Exercices sur l'ordre en arithmétique

Igor Kortchemski

N.B. Certains exercices utilisent le théorème "Lifting the exponent" (LTE).

- Rappels de cours -

On considère $a \in \mathbb{Z}$ et $n \geq 1$ des entiers premiers entre eux. L'ordre de a modulo n est le le plus petit entier non nul, noté $\omega_n(a)$, tel que $a^{\omega_n(a)} \equiv 1 \pmod{n}$. On utilisera les résultats suivants :

– Si $k \geq 1$ est un entier vérifiant $a^k \equiv 1 \pmod{n}$, alors $\omega_n(a)$ divise k.
– Si ϕ désigne la fonction indicatrice d'Euler, on rappelle que $\phi(n)$ est le nombre d'entiers, compris au sens large entre 1 et $n-1$, premiers avec n, que $\phi(ab) = \phi(a)\phi(b)$ lorsque a et b sont des entiers premiers entre eux, et que $a^{\phi(n)} \equiv 1 \pmod{n}$ (théorème d'Euler). En particulier, $\omega_n(a)$ divise $\phi(n)$ (ce qui, dans le cas où $n = p$ est premier, donne $\omega_p(a) \mid p-1$). Ceci est en particulier utile lorsqu'on veut cherche l'ordre d'un entier modulo n à la main : il suffit de tester les diviseurs de $\phi(n)$.

- Exercices -

Exercice 1 Trouver tous les entiers $n \geq 1$ tels que n divise $2^n - 1$.

Exercice 2 Trouver tous les entiers $n \geq 1$ impairs tels que n divise $3^n + 1$.

Exercice 3 Existe-t-il des entiers $n \geq 1$ tels que 9 divise $7^n + n^3$?

Exercice 4 Soit p un nombre premier. Montrer que tout diviseur premier de $2^p - 1$ est strictement plus grand que p.

Exercice 5 Soient p, q, r des nombres premiers tels que p soit impair et divise $q^r + 1$. Montrer que $2r$ divise $p-1$ ou p divise $q^2 - 1$.

Exercice 6 Trouver tous les entiers $m, n \geq 1$ tels que mn divise $3^m + 1$ et mn divise $3^n + 1$.

Exercice 7 Soient p, q deux nombres premiers tels que q divise $3^p - 2^p$. Montrer que p divise $q-1$.

Exercice 8 (Olympiade Chine 2006) Trouver les entiers $a, n \geq 1$ tels que n divise $((a+1)^n - a^n)$.

Exercice 9 Soient $a, b > 1$ impairs tels que $a + b = 2^\alpha$ avec $\alpha \geq 1$. Montrer qu'il n'y a pas d'entiers $k > 1$ tels que k^2 divise $a^k + b^k$.

Exercice 10 Trouver tous les entiers n tels que 19 divise $2^{3n+4} + 3^{2n+1}$.

Exercice 11 Soient a, b, n des nombres entiers strictement positifs avec $a > b$. Montrer que n divise $\phi(a^n - b^n)$.

Exercice 12 Soient $n, k \geq 2$ des entiers tels que n divise $k^n - 1$. Peut-on avoir $\mathrm{PGCD}(n, k-1) = 1$?

Exercice 13 Soient x et y deux entiers positifs premiers entre eux. Si k est un entier impair positif qui divise $x^{2^n} + y^{2^n}$ avec $n \geq 1$, alors il existe un entier m tel que $k = 2^{n+1}m + 1$.

Exercice 14 Trouver tous les p, q premiers tels que pq divise $2^p + 2^q$.

Exercice 15 (Olympiade Irlande 1996) Soient p un nombre premier et a, n des entiers strictement positifs. Prouver que si $2^p + 3^p = a^n$, alors nécessairement $n = 1$.

Exercice 16 Soit $n > 1$ un entier impair. Si $m \geq 1$ est un entier, montrer que n ne divise pas $m^{n-1} + 1$.

Exercice 17 (Olympiades Internationales de Mathématiques 1990) Trouver tous les entiers $n \geq 1$ tels que n^2 divise $2^n + 1$.

Exercice 18 (Olympiade Bulgarie 1997) Pour un entier $n \geq 2$, $3^n - 2^n$ est une puissance d'un nombre premier. Montrer que n est premier.

