ÉQUATIONS DIOPHANTIENNES MODULO N

Igor Kortchemski

- Rappels de cours -

Pour résoudre des équations diophantiennes, on a souvent recours à des congruences en considérant l'équation modulo N. Mais quel modulo N choisir ?

— s'il y a des puissances p-ième avec p premier, essayez $N = p^2$, p^3, etc.

En effet, si a n'est pas divisible par p, d'après le théorème d'Euler, $a^{p^{k-1}(p-1)} \equiv 1 \mod p^k$, de sorte que $(a^p)^{p^{k-2}(p-1)} \equiv 1 \mod p^k$, ce qui limite le nombre de valeurs prises par a^p modulo p^k.

— lorsqu'il intervient une puissance n-ième (avec n un entier connu), il peut être utile de choisir pour N un nombre premier congru à 1 modulo n.

En effet, dans ce cas, $a^{N-1} \equiv 1 \mod N$ d'après le petit théorème de Fermat, de sorte que $(a^n)^{\frac{N-1}{n}} \equiv 1 \mod N$, ce qui limite le nombre de valeurs prises par a^n modulo N.

— lorsqu'il intervient une puissance n-ième (où n est l'inconnue), disons a^n, il peut être utile de choisir $N = a^k$ (avec k supérieur à la plus grande solution supposée).

— lorsqu'il intervient une puissance n-ième (où n est l'inconnue), disons a^n, il peut être utile de choisir pour N un diviseur pas trop grand de $a^k - 1$ pour un certain entier k.

En effet, si on sait que n est congru à nombre fixé modulo un certain m (ou bien prend un nombre de valeurs limitées modulo m), il peut être judicieux de trouver N tel que l'ordre de a modulo N vaut m, ou bien divise m, ou bien soit un multiple de m. Dans les deux premiers cas, N divise $a^m - 1$, et dans le dernier cas N divise $a^k - 1$ avec k multiple de N.

En effet, dans les deux premiers cas, a^n est alors constant modulo N, et dans le troisième cas, a^n prend un nombre de valeurs limitées modulo N.

Il peut aussi être utile d'utiliser le fait que si $a^k \equiv 1 \mod N$ et si ω est l'ordre de a modulo N, alors $a^\omega - 1$ divise $a^k - 1$.

– Pour les équations de type $a^x = b^y + c$ (avec a, b, c connus et x et y connus) ayant un nombre fini de solutions, on considère (x_0, y_0) la "plus grande", en supposant $x > x_0, y > y_0$ on la retranche à l'équation originelle pour obtenir $a^{x_0}(a^{x-x_0} - 1) = b^{y_0}(b^{y-y_0} - 1)$. Quand a et b sont premiers entre eux, on a alors a^{x_0} qui divise $b^{y-y_0} - 1$. Si ω est l'ordre de b modulo a^{x_0}, on en déduit que $b^\omega - 1$ divise $b^{y-y_0} - 1$ et donc divise $a^{x-x_0} - 1$. On trouve alors un diviseur premier sympathique de $b^\omega - 1$ et on continue de proche en proche (on peut aussi partir du fait que b^{y_0} divise a^{x-x_0}) jusqu'à aboutir à une contradiction. C'est la méthode de *Dan Schwarz* (qui revient grosso modo à ce qui précède, mais donne peut-être plus facilement les bons modulos à considérer).

- Exercices -

Exercice 1 Soient $m, n \geq 1$ des entiers. Montrer que $3^m + 3^n + 1$ n'est pas un carré parfait.

Exercice 2 Trouver tous les entiers $x, y \geq 1$ tels que $3^x - 2^y = 7$.

Exercice 3 Trouver tous les entiers $x, y \in \mathbb{Z}$ tels que $15x^2 - 7y^2 = 9$.

Exercice 4 Montrer que quel que soit $n > 1$, $n^5 + 7$ n'est pas un carré.

Exercice 5 Trouver tous les entiers $n \geq 1$ tels que $2^n + 12^n + 2014^n$ soit un carré parfait.

