

le second est une puissance de 2, donc ils sont premiers entre eux.

d) Le nombre 2^n a $n + 1$ chiffres binaires et $2^n - 1$ en a n ; donc d_1 a 241 chiffres binaires et d_2 en a 120. Bien entendu $d_3 = 1$ en a un seul.

Comme $2^{10} = 1024$ est proche de 10^3 , le nombre $2^{240} = (2^{10})^{24}$ est approximativement $(10^3)^{24}$, donc a environ 73 chiffres décimaux. *Le nombre exact de chiffres décimaux de d_1 est l'entier n tel que $10^{n-1} \leq 2^{240} < 10^n$, comme*

$$240 \cdot \frac{\log 2}{\log 10} = 72,24\dots$$

le nombre de chiffres de d_1 en base dix est en fait 73.

De même d_2 , qui est proche de $(10^3)^{12}$, a environ 37 chiffres décimaux; *en fait*

$$120 \cdot \frac{\log 2}{\log 10} = 36,12\dots$$

et le nombre de chiffres décimaux de d_2 est précisément 37.

Pour $n \geq 1$ le dernier chiffre décimal de 2^n est 2, 4, 8 ou 6 selon que $n \equiv 1, 2, 3$ ou $0 \pmod{4}$. Comme 240 et 120 sont multiples de 4, le dernier chiffre décimal de d_1 est 6 et celui de d_2 est 5. Celui de d_3 est 1.

6. Pour chacun des quatre nombres premiers 37, 41, 43, 47,

- 1 et 4 sont résidus quadratiques puisque ce sont des carrés dans \mathbf{Z} ,
- -1 est résidu quadratique quand p est congru à 1 modulo 4, donc pour 37 et 41, et il est non-résidu pour les deux autres.
- 2 est résidu quadratique quand p est congru à 1 ou 3 modulo 8, donc pour 41 et 47, et il est non-résidu pour les deux autres.
- Par multiplicativité du symbole de Legendre, -2 est résidu quadratique quand p est congru à 1 ou 3 modulo 8, donc pour 41 et 43, il est non-résidu pour les deux autres.

Le tableau est

	$41 \equiv 1$	$43 \equiv 3$	$37 \equiv 5$	$47 \equiv 7$	(mod 8)
$\left(\frac{-1}{p}\right)$	1	-1	1	-1	
$\left(\frac{2}{p}\right)$	1	-1	-1	1	
$\left(\frac{-2}{p}\right)$	1	1	-1	-1	

La loi de réciprocité quadratique affirme que

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

On trouve ainsi

$$\begin{aligned} \left(\frac{3}{37}\right) &= \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1, \\ \left(\frac{3}{41}\right) &= \left(\frac{41}{3}\right) = \left(\frac{-1}{3}\right) = -1, \\ \left(\frac{3}{43}\right) &= -\left(\frac{43}{3}\right) = -\left(\frac{1}{3}\right) = -1, \\ \left(\frac{3}{47}\right) &= -\left(\frac{47}{3}\right) = -\left(\frac{2}{3}\right) = 1. \end{aligned}$$

7. On considère un corps fini ayant $q = 64$ éléments.

a) Comme 64 est une puissance de 2, la caractéristique de ce corps est 2.

b) Le groupe multiplicatif du corps est cyclique d'ordre $q - 1 = 63$, les entiers n pour lesquels il existe un sous-groupe d'ordre n sont les diviseurs de $q - 1$. Par conséquent les entiers $n \geq 1$ pour lesquels il existe au moins une racine primitive n -ième de l'unité dans ce corps sont les diviseurs de $q - 1 = 63$, donc ce sont les nombres 1, 3, 7, 9, 21 et 63. Quand n divise $q - 1$, il y a exactement $\varphi(n)$ éléments d'ordre n dans le groupe cyclique d'ordre $q - 1$, donc il y a 1 élément d'ordre 1, 2 d'ordre 3, 6 d'ordre 9, 6 d'ordre 7, 12 d'ordre 21 et 36 d'ordre 63.