Exercice 19 (Olympiade États-Unis 2003) Trouver tous les nombres premiers p, q, r tels que p divise $1 + q^r$, q divise $1 + r^p$ et r divise $1 + p^q$.

Exercice 20 Trouver tous les entiers $a, b, c > 1$ deux à deux premiers entre eux tels que

$$b \mid 2^a + 1, \qquad c \mid 2^b + 1, \qquad a \mid 2^c + 1.$$

- Solutions -

<u>*Solution de l'exercice 1*</u> Soit $n > 1$ tel que n divise $2^n - 1$. Il est clair que n est impair. Soit p le plus petit facteur premier de n, qui est donc impair. Alors $2^n \equiv 1 \pmod{p}$. Soit ω l'ordre de 2 modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \pmod{p}$. Ainsi ω divise $p-1$. D'après la condition sur p, on a nécessairement $\omega = 1$. Alors $2 \equiv 1 \pmod{p}$, ce qui est absurde. On a donc $n = 1$.

<u>*Solution de l'exercice 2*</u> Soit $n > 1$ tel que n divise $3^n + 1$. Soit p le plus petit facteur premier de n, qui est donc impair, de sorte que $p > 3$. Alors $3^{2n} \equiv 1 \pmod{p}$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \pmod{p}$. Ainsi ω divise $p-1$. On en déduit que ω divise $\mathrm{PGCD}(2n, p-1)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas, $3 \equiv 1 \pmod{p}$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1 \pmod{p}$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

<u>*Solution de l'exercice 3*</u> Soit q un diviseur premier de $2^p - 1$. Soit ω l'ordre de 2 modulo q. Alors ω divise p, de sorte que $\omega = 1$ ou $\omega = p$. Dans le premier cas, on aurait $2 \equiv 1 \mod q$, absurde. Donc $\omega = p$. Or, d'après le petit théorème de Fermat, $2^{q-1} \equiv 1 \mod q$. Donc p divise $q-1$, de sorte que $q - 1 \geq p$, ce qui implique que $q > p$.

<u>*Solution de l'exercice 4*</u> Comme p divise $q^r + 1$, il divise également $q^{2r} - 1$. Ainsi, en notant ω l'ordre de q modulo p, on a $\omega \mid 2r$. Comme p est impair, il ne peut pas diviser $q^r - 1$. Ainsi $\omega \in \{1, 2, 2r\}$.

Cas 1 : $\omega = 1$. Dans ce cas, p divise $q-1$, et donc p divise bien $q^2 - 1$.

Cas 2 : $\omega = 2$. Dans ce cas, p divise $q^2 - 1$.

Cas 3 : $\omega = 2r$. Dans ce cas, d'après le petit théorème de Fermat, $q^{p-1} \equiv 1 \mod p$, et donc $2r$ divise $p-1$.

Ceci conclut.

<u>*Solution de l'exercice 5*</u> Soit $n \geq 1$ tel que 9 divise $7^n + n^3$. Comme un cube est congru à $0, -1$ ou 1 modulo 9, on en déduit que $n^6 \equiv 1 \bmod 9$ et donc que $7^{2n} \equiv 1 \pmod{9}$. Or l'ordre de 7 modulo 9 est 3. On en déduit que 3 divise $2n$. Ainsi 3 divise n. Il faudrait donc que 3 divise 7^n, ce qui est absurde. Il n'y a donc pas de tels entiers.

<u>*Solution de l'exercice 6*</u> On suppose $m, n \geq 2$. Soit p le plus petit diviseur de n. Alors $3^{2n} \equiv 1 \bmod p$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \pmod{p}$. Ainsi ω divise $p-1$. On en déduit que ω divise $\mathrm{PGCD}(p-1, 2n)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas, $3 \equiv 1 \pmod{p}$ et donc $p = 2$. Dans le deuxième cas, $3^2 \equiv 1 \pmod{p}$ et donc $p = 2$. On en déduit que n est pair. On montre de même que m est pair. Alors 4 divise $3^m + 1$, ce qui n'est pas possible car m est pair.

Il reste à examiner le cas où m ou n vaut 1 et il vient que les solutions sont $(1,1)$, $(1,2)$ et $(2,1)$.