Exercice 6 Existe-t-il des nombres rationnels positifs ou nuls x, y et z tels que $x^5 + 2y^5 + 5z^5 = 11$?

Exercice 7 Montrer que 19^{19} ne peut pas s'écrire comme la somme d'un cube et d'une puissance quatrième de nombres entiers.

Exercice 8 Trouver tous les entiers $x, y \geq 1$ tels que $x^5 = y^2 + 4$.

Exercice 9 Trouver tous les entiers $a, y \geq 1$ tels que $3^{2a-1} + 3^a + 1 = 7^y$.

Exercice 10 Trouver tous les entiers $a, b \geq 1$ tels que les deux nombres $a^5b + 3$ et $ab^5 + 3$ soient des cubes de nombres entiers.

Exercice 11 Trouver tous les entiers $x, y, z \geq 0$ tels que $5^x 7^y + 4 = 3^z$.

Exercice 12 Trouver tous les entiers $n, m, r \geq 1$ tels que $n^5 + 49^m = 1221^r$.

Exercice 13 Trouver tous les entiers $a \geq 1$ tels que l'entier $1 - 8 \cdot 3^a + 2^{a+2}(2^a - 1)$ soit un carré parfait.

Exercice 14 Trouver tous les entiers $x, y \geq 0$ tels que $2^x = 3^y + 5$.

Exercice 15 Trouver tous les entiers $m, n \geq 0$ tels que $3^m - 7^n = 2$.

Exercice 16 Trouver tous les entiers $k, n, m \geq 0$ tels que $5^n - 3^k = m^2$.

Exercice 17 Trouver tous les entiers $a, b, c, d \geq 1$ tels que $4^a \cdot 5^b - 3^c \cdot 11^d = 1$.

Exercice 18 Trouver tous les nombres entiers $x, y \geq 1$ tels que $7^x = 3^y + 4$.

Exercice 19 Trouver tous les entiers $x, y \geq 0$ tels que $33^x + 31 = 2^y$.

Exercice 20 Trouver tous les entiers $x, y \geq 1$ tels que $2^x + 3 = 11^y$.

Exercice 21 Trouver tous les entiers $x, y \geq 1$ tels que $2^x - 5 = 11^y$.

- Solutions des exercices -

Solution de l'exercice 1

On travaille modulo 8 : on remarque que $3^m + 3^n + 1$ est congru à 3, 5 ou 7 modulo 8. Or un carré est congru à 0, 1 ou 4 modulo 8, ce qui conclut.

Solution de l'exercice 2

On vérifie que $y = 1$ donne la solution $x = 2$, et que $y = 2$ ne donne pas de solution. On suppose donc $y \geq 3$. Il judicieux de travailler modulo 8 : on doit avoir $3^x \equiv 7 \mod 8$. Or une puissance de 3 n'est jamais congrue à 7 modulo 8, ce qui conclut.

Solution de l'exercice 3 Modulo 3, on voit que $3 \mid y$, puis que $3 \mid x$. En écrivant $y = 3y'$ et $x = 3x'$, on obtient $15x'^2 - 7y'^2 = 1$. On arrive alors à une contradiction modulo 3 car 2 n'est pas un carré modulo 3.

Solution de l'exercice 4 On a affaire à une puissance 5 connue ; on regarde donc modulo 11 : $n^5 + 7$ peut être congru 6, 7 ou 8 modulo 11, mais on vérifie qu'un carré n'est jamais congru à ces nombres modulo 11.

Solution de l'exercice 5 Regardons l'expression modulo 3 : $2^n + 12^n + 2014^n \equiv (-1)^n + 1 \mod 3$. Comme un carré n'est jamais congru à 2 modulo 3, on en déduit que n est impair. Regardons ensuite l'expression modulo 7 :

$$2^n + 12^n + 2014^n \equiv 2^n + (-2)^n + 5^n \equiv 5^n \mod 7$$

car n est impair. Lorsque n est impair, 5^n ne peut être congru qu'à 3, 5 ou 6 modulo 7. Or un carré est congru à $0, 1, 2$ ou 4 modulo 7. Il n'existe donc pas d'entiers $n \geq 1$ tels que $2^n + 12^n + 2014^n$ soit un carré parfait.

