Compter les carrés dans $\mathbb{Z}_n$

Walter D. Stangl
Université Biola La Mirada, CA 90639

Un problème élémentaire de théorie des nombres consiste à déterminer les formes possibles des carrés parmi les entiers positifs. Par exemple, il est facile de voir que tout carré doit être de la forme $3k$ ou $3k+1$. (Puisque tout entier peut s'écrire sous l'une des formes $3q$, $3q+1$, ou $3q+2$, élever simplement au carré ces nombres et simplifier). Reformulée, cette assertion est que 0 et 1 sont les carrés dans $\mathbb{Z}_3$, l'anneau des classes d'équivalence des entiers modulo 3. En général, un carré a la forme $nk+r$ si, et seulement si, r est un carré dans l'anneau $\mathbb{Z}_n$. Combien de carrés y a-t-il dans $\mathbb{Z}_n$?

Notions fondamentales. Un élément a dans $\mathbb{Z}_n$ est un *carré* dans $\mathbb{Z}_n$ si et seulement si $x^2 = a$ a une solution dans $\mathbb{Z}_n$. Les unités de $\mathbb{Z}_n$ sont les éléments qui sont premiers à n. Les unités qui sont des carrés sont habituellement appelées *résidus quadratiques* (ou, plus précisément, les résidus quadratiques mod n dans le système des résidus réduit) [1, p. 84]. Les résidus quadratiques ont été complètement caractérisés [2, p. 201], et les résultats standards seront utilisés dans ce qui suit.

On adoptera la notation suivante : $q(n)$ = le nombre de résidus quadratiques dans $\mathbb{Z}_n$, et $s(n)$ = le nombre des carrés dans $\mathbb{Z}_n$. Par exemple, $q(8) = 1$ puisque $x^2 = 1$ a une solution dans $\mathbb{Z}_8$, (en fait, les quatre unités, notamment 1, 3, 5, et 7, sont toutes solutions), et $x^2 = 3, x^2 = 5$, et $x^2 = 7$ n'ont pas de solutions dans $\mathbb{Z}_8$. Aussi, $s(8) = 3$ puisque $x^2 = 0$ et $x^2 = 4$ ont aussi des solutions dans $\mathbb{Z}_8$, mais $x^2 = 2$ et $x^2 = 6$ n'en ont pas.

Un fonction de théorie des nombres $f(n)$ est *multiplicative* si $\gcd(m, n) = 1$ implique $f(mn) = f(m) \cdot f(n)$. Les fonctions typiques de théorie des nombres qui sont multiplicatives incluent le nombre de diviseurs positifs de n et la somme de ces diviseurs [1, p. 109]. Une fonction de théorie des nombres qui est multiplicative est complètement caractérisée par ses valeurs sur les puissances des nombres premiers. Et $q(n)$ et $s(n)$ sont multiplicatives ; on dérive des formules récursives et en forme fermée pour ces fonctions sur les puissances de nombres premiers. Cela nous permettra de calculer $s(n)$ et $q(n)$ pour tout n, en utilisant la factorisation en nombres premiers de n.

Supposons que $\gcd(m, n) = 1$. Alors $\mathbb{Z}_{mn}$ est isomorphe à $\mathbb{Z}_m \times \mathbb{Z}_n$, selon l'isomorphisme d'anneaux $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ défini par $h(z) = (z \bmod m, z \bmod n)$ [3, p. 80]. Supposons que a est un carré dans $\mathbb{Z}_{mn}$. Alors il existe un certain b dans $\mathbb{Z}_{mn}$ tel que $b^2 = a$. Puisque h est une fonction de $\mathbb{Z}_{mn}$ dans $\mathbb{Z}_m \times \mathbb{Z}_n$, il existe $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$, tel que $h(b) = (x, y)$. Alors $h(a) = h(b^2) = [h(b)]^2 = (x, y)^2 = (x^2, y^2)$, et donc $h(a)$ est un carré dans $\mathbb{Z}_m \times \mathbb{Z}_n$. Par conséquent $s(mn) \leq s(m) \cdot s(n)$.

D'un autre côté, si u dans $\mathbb{Z}_m$ et v dans $\mathbb{Z}_n$ sont des carrés, alors il existe x dans $\mathbb{Z}_m$ et y dans $\mathbb{Z}_n$, tels que $(x^2, y^2) = (u, v)$ dans $\mathbb{Z}_m \times \mathbb{Z}_n$. Ainsi, $h^{-1}(u, v) = h^{-1}[(x, y)^2] = [h^{-1}(x, y)]^2$, donc $h^{-1}(u, v)$ est un carré dans $\mathbb{Z}_{mn}$. Par conséquent, $s(mn) \geq s(m) \cdot s(n)$.

La combinaison de ces résultats amène l'égalité souhaitée, montrant que $s(n)$ est une fonction multiplicative. Étendre la preuve à $q(n)$ nécessite simplement d'observer que pour tout entier b, $\gcd(b, mn) = 1$ si, et seulement si, $\gcd(b, m) = 1$ et $\gcd(b, n) = 1$.

Formule de récurrence. Notre prochain but est de démontrer une formule générale de récurrence pour le nombre de carrés dans $\mathbb{Z}_{p^n}$ où p est un nombre premier supérieur à 2. Une fois que ceci sera fait, les formules en forme fermée pour les différentes composantes complèteront notre procédure de comptage. On commence par l'observation que les carrés dans $\mathbb{Z}_{p^n}$ qui ne sont pas des résidus quadratiques sont engendrés par les carrés dans $\mathbb{Z}_{p^{n-2}}$, i.e., b est un carré dans $\mathbb{Z}_{p^{n-2}}$ si et seulement si bp^2 est un carré dans $\mathbb{Z}_{p^n}$.

D'abord, supposons qu'il existe c dans $\mathbb{Z}_{p^{n-2}}$ tel que $c^2 = kp^{n-2} + b$ dans $\mathbb{Z}$. Alors $c^2p^2 = kp^n + bp^2$. Maintenant $cp < p^n$, donc $(cp)^2 = bp^2$ est un carré dans $\mathbb{Z}_{p^n}$. Inversement, supposons qu'il existe y dans $\mathbb{Z}_{p^n}$ tel que $y^2 = mp^n + sp^2$ dans $\mathbb{Z}$. Alors p^2 divise y^2, donc p divise y. Ainsi, il existe c tel que $y = cp$. Alors $c^2 = mp^{n-2} + s$ et s est un carré dans $Z_{p^{n-2}}$.

Maintenant on souhaite compter tous les carrés dans $\mathbb{Z}_{p^n}$. On commence par observer que les carrés sont de deux sortes. Puisque $q(p^n)$ compte les carrés dans $\mathbb{Z}_{p^n}$ qui sont des unités, on doit simplement compter les carrés qui ne sont pas des unités, i.e., les multiples de p. Supposons que kp est un carré dans $\mathbb{Z}_{p^n}$. Alors il existe un b tel que $b^2 = cp^n + kp$. Alors p divise b^2, et donc b. Par conséquent, p^2 divise b^2, et donc kp, donc p divise k. Donc les multiples de p qui sont des carrés sont des multiples de p^2. Mais par le résultat précédent, le nombre de ceux-ci est donné par $s(p^{n-2})$.

Ainsi on