<u>*Solution de l'exercice 7*</u> Il est clair que $q \geq 5$. Notons ω l'ordre $3/2$ modulo q (ici, et similairement dans la suite, $1/2$ désigne l'inverse de 2 modulo q). Alors ω divise p, donc $\omega = 1$ ou p. Le premier cas n'étant pas possible, on a donc $\omega = p$. Or d'après le petit théorème de Fermat, $(3/2)^{q-1} \equiv 1 \pmod{q}$. On en tire que ω divise $q-1$, d'où le résultat.

<u>*Solution de l'exercice 8*</u> Supposons que $n \geq 2$. Soit p le plus petit facteur premier de n. Alors p divise $(a+1)^n - a^n$. En d'autres termes, $((a+1)/a)^n \equiv 1 \pmod{p}$. Soit ω l'ordre de $(a+1)/a$ modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $((a+1)/a)^{p-1} \equiv 1 \pmod{p}$ de sorte que ω divise $p-1$. D'après la condition sur p, nécessairement $\omega = 1$. Ceci implique $a + 1 \equiv a \pmod{p}$, ce qui est absurde.

Les solutions sont donc $n = 1$ et a quelconque.

<u>*Solution de l'exercice 9*</u> Raisonnons par l'absurde et considérons un entier $k > 1$ tel que k^2 divise $a^k + b^k$. En raisonnant modulo 4 on voit que k est impair. Comme $a + b$ est une puissance de 2, il en découle que a et b sont premiers entre eux. Soit p le plus petit facteur premier de k qui est donc différent de 2 et ne divise ni a, ni b.

Soit ω l'ordre de $-a/b$ modulo p. Comme $a^k + b^k \equiv 0 \pmod{p}$, on a $(a/b)^k \equiv -1 \pmod{p}$, soit, puisque k est impair, $(-a/b)^k \equiv 1 \pmod{p}$. Ainsi, ω divise k, mais aussi $p-1$ d'après le petit théorème de Fermat. Par définition de p, k et $p-1$ sont premiers entre eux. Donc $\omega = 1$. Ainsi, $a + b \equiv 0 \pmod{p}$, ce qui est absurde et conclut la solution.

Solution de l'exercice 10 Les conditions de l'énoncé impliquent que $9^n \equiv 8^n \pmod{19}$. Mais l'inverse de 8 modulo 19 est 12. On en déduit que $13^n \equiv 108^n \equiv (9 \times 8)^n \equiv 1 \pmod{19}$. Or 13 est racine primitive modulo 19. Les entiers recherchés sont donc les multiples de 18.

Solution de l'exercice 11 Traitons d'abord le cas où a et b sont premiers entre eux. Alors a et b sont premiers avec $a^n - b^n$ et il est clair que l'ordre de a/b modulo $a^n - b^n$ est n. On en déduit que n divise $\phi(a^n - b^n)$.

Si $d > 1$ est le PGCD de a et de b, notons $u = a/d$ et $v = b/d$ de sorte que u et v sont premiers entre eux. D'après ce qui précède, n divise $\phi(u^n - v^n)$. En utilisant la formule exprimant $\phi(N)$ en fonction des facteurs premiers de N, on voit que $\phi(u^n - v^n)$ divise $\phi(d^n(u^n - v^n)) = \phi(a^n - b^n)$, ce qui conclut.

Solution de l'exercice 12 Soit p le plus petit facteur premier de n. Modulo p, l'ordre de k divise n puisque $k^n \equiv 1 \pmod{p}$. Par ailleurs, d'après le théorème de Fermat, l'ordre de k modulo p divise $p-1$. Or p est le plus petit facteur premier de n : le seul diviseur de n strictement inférieur à p est 1. L'ordre de p, diviseur de n inférieur ou égal à $p-1$, vaut donc nécessairement 1, ce qui prouve précisément que $k \equiv 1 \pmod{p}$, donc que p divise $k-1$, de sorte que $\mathrm{PGCD}(n, k-1)$ vaut au moins p. La réponse est donc non.