Solution de l'exercice 6 Nous allons montrer qu'il n'existe pas de tels rationnels x, y, z. On raisonne par l'absurde en supposant qu'il en existe. Soit d le plus petit dénominateur commun de x, y et z. On peut alors écrire $x = \frac{a}{d}$, $y = \frac{b}{d}$ et $z = \frac{c}{d}$ pour certains entiers a, b et c. L'équation que l'on cherche à résoudre devient alors :

$$a^5 + 2b^5 + 5c^5 = 11d^5.$$

Comme nous avons affaire à des puissances cinquièmes, il est judicieux d'étudier cette équation modulo 11. Une recherche exhaustive (ou l'utilisation du petit théorème de Fermat) montre qu'une puissance 5-ième est congrue à 0, 1 ou -1 modulo 11. On en déduit que la congruence $a^5 + 2b^5 + 5c^5 \equiv 0 \pmod{11}$ implique que a, b et c sont tous les trois multiples de 11. Ainsi, $a^5 + 2b^5 + 5c^5$ est divisible par 11^5, d'où on déduit que d est lui aussi divisible par 11. Les fractions $\frac{a}{d}$, $\frac{b}{d}$ et $\frac{c}{d}$ peuvent donc, toutes les trois, être simplifiées par 11. Ceci contredit la minimalité de d et termine la démonstration.

Solution de l'exercice 7

On a affaire à des puissances troisièmes et quatrièmes (exposants connus). D'après ce qu'on a vu, il est judicieux de considérer un nombre premier p congru à 1 modulo 3 et congru à 1 modulo 4, par exemple $p = 13$. On voit qu'effectivement, modulo 13, un cube est congru à $0, 1, 5, 8, 12$ et une puissance quatrième à $0, 1, 3, 9$. Or

$$19^{19} \equiv (6^{12}) \cdot 6^7 \equiv (6^2)^3 \cdot 6 \equiv (-3)^3 \cdot 6 \equiv 7 \mod 13.$$

Or il n'est pas possible de former un entier congru à 7 modulo 13 en additionnant un entier choisi dans $\{0, 1, 5, 8, 12\}$ avec un entier choisi dans $\{0, 1, 3, 9\}$. Ceci conclut.

Solution de l'exercice 8 On a affaire à des puissances 5 et 2 (exposants connus). D'après ce qu'on a vu, il est judicieux de considérer un nombre premier p congru à 1 modulo 5 et congru à 1 modulo 2, par exemple $p = 11$. On voit qu'effectivement, modulo 11, une puissance cinquième est congrue à $0, 1, 10$ et un carré à $0, 1, 3, 4, 5, 9$. Or il n'est pas possible de former un entier congru à 4 modulo 11 en soustrayant à un entier choisi dans $\{0, 1, 10\}$ un entier choisi dans $\{0, 1, 3, 4, 5, 9\}$. Ceci conclut.

Solution de l'exercice 9 Tout d'abord, $(a, y) = (1, 1)$ est solution. On suppose donc que $a, y \geq 2$. En regardant modulo 9 et en utilisant le fait que l'ordre de 7 modulo 9 vaut 3, on obtient que $y \equiv 0 \mod 3$. On cherche donc

p tel que l'ordre de 7 modulo p vaut 3. Dans ce cas, on doit avoir $p \mid 7^3 - 1$ et on voit que $p = 19$ convient. Ainsi, $3^{2a-1} + 3^a + 1 \equiv 1 \mod 19$. (Alternativement, on aurait pu direcement dire que comme 3 divise y, 19 divise $7^3 - 1$ qui divise $7^y - 1$).

Donc $19 \mid 3^{a-1} + 1$, donc $3^{a-1} \equiv 18 \mod 19$. Or l'ordre de 3 modulo 9 vaut 18. On en déduit que $a \equiv 10 \mod 18$.

On cherche donc ensuite p tel que l'ordre de 3 modulo p vaut 18 ou, pour simplifiser, divise 18 si possible. On trouve que $p = 7$ convient (l'ordre de 3 modulo 7 vaut 6). Modulo 7, on a donc $3^{19} + 3^{10} + 1 \equiv 0 \mod 7$, ce qui est absurde.

