partir d'un certain point.

□

3.3 Estimations II

Nous avons déjà vu au tour précédent comment faire des estimations à partir de principes simples. Certains exercices peuvent être résolus par des estimations plus élaborées, dont nous allons montrer certains exemples ici.

Exemple 30. *(Angleterre 95) Trouver toutes les solutions entières positives de l'équation*

$$\left(1 + \frac{1}{a}\right)\left(1 + \frac{1}{b}\right)\left(1 + \frac{1}{c}\right) = 2.$$

Ici le terme de droite demeure constant tandis que le terme de gauche diminue quand a, b et c deviennent grands. Si toutes les trois variables sont très grandes, chacun des trois facteurs vaut environ 1 et l'équation ne peut pas être satisfaite. On va maintenant préciser cette idée.

Solution. L'équation est symétrique en a, b et c, on peut donc supposer sans perte de généralité que $a \geq b \geq c$. Alors d'un côté le terme de gauche vaut 2, mais d'un autre il vaut au plus $(1 + \frac{1}{c})^3$. Or un calcul rapide montre que $(1 + \frac{1}{c})^3 < 2$ si $c \geq 4$, ce qui entraîne $c \leq 3$. On distingue trois cas:

- $c = 1$: Comme $(1 + \frac{1}{a}) > 1$ et $(1 + \frac{1}{c}) = 2$, le terme de gauche est strictement plus grand que 2, contradiction.
- $c = 2$: L'équation devient $(1 + \frac{1}{a})(1 + \frac{1}{b}) = \frac{4}{3}$ et de façon similaire au cas précédent on obtient l'estimation $\frac{4}{3} \leq (1 + \frac{1}{b})^2$, autrement dit $b \leq 6$. Comme $(1 + \frac{1}{a}) > 1$ on a également $b \geq 4$. En testant les trois valeurs possibles de b on obtient les solutions $(7, 6, 2)$, $(9, 5, 2)$ et $(15, 4, 2)$.
- $c = 3$: L'équation devient $(1 + \frac{1}{a})(1 + \frac{1}{b}) = \frac{3}{2}$ et comme précédemment on obtient ici $b \leq 4$ et $b \geq c = 3$. En testant les deux valeurs possibles de b on obtient les solutions $(8, 3, 3)$ et $(5, 4, 3)$.

En fin de compte, les solutions sont donc les permutations de

$$(7, 6, 2), (9, 5, 2), (15, 4, 2), (8, 3, 3), (5, 4, 3).$$

Attention! Dans cet exemple on a posé par symétrie que $a \geq b \geq c$ pour simplifier le problème. Cependant cette relation n'est pas forcément vérifiée par les solutions et donc quand on écrit les solutions du problème il ne faut pas oublier d'indiquer aussi les possibles permutations. Les débutants se laissent souvent avoir. □

En faisant plusieurs estimations, on a trouvé des bornes supérieures pour c et b et à la fin il nous restait juste quelques cas à tester. Je ne connais pas de solution de ce problème qui se passe complètement des estimations.

Exemple 31. *Trouver toutes les solutions entières positives de l'équation*

$$abc = ab + bc + ca + 12.$$

Ici le terme de gauche croît plus vite que celui de droite quand a, b et c augmentent. Le terme de gauche est un polynôme de degré 3, celui de droite seulement de degré 2. Comment peut-on quantifier tout cela?

Solution. Sans perte de généralité, soit $a \geq b \geq c$. Comme on a déjà vu, c doit être petit. En effet, pour $c \geq 4$ on obtient immédiatement $abc \geq 4ab \geq ab + bc + ca + 4^2 > ab + bc + ca + 12$, contradiction. Ainsi $c \leq 3$.

- $c = 3$: $3ab = ab+3a+3b+12 \Leftrightarrow ab+(a-3)(b-3) = 21$. Puisque $a \geq b \geq 3$ on a $ab \leq 21$. Pour (a, b) les seules solutions potentielles sont $(7, 3), (6, 3), (5, 3), (4, 3), (3, 3), (5, 4), (4, 4)$ et un calcul rapide montre qu'il n'y a que la première qui en est effectivement une.
- $c = 2$: $2ab = ab + 2a + 2b + 12 \Leftrightarrow (a - 2)(b - 2) = 16$. Vu que $a \geq b \geq 2$, on obtient les solutions $(a, b) = (18, 3), (10, 4), (6, 6)$.
- $c = 1$: $ab = ab + a + b + 12 \Leftrightarrow a + b = -12$ n'a pas de solution positive

En fin de compte les solutions (a, b, c) sont donc les permutations de

$$(18, 3, 2), (10, 4, 2), (6, 6, 2), (7, 3, 3).$$

□

Exemple 32. *Trouver toutes les solutions entières positives de* $x^3 - y^3 = xy + 61$.