Solution de l'exercice 13 k n'est pas supposé premier, mais si tous ses facteurs premiers vérifient le résultat, alors un produit de nombres congrus à $1 \pmod{2^{n+1}}$ sera lui-même $\equiv 1 \pmod{2^{n+1}}$. Il suffit donc de démontrer que tout facteur premier p de $x^{2^n} + y^{2^n}$ vérifie $p \equiv 1 \pmod{2^{n+1}}$. Par ailleurs, si p divisait x, comme par hypothèse il divise $x^{2^n} + y^{2^n}$, il diviserait également y : x et y ne seraient pas premiers entre eux. Donc x et p sont premiers entre eux, et y et p sont premiers entre eux. Notons $1/x$ l'inverse de x modulo p, de sorte que $x^{2^n} + y^{2^n} \equiv x^{2^n}\left(1 + (y/x)^{2^n}\right) \equiv 0 \pmod{p}$ équivaut à : $(y/x)^{2^n} \equiv -1 \pmod{p}$. Donc cet élément y/x a pour ordre 2^{n+1}, car 2^{n+1} est la première puissance de 2 vérifiant $(y/x)^{2^k} \equiv 1 \pmod{p}$, et 2^{n+1} n'a pas d'autre diviseur que des puissances de 2. Comme $(y/x)^{p-1} \equiv 1 \pmod{p}$, 2^{n+1} divise $p-1$, ce qui est précisément le résultat cherché. Un cas particulier important : pour $n = 1$, tout diviseur d'une somme de deux carrés premiers entre eux est congru à 1 modulo 4.

Solution de l'exercice 14 Remarquons tout d'abord que si $p = 2$, $2q$ divise $4 + 2^q$ si et seulement si soit $q = 2$, soit $2q$ divise 6, puisque pour tout q impair q divise $2^{q-1} - 1$, donc $2q$ divise $2^q - 2$. D'où les solutions : $(p, q) = (2, 2), (2, 3)$ ou $(3, 2)$. On supposera désormais p et q impairs. Appelons ω_p et ω_q les ordres de 2 modulo p et q respectivement. Si p divise $2^p + 2^q$, donc $2^{p-1} + 2^{q-1}$, comme p divise $2^{p-1} - 1$, p divise $2^{q-1} + 1$, donc $2^{2(q-1)} - 1$. Dès lors, ω_p divise $p-1$ et $2(q-1)$ mais ne divise pas $q-1$. Si la plus grande puissance de 2 divisant ω_p (resp ω_q) est 2^{v_p} (resp 2^{v_q}), le fait que ω_p divise $2(q-1)$ et pas $q-1$ entraîne que $v_p > v_q$, car $q-1$ est divisible par ω_q donc par 2^{v_q} et pas par 2^{v_p}. Le même raisonnement, en échangeant p et q, aboutit à $v_q > v_p$, ce qui est manifestement incompatible. Il n'existe donc pas de couples de nombres premiers impairs vérifiant cette condition.

Solution de l'exercice 15 Si $p = 2$, $2^2 + 3^2 = 13$ vérifie bien la relation demandée : ce n'est pas une puissance ≥ 2 d'un entier. Si maintenant p est impair, $2^p + 3^p$ est divisible par $2 + 3 = 5$, et n'est divisible par 25 que si p est divisible par 5 donc, puisque par hypothèse p est premier, si $p = 5$. En effet, $3^p = (5-2)^p \equiv (-2)^p + p.5(-2)^{p-1} \pmod{25}$. C'est aussi une conséquence du théorème LTE. On en déduit que, hormis éventuellement pour $p = 5$, le facteur 5 apparaît avec l'exposant 1, ce qui suffit à démontrer le résultat cherché. Pour $p = 5$, il apparaît bien avec l'exposant 2, mais $3^5 + 2^5 = 275$ n'est pas une puissance ≥ 2 d'un entier, ce qui achève la démonstration.

Solution de l'exercice 16 C'est une conséquence presque immédiate de l'exercice 13. Soit 2^k la plus grande puissance de 2 divisant $n-1$: posons $n - 1 = 2^k q$, $s = m^{n-1} + 1 = x^{2^k} + y^{2^k}$ avec $x = m^q$ et $y = 1$. D'après l'exercice 13, tout diviseur de s est donc congru à 1 modulo 2^{k+1}. Or par définition de 2^k, n n'est pas congru à 1 modulo 2^{k+1}. Donc n ne divise pas s.