Solution de l'exercice 10 Supposons que $a^5b + 3$ et $ab^5 + 3$ soient tous les deux des cubes. D'après ce qu'on a vu, il est judicieux de considérer l'équation modulo 9. Tout d'abord, il est clair que 3 ne divise ni a, ni b. Or un cube non divisible par 3 est congru à 1 ou 8 modulo 9. Ainsi, a^5b et ab^5 sont congrus à 5 ou 7 modulo 9. Leur produit est donc congru à 4, 7 ou 8 modulo 9. Or $a^5b \cdot ab^5 = (ab)^6 \equiv 1 \mod 9$ d'après le théorème d'Euler. Absurde.

Solution de l'exercice 11

Il est clair que $(x, y) \neq (0, 0)$ et que $z \geq 1$. Tout d'abord $(x, y, z) = (1, 0, 2)$ est bien solution.

Si $y = 0$ (et $x \geq 1$), en regardant l'équation modulo 5, on trouve $z \equiv 2 \mod 4$. Si $y \geq 1$, en regardant modulo 7, on trouve que $z \equiv 4 \mod 6$. Dans tous les cas, z est pair. On écrit donc $z = 2n$.

Alors $5^x 7^y = (3^n - 2)(3^n + 2)$. Comme $3^n - 2$ et $3^n + 2$ sont premiers entre eux, deux cas de figure se présentent :

Cas 1 : $3^n - 2 = 5^x$ *et* $3^n + 2 = 7^y$. En regardant modulo 3 la deuxième équation, on voit qu'il n'y a pas de solutions.

Cas 2 : $3^n - 2 = 7^y$ *et* $3^n + 2 = 5^x$. Alors $4 = 5^x - 7^y$. Supposons par l'absurde que $x, y \geq 1$. En regardant modulo 7, on voit $x \equiv 2 \mod 6$ et donc que x est pair. En regardant modulo 5, on voit que $y \equiv 0 \mod 4$ et donc que y est pair. En écrivant $x = 2x'$ et $y = 2y'$, on a donc $4 = (5^{x'} - 7^{y'})(5^{x'} + 7^{y'})$, ce qui ne donne pas des solutions. On a donc $x = 0$ ou $y = 0$, et on retrouve la seule solution $(x, y, z) = (1, 0, 2)$.

Solution de l'exercice 12 On va montrer qu'il n'y a pas de solutions. Tout d'abord, il est clair que n est pair. Modulo 8, on voit que r est pair. Écrivons donc $r = 2s$. L'équations se réécrit alors $n^5 = (1221^s - 7^m)(1221^s + 7^m)$. Comme le PGCD de $1221^s - 7^m$ et de $1221^s + 7^m$ vaut 2, deux cas de figure se présentent.

Cas 1. $1221^s - 7^m = 2x^5$ et $1221^s + 7^m = 16y^5$ avec $x, y \geq 1$ entiers. Alors $1221^s = x^5 + 8y^5$ et $7^m = 8y^5 - x^5$. Comme on a affaire à des puissances 5-ièmes, il est judicieux de considérer l'équation modulo 11. Comme une puissance 5-ième est congrue 0, 1 ou -1 modulo 11, de $0 \equiv 1221^s \equiv x^5 + 8y^5 \mod 11$, on voit que 11 divise x et y, ce qui contredit le fait que $7^m = 8y^5 - x^5$.

Cas 2. $1221^s - 7^m = 16x^5$ et $1221^s + 7^m = 2y^5$ avec $x, y \geq 1$ entiers. Comme dans le premier cas, on trouve que $1221^s = 8x^5 + y^5$ et $7^m = y^5 - 8x^5$. Modulo 11, on trouve encore que 11 divise à la fois x et y, ce qui est absurde.