8. Les générateurs du groupe cyclique $(\mathbf{Z}/7\mathbf{Z})^\times$ (c'est-à-dire les éléments d'ordre 6) sont les classes de 3 et 5 modulo 7 (il y en a 2 puisque $\varphi(6) = 2$).

Les nombres premiers p tels que le polynôme cyclotomique $\Phi_7(X)$ soit irréductible sur le corps fini \mathbf{F}_p à p éléments sont les nombres premiers p dont la classe modulo 7 engendre $(\mathbf{Z}/7\mathbf{Z})^\times$, donc ce sont les nombres premiers congrus à 3 ou 5 modulo 7.

On ne le demandait pas, mais on peut ajouter que dans le groupe cyclique $(\mathbf{Z}/7\mathbf{Z})^\times$, les classes de 2 et 4 sont d'ordre 3 (il y en a bien 2 = $\varphi(3)$), celle de 6 (qui est celle de -1) d'ordre 2 (il n'y en a qu'une puisque $\varphi(2) = 1$) et celle de 1 d'ordre 1 (comme il se doit).

Il en résulte que, pour un nombre premier p congru à 2 ou 4 modulo 7, le polynôme Φ_7 se décompose en un produit de deux polynômes irréductibles sur \mathbf{F}_p de degrés 3, tandis que pour p congru à 6 modulo 7, le polynôme Φ_7 se décompose en un produit de trois polynômes irréductibles sur \mathbf{F}_p de degrés 2. Pour p congru à 1 modulo 7, le polynôme Φ_7 se décompose totalement dans \mathbf{F}_p , ce qui veut dire que \mathbf{F}_p^\times contient les 6 racines primitives 7èmes de l'unité (quand $p - 1$ est multiple de 7

tout groupe cyclique d'ordre $p - 1$ contient un sous-groupe d'ordre 7, ce sous-groupe est cyclique et il y a 6 générateurs). Enfin pour $p = 7$ le polynôme Φ_7 se décompose complètement sur le corps \mathbf{F}_7 en $\Phi_7(X) = (X - 1)^6$.

9. Soient $f \in \mathbf{F}_p[X]$ un polynôme irréductible de degré d , K un corps fini de caractéristique p et $\alpha \in K$ une racine de f . Les racines de f dans K sont

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}.$$

Ces éléments sont deux-à-deux distincts, au nombre de d , et le polynôme f est complètement décomposé dans K .

10. Le code cyclique sur \mathbf{F}_2 de longueur 7 dont le polynôme générateur est

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$$

a pour dimension 1, il est donc composé des deux éléments

$$(0, 0, 0, 0, 0, 0, 0) \quad \text{et} \quad (1, 1, 1, 1, 1, 1, 1).$$

11. Soient n un entier ≥ 2 , F_n le nombre de Fermat $2^{2^n} + 1$, p un diviseur premier de F_n .

a) L'ordre de 2 divise 2^{n+1} car $2^{n+1} \equiv 1 \pmod{p}$ mais ne divise pas 2^n car $2^n \equiv -1 \pmod{p}$. Donc c'est 2^{n+1} .

b) L'ordre de 2 modulo p divise $p - 1$, donc p est congru à 1 modulo 2^{n+1} .

c) Le nombre 2 est résidu quadratique modulo p car p est congru à 1 modulo 8 (et même modulo 2^{n+1} – on a supposé $n \geq 2$).

d) Comme 2 est résidu quadratique modulo p et que le symbole de Legendre $\left(\frac{2}{p}\right)$ est congru à $2^{(p-1)/2}$ modulo p , on en déduit que le nombre $2^{(p-1)/2}$ est congru à 1 modulo p . Cela signifie que l'ordre de 2 modulo p divise $(p-1)/2$. Comme cet ordre est 2^{n+1} , on en déduit que 2^{n+1} divise $(p-1)/2$, ce qui signifie que p est congru à 1 modulo 2^{n+2} .