Solution de l'exercice 17 Les nombres entiers 1 et 3 sont solutions. Montrons qu'il n'y en a pas d'autres. Il est clair que n est impair. Ensuite, en considérant p le plus petit facteur premier de n et ω, l'ordre de 2 modulo p, on voit que ω divise à la fois $2n$ et $p-1$. Par définition de p, le PGCD de ces deux entiers vaut 2. Donc $2^2 \equiv 1 \pmod{p}$. Donc $p = 3$. Écrivons $n = 3u$, avec $u \geq 2$ et appliquons le théorème LTE (n est impair) : $2v_3(n) \leq v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = 1 + v_3(n)$. Donc $v_3(n) = 1$ et 3 ne divise pas u. Soit maintenant q le plus petit diviseur premier de u. Alors $q \mid 8^u + 1$. Donc, en notant ω' l'ordre de 8 modulo q, comme précédemment, ω' divise le

PGCD de $2u$ et $q-1$, qui vaut 2. Donc q divise 63, soit $q=7$. Finalement, écrivons $n=21r$, avec $r \geq 1$. Alors $7 \mid 2^{21r}+1 \equiv 2 \pmod 7$, ce qui est absurde.

<u>*Solution de l'exercice 18*</u> On suppose $n>2$ et que $3^n-2^n=p^k$ pour $k \geq 1$. Montrons d'abord que n est impair. Si $n=2n'$, alors $3^n-2^n=(3^{n'}-2^{n'})(3^{n'}+2^{n'})$. Il existe donc $\alpha > \beta \geq 0$ tels que : $3^{n'}+2^{n'}=p^\alpha$ et $3^{n'}-2^{n'}=p^\beta$. Alors $2^{n'+1}=p^\beta(p^{\alpha-\beta}-1)$. Donc $p=2$, ce qui est absurde, ou $\beta=0$ qui conduit à $n=2$, exclu. Ainsi n est impair.

Raisonnons par l'absurde et considérons q est un nombre premier divisant n avec $q<n$. Écrivons $n=qr$. Un raisonnement direct montre que 3^q-2^q est une puissance de p, disons $3^q-2^q=p^{k'}$ avec $k'<k$. En appliquant LTE, on voit que $v_p(r)=k-k'$. Écrivons donc $r=p^{k-k'}u$ avec p ne divisant pas u. Alors :

$$\begin{aligned} p^k &= 3^n-2^n = 3^{qp^{k-k'}u}-2^{qp^{k-k'}u} = (3^q)^{p^{k-k'}u}-(2^q)^{p^{k-k'}u} \\ &= (p^{k'}+2^q)^{p^{k-k'}u}-(2^q)^{p^{k-k'}u} \geq p^{k-k'}u\cdot p^{k'}\cdot 2^{q(p^{k-k'}u-1)} = p^k u\cdot 2^{q(p^{k-k'}u-1)} > p^k, \end{aligned}$$

ce qui est absurde : n est donc premier.

<u>*Solution de l'exercice 19*</u> On commence par examiner la condition « p divise $1+q^r$ ». Elle se récrit $q^r \equiv -1 \pmod p$ et implique donc, en particulier, $q^{2r} \equiv 1 \pmod p$. Ainsi l'ordre de q modulo p est un diviseur de $2r$. Comme r est supposé premier, c'est donc un élément de l'ensemble $\{1,2,r,2r\}$. Si on suppose en outre que $p \neq 2$, on a $q^r \not\equiv 1 \pmod p$, et donc l'ordre de q modulo p est nécessairement 2 ou $2r$. Dans le premier cas, en utilisant que p est premier, on obtient $q \equiv -1 \pmod p$, alors que dans le deuxième cas, on en déduit que $2r$ divise $p-1$. En permutant les nombres p,q et r, on obtient bien sûr des conséquences analogues des deux autres conditions « q divise $1+r^p$ » et « r divise $1+p^q$ ».