Solution de l'exercice 13 La quantité $1 - 8 \cdot 3^a + 2^{a+2}(2^a - 1)$ est égale à $(2^{a+1} - 1)^2 - 2^3 \cdot 3^a$. On remarque que c'est un carré pour $a = 3$ (elle vaut $9 = 3^2$) et $a = 5$ (elle vaut $2045 = 25^2$) mais pas pour $a \in \{1, 2, 4, 6, 7, 8\}$. On suppose dorénavant $a \geq 9$.

Supposons que $1 - 8 \cdot 3^a + 2^{a+2}(2^a - 1)$ soit un carré, c'est-à-dire, puisque cette quantité est impaire, qu'il existe un entier impair k tel que

$$(2^{a+1} - 1)^2 - 2^3 \cdot 3^a = (2k + 1)^2. \tag{1}$$

Ainsi

$$(2^{a+1} - 1)^2 - (2k + 1)^2 = 2^3 \cdot 3^a, \tag{2}$$

soit encore $(2^a - k - 1)(2^a + k) = 2 \cdot 3^a$. Il existe alors un entier $b \geq 0$ tel que l'une des deux situations suivantes se produit (en discutant selon la parité de k) :

Cas 1. On a $2^a + k = 2 \cdot 3^b$ et $2^a - k - 1 = 3^{a-b}$.

Cas 2. On a $2^a + k = 3^b$ et $2^a - k - 1 = 2 \cdot 3^{a-b}$.

Traitons d'abord le cas 1. On a $2k + 1 = 2 \cdot 3^b - 3^{a-b}$, et donc $b \geq a - b$. De plus, $2^{a+1} - 1 = 3^{a-b} + 2 \cdot 3^b$. Donc

$$2^{a+1} - 1 = 3^{a-b}(1 + 2 \cdot 3^{2b-a}).$$

Comme $a \geq 9$, on a $a - b \geq 3$, de sorte que 3^3 divise $2^{a+1} - 1$. Or l'ordre de 2 modulo 3^3 vaut 18. Donc $a \equiv 17 \mod 18$. Il est donc naturel de considérer l'équation modulo 19 car alors 2^{a+1} est constant modulo 19, et vaut 1 (alternativement, $19 \mid 2^{18} - 1 \mid 2^{a+1} - 1$). Donc

$$(2^{a+1} - 1)^2 - 2^3 \cdot 3^a \equiv (1-1)^2 - 2^3 \cdot 13 \equiv 10 \mod 19.$$

Alors, par (1), $(2k+1)^{18} \equiv 10^9 = 18 \mod 19$, ce qui contredit le petit théorème de Fermat.

Traitons le cas 2. On a $2k + 1 = 3^b - 2 \cdot 3^{a-b}$, et donc $b \geq a - b$. De plus, $2^{a+1} - 1 = 3^b + 2 \cdot 3^{a-b}$. Donc

$$2^{a+1} - 1 = 3^{a-b}(3^{2b-a} + 2),$$

et on conclut comme dans le premier cas.

Il n'y a donc pas de solution $a \geq 9$. En conclusion, les seules solutions sont 3 et 5.

Solution de l'exercice 14 Pour $x \leq 5, y \leq 3$, on trouve les solutions $(x, y) = (3, 1)$ et $(x, y) = (5, 3)$. On suppose donc $x \geq 6$ et $y \geq 4$.

Il est naturel de commencer par regarder modulo $3^4, 3^5, ..., 2^6, 2^7, ...$ On regarde modulo 2^6 : l'ordre de 3 modulo 64 vaut 16. On trouve donc que $y \equiv 11 \mod 16$. Pour rendre 3^y constant, il est naturel de regarder modulo $p = 17$, car alors $3^y + 5 \equiv 3^{11} + 5 \equiv 12 \mod 17$. Or on vérifie que les puissances de 2 ne valent jamais 12 modulo 17. Ceci montre qu'il n'y a pas d'autres solutions.