Ici le côté gauche est de degré 3 et le côté droit de degré 2, mais le côté gauche peut rester petit même pour des x et y très grands. L'argument qu'on avait utilisé pour l'exercice précédent ne s'applique pas directement ici. Ce qui importe est la différence des deux nombres. C'est grâce à elle que le côté gauche croît plus vite que le côté droit.

Solution. Pour approfondir ce raisonnement, on pose $d = x - y$. Comme le côté droit de l'équation est toujours positif, on a $d > 0$. En substituant on trouve $(y+d)^3 - y^3 = (y+d)y + 61 \Leftrightarrow (3d-1)y^2 + (3d^2 - d)y + d^3 = 61$, en particulier $d^3 \leq 61$ donc $d \leq 3$, car les deux parenthèses à gauche sont non négatives. Pour $d = 1$ on obtient l'équation $y^2 + y - 30 = 0$ avec comme unique solution positive $y = 5 \Rightarrow x = 6$. Pour $d = 2, 3$ les équations correspondantes n'ont pas de solutions entières. La seule solution est donc $(x, y) = (6, 5)$. □

Un autre contexte où il peut être intéressant de procéder à des estimations est lorsque certains termes sont des factorielles. Un autre outil pratique pour procéder à des estimations est d'utiliser des valuations p-adiques. Nous allons voir un exemple qui combine ces deux idées, mais auparavant nous avons besoin d'un peu de préparation

Proposition 32 (Formule de Stirling)**.** *Asymptotiquement, nous avons l'approximation*

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

Autrement dit, lorsque n devient arbitrairement grand, le quotient de ces deux expressions devient arbitrairement proche de 1*.*

Je n'ai vu aucun exercice d'olympiades qui utilise la formule de Stirling et je ne vous recommande pas de l'apprendre par cœur. Pour les olympiades il suffit d'utiliser des approximations plus grossières, par exemple que $n!$ grandit à peu près comme n^n, et donc que pour tout entier a on a $n! > a^n$ si n est suffisamment grand. Il existe un nombre infini de variations sur ce thème, et il convient de trouver l'estimation appropriée pour un problème donné.

Exemple 33 (IMO 2019, P4)**.** *Trouver tous les couples d'entiers naturels non nuls* (k, n) *tels que*

$$k! = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}).$$

Solution. Au vu du nombre de puissances de 2 dans la formulation de ce problème, il est logique d'étudier la valuation 2-adique des deux côtés de l'équation. Pour le côté gauche,

nous avons l'estimation $v_2(k!) < k$ (il vous est demandé de prouver une généralisation de ce fait en exercice). D'autre part, pour le côté droit la valuation 2-adique vaut

$$v_2(2^n - 1) + v_2(2^n - 2) + \ldots + v_2(2^n - 2^{n-1}) = 0 + 1 + \ldots + (n-1) = \frac{n(n-1)}{2}.$$

Ainsi, puisque les deux côtés de l'équation sont égaux on obtient l'estimation

$$k > \frac{n(n-1)}{2}.$$

Afin d'obtenir une estimation dans l'autre sens, on remarque que

$$(2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}) < (2^n)(2^n)(2^n) \cdots (2^n) = 2^{n^2}.$$

En combinant cette estimation avec l'estimation précédente on trouve

$$2^{n^2} > (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}) = k! > \left(\frac{n(n-1)}{2}\right)!$$

Cependant, par la remarque faite précédemment que la factorielle grandit plus vite que n'importe quelle exponentielle, l'inégalité ci-dessus ne peut probablement être vraie que si n est suffisamment petit. Nous allons rendre cette dernière remarque plus précise:

Pour cet exercice nous allons utiliser l'estimation $k! \geq (k/e)^k$ pour tout entier k. En utilisant cette estimation on obtient ainsi

$$\left(\frac{n(n-1)}{2}\right)! > \left(\frac{n(n-1)}{6}\right)^{\frac{n(n-1)}{2}} = \sqrt{\frac{n(n-1)}{6}}^{n^2-n}.$$

On prouve facilement que cette dernière expression est strictement supérieure à 2^{n^2} lorsque $n \geq 7$, donc il suffit de considérer les paires (k, n) avec $n \leq 6$.

En étudiant toutes les valeurs possibles de n, on trouve que les seules solutions sont $(k, n) = (1, 1)$ et $(3, 2)$. □