On suppose maintenant que p,q et r sont tous les trois impairs, et pour commencer que l'on est dans le cas où $q \equiv -1 \pmod p$. Le nombre premier p ne peut donc pas diviser $q-1$ (puisqu'il divise déjà $q+1$ et qu'il ne vaut pas 2). D'après les résultats du premier alinéa, la condition « q divise $1+r^p$ » implique donc que $r \equiv -1 \pmod q$. En appliquant à nouveau le même argument, on trouve que $p \equiv -1 \pmod r$. Or les trois congruences précédentes ne sont pas compatibles. En effet, par exemple, elles impliquent $q \geq p-1$, $r \geq q-1$ et $p \geq r-1$, ce qui ne peut se produire, étant donné que p,q et r sont des nombres premiers impairs, que si $p=q=r$; on a alors manifestement $q \not\equiv -1 \pmod p$. On en déduit que, toujours dans le cas où p,q et r sont supposés impairs, $2r$ divise $p-1$. En permutant circulairement les variables, on démontre de même que $2p$ divise $q-1$ et $2q$ divise $r-1$. Ainsi $8pqr$ divise $(p-1)(q-1)(r-1)$, ce qui n'est pas possible étant donné que $8pqr > (p-1)(q-1)(r-1)$. Finalement, il n'y a pas de solution lorsque p,q et r sont tous les trois impairs.

On en vient à présent au cas où l'un de ces trois nombres est égal à 2. Quitte à permuter circulairement à nouveau p,q et r, on peut supposer que c'est p. Les conditions de l'énoncé disent alors que q est impair, que $\mathrm{r}^2 \equiv -1 \pmod q$ et que $2^q \equiv -1 \pmod r$. Selon ce qui a été fait dans le premier alinéa, cette dernière congruence entraîne que $r=3$ ou que $2q$ divise $r-1$. Le premier cas conduit à $9 \equiv -1 \pmod q$, ce qui ne se produit que si $q=5$ puisque l'on a déjà écarté le cas $q=2$. On vérifie par ailleurs que le triplet $(2,5,3)$ est bien solution. Dans le second cas, le produit $2q$ divise $r-1$, mais aussi $2(r^2+1)$ puisqu'on sait que $r^2 \equiv -1 \pmod q$. Ainsi $2q$ divise $2(r^2+1)-2(r+1)(r-1)=4$, ce qui ne peut arriver.

En conclusion, il y a exactement trois solutions qui sont les triplets $(2,5,3)$, $(5,3,2)$ et $(3,2,5)$.

<u>*Solution de l'exercice 20*</u> Nous allons montrer qu'il n'y a pas de solution. Par l'absurde, soit (a,b,c) une solution. Tout d'abord, on remarque que a,b,c sont impairs. Pour un entier a, on notera $\pi(a)$ le plus petit nombre premier divisant a. On commence par prouver le petit lemme utile suivant :

Lemme. Si p est un nombre premier divisant 2^k+1 et $p<\pi(k)$, alors $p=3$.

Pour voir cela, il suffit, en notant w l'ordre de 2 modulo p, de voir que w divise à la fois $2k$ et $p-1$, ce qui impose $p=3$.

Revenons au problème. Par symétrie, on peut supposer que $\pi(a)<\pi(b),\pi(x)$. Comme $\pi(a)$ divise 2^c+1, le lemme implique que $\pi(a)=3$. Écrivons ainsi $a=3a_0$.

Montrons que 3 ne divise pas a_0. Dans le cas contraire, 9 diviserait 2^c+1, et donc $2^{2c}-1$. Or 9 divise 2^n-1 ssi 6 divise n. Donc 6 divise c, ce qui contredit le fait que a et c sont premiers entre eux.

Soit maintenant $q=\pi(a_0bc)$ et montrons que q divise b. Si q divise a_0 (et donc a), alors $\pi(q)<c$ (car a et c sont premiers entre eux), et de plus q divise 2^c+1. Donc $q=3$, absurde. De même, q ne divise pas c. En conclusion, q divise b.

Finalement, notons e l'ordre de 2 modulo q, de sorte que e divise $q-1$ et $2a$. Or les seuls facteurs premiers de $2a$ plus petits que q sont 2 et 3, donc e divise 6. Donc q divise $2^6 - 1 = 9 \cdot 7$, ce qui force $q = 7$. Mais alors

$$2^a + 1 \equiv (2^3)^{a_0} + 1 \equiv 2 \pmod 7.$$

Donc q ne divise $2^a + 1$, en contradiction avec le fait que q divise b qui divise $2^a + 1$.