Solution de l'exercice 15 On vérifie qu'il n'y a qu'une seule solution pour $m \leq 2 : (m, n) = (2, 1)$. On suppose donc que $m \geq 3$ et $n \geq 2$. On applique la méthode de Dan Schwarz en réécrivant l'équation sous la forme

$$3^2(3^{m-2} - 1) = 7(7^{n-1} - 1).$$

Ainsi $3^2 \mid 7^{n-1} - 1$. Or l'ordre de 7 modulo 3^2 vaut 3. Donc $19 \mid 7^3 - 1 \mid 7^{n-1} - 1$, de sorte que $19 \mid 3^{m-2} - 1$.

Or l'ordre de 3 modulo 19 vaut 18. Donc $37 \mid 3^{18} - 1 \mid 3^{m-2} - 1$, de sorte que $37 \mid 7^{n-1} - 1$.

Or l'ordre de 7 modulo 37 vaut 9. Donc $3^3 \mid 7^9 - 1 \mid 7^{n-1} - 1$, de sorte que $3^3 \mid 3^2(3^{m-2} - 1)$. C'est absurde, il n'y a donc pas d'autres solutions.

Solution de l'exercice 16 Modulo 4, on voit que k est pair. Modulo 3, on voit que n est pair. Écrivons donc $k = 2p$ et $n = 2q$. Ainsi, $(5^q - m)(5^q + m) = 9^p$. Ccomme $5^q - m$ et $5^q + m$ sont premiers entre eux, on a $5^q + m = 9^v$ et $5^q - m = 9^u$ avec $v > u \geq 0$. Alors $2 \cdot 5^q = 9^v + 9^u$, ce qui force $u = 0$. Ainsi, $2 \cdot 5^q = 9^p + 1$.

Si $q = 0$, $p = 0$ donne une solution. On suppose donc $q > 0$. Modulo 5, on voit que p est impair. Écrivons donc $p = 2r + 1$, de sorte que $2 \cdot 5^q = 3^{4r+2} + 1$. La valeur $q = 1$ donne la solution $p = 1$. Supposons donc $q \geq 2$. Comme l'ordre de 3 modulo 25 vaut 20, on a $8 = 3^2 - 1 \mid 3^{20} - 1 \mid 3^{4r+2} - 1$, ce qui est absurde.

Les seules solutions sont donc $(n, k, m) = (0, 0, 0)$ et $(n, k, m) = (2, 2, 4)$.

Remarque. À partir de $2 \cdot 5^q = 9^p + 1$, on aurait pu invoquer le théorème de Zsigmondy qui implique, lorsque $p \geq 2$, l'existence d'un nombre premier s tel que s divise $9^p + 1$ mais pas $9 + 1$.

Solution de l'exercice 17 On va montrer que la seule solution est $(a, b, c, d) = (1, 2, 2, 1)$.

Modulo 4, on a $3^{c+d} \equiv 3 \mod 4$, ce qui implique $c + d$ est impair.

Modulo 3, on trouve que b est impair. Écrivons $b = 2n$ avec $n \geq 1$.

Modulo 8, en utilisant le fait que $c + d$ est impair et b est pair, on trouve que $4^a \equiv 4 \mod 8$, ce qui implique $a = 1$.

Ainsi, $3^c \cdot 11^d = 4 \cdot 5^{2n} - 1$, ou encore $(2 \cdot 5^n - 1)(2 \cdot 5^n + 1) = 3^c \cdot 11^d$. Comme $2 \cdot 5^n - 1$ et $2 \cdot 5^n + 1$ sont premiers entre eux, deux cas de figure se présentent.

Cas 1. $2 \cdot 5^n - 1 = 3^c$ et $2 \cdot 5^n + 1 = 11^d$. Le cas $n = 1$ donne la solution $c = 2$ et $d = 1$. On suppose donc $n \geq 2$ et $d \geq 2$. L'ordre de 11 modulo 25 vaut 5, donc $3 \mid 11^{20} - 1 \mid 11^d - 1 = 2 \cdot 5^n$, ce qui est absurde.

Cas 2. $2 \cdot 5^n - 1 = 11^d$ et $2 \cdot 5^n + 1 = 3^c$. Le cas $n = 1$ ne donne pas de solutions, on suppose donc $n \geq 1$ et $c \geq 1$. L'ordre de 3 modulo 25 vaut 20, donc $3^2 - 1 \mid 3^{20} - 1 \mid 3^c - 1 = 2 \cdot 5^n$, ce qui est absurde.

Solution de l'exercice 18

Tout d'abord $(x, y) = (1, 1)$ est une solution, et il n'y a pas de solution pour $y = 2$. On suppose donc $y \geq 3$ par la suite.

Première solution. Réécrivons l'équation en utilisant la méthode de Dan Scwharz :

$$7(7^{x-1}-1) = 3(3^{y-1}-1).$$

L'ordre de 3 modulo 7 vaut 6. Donc $13 \mid 3^6 - 1 \mid 3^{y-1} - 1$, de sorte que $13 \mid 7^{x-1} - 1$.
Or l'ordre de 7 modulo 13 vaut 12. Donc $3^2 \mid 7^{12} - 1 \mid 7^{x-1} - 1$. Donc 3^2 divise $3(3^{y-1} - 1)$, absurde.

Deuxième solution. On a affaire à des puissances 7^x et 3^y inconnues. D'après ce qu'on a vu, il est judicieux de travailler modulo $7, 7^2, ..., 3, 3^2, ...$

En regardant modulo 7, on voit que y est impair. Puis, en regardant modulo 4, on voit que x est impair. Ensuite, modulo 5, on voit que x et y sont congrus à 1 modulo 4. Modulo 9, on trouve que x est congru à 2 modulo 3. D'après le théorème chinois, on en déduit que x est congru à 5 modulo 12. Donc, comme $7^{12} \equiv 1 \mod 13$, on en déduit que 7^x est congru à 11 modulo 13. Or, comme $y \equiv 1 \mod 4$, 3^y est congru à 1, 3 ou 9 modulo 13. Contradiction.

Troisième solution. Modulo 27, on a $7^x \equiv 4 \mod 27$. Or l'ordre de 7 modulo 27, noté ω, vaut 9. En effet, 27 divise $7^{18} - 1$ d'après le petit théorème de Fermat, de sorte ω divise 18. On vérifie que 27 ne divise pas $7^9 + 1$. Ainsi ω divise 9 et on vérifie que $\omega = 9$. Comme $7^8 \equiv 4 \mod 27$, on trouve que $x \equiv 8 \mod 9$.

Ainsi, x est constant modulo 9. D'après ce qu'on a vu, il peut être judicieux de trouver N tel que l'ordre de 7 modulo N soit 9. On a

$$7^9 - 1 = (7^3 - 1)(7^6 + 7^3 + 1) = (2 \cdot 3^2 \cdot 19) \cdot (3 \cdot 37 \cdot 1063).$$

On prend donc $N = 37$. Comme 37 ne divise pas $7^3 - 1$, l'ordre de 7 modulo 37 vaut bien 9. Ainsi, $7^x \equiv 7^8 \equiv 12 \mod 37$.

En regardant modulo 8, on voit que y est impair. Or 3^{2k+1} peut être congru à $3, 27, 21, 4, 36, 28, 30, 11$ ou 25 modulo 37, mais pas à 12. Ceci conclut.

<u>*Solution de l'exercice 19*</u> Tout d'abord, $(x, y) = (0, 5)$ et $(x, y) = (1, 6)$ sont solutions. On suppose donc que $x \geq 2$ et $y \geq 7$. On applique la méthode de Dan Schwarz en réécrivant l'équation

$$3 \cdot 11(3^{x-1} - 1) = 2^6(2^{y-6} - 1).$$

Donc $2^6 \mid 3^{x-1} - 1$. Or l'ordre de 3 modulo 2^6 vaut 16. Donc $3^{16} - 1 \mid 3^{x-1} - 1$. Donc $193 \mid 3^{16} - 1 \mid 2^{y-6} - 1$. Mais l'ordre de 2 modulo 193 vaut 96, donc $3^2 \mid 2^{96} - 1 \mid 2^{y-6} - 1$. Donc $3^2 \mid 3 \cdot 11(3^{x-1} - 1)$, ce qui force $x = 1$ et conclut.

<u>*Solution de l'exercice 20*</u> On vérifie tout d'abord que pour $x \leq 4$, seul $x = 3$ donne la solution $y = 1$. On suppose donc que $x \geq 5$ dans la suite.

Première solution. Appliquons la méthode Dan Schwarz en réécrivant l'équation sous la forme

$$2^3(2^{x-3} - 1) = 11 \cdot (11^{y-1} - 1).$$

Donc 11 divise $2^{x-3} - 1$. Or l'ordre de 2 modulo 11 vaut 10. Donc $13 \mid 2^{10} - 1 \mid 2^{x-3} - 1$, de sorte que $13 \mid 11^{y-1} - 1$.
Or l'ordre de 11 modulo 13 vaut 12. Donc $2^4 \mid 11^{12} - 1 \mid 11^{y-1} - 1$. Donc $2^4 \mid 2^3 \cdot (2^{x-3} - 1)$, ce qui est absurde.

Deuxième solution. Considérons l'équation modulo $2^5 = 32$. On a $11^y \equiv 3 \mod 32$. On vérifie que $11^7 \equiv 3 \mod 32$ et que l'ordre de 11 modulo 32 vaut 8. Ainsi, $y \equiv 7 \mod 8$.

Considérons l'équation modulo 11. On a $2^x \equiv 8 \mod 11$. On vérifie que l'ordre de 2 modulo 11 vaut 10, de sorte que $x \equiv 3 \mod 10$.

D'après ce qu'on a vu, il est judicieux de considérer l'équation modulo un nombre premier p tel que l'ordre de 11 modulo p vaut (ou divise) 8. Or

$$11^8 - 1 = (11^4 + 1)(11^2 + 1)(11 - 1)(11 + 1) = (2 \cdot 7321) \cdot (2 \cdot 61) \cdot (2 \cdot 5) \cdot (2^2 \cdot 3).$$

Prenons donc $p = 61$. L'ordre de 11 modulo 61 vaut alors 4, et $11^y \equiv 50 \mod 61$.

Or 2^x est de la forme $8 \cdot 2^{10k} \equiv 8 \cdot 48^k \mod 61$. Supposons qu'il existe un entier $k \geq 1$ tel que $8 \cdot 48^k \equiv 50 \mod 61$, ou encore, comme 23 est l'inverse de 8 modulo 61, que $48^k \equiv 52 \mod 61$. Or les puissances de 48 ne valent que $48, 47, 60, 14, 14$ et 1 modulo 61. Ceci conclut.

Troisième solution. En commencçant comme dans la deuxième solution, on aurait pu ensuite essayer de considérer l'équation modulo un nombre premier p tel que l'ordre de 11 modulo p est un multiple de 8. Pour cela, on remarque que 17 divise $11^8 + 1$, de sorte que l'ordre de 11 modulo 17 vaut 16. On vérifie que modulo 17 on obtient bien une contradiction.

Solution de l'exercice 21 Tout d'abord, $(x, y) = (4, 1)$ est solution. On suppose que $y \geq 2, x \geq 4$. On applique la méthode de Dan Schwarz en réécrivant l'équation

$$2^4(2^{x-4} - 1) = 11(11^{y-1} - 1).$$

Donc $2^4 \mid 11^{y-1} - 1$. Or l'ordre de 11 modulo 2^4 vaut 4. Donc $61 \mid 11^4 - 1 \mid 11^{y-1} - 1$, de sorte que $61 \mid 2^{x-4} - 1$. Mais l'ordre multiplicatif de 11 modulo 2^4 vaut 4. Donc $61 \mid 11^4 - 1 \mid 11^{y-1} - 1$. Or l'ordre de 2 modulo 61 vaut 60, donc $41 \mid 2^{60} - 1 \mid 2^{x-4} - 1$, de sorte que $41 \mid 11^{y-1} - 1$. Or l'ordre multiplicatif de 11 modulo 41 vaut 40, on a $2^5 \mid 11^{40} - 1 \mid 11^{y-1} - 1$, de sorte que $2^5 \mid 2^4(2^{x-4} - 1)$. Ceci est absurde et montre qu'il n'y a pas d'autres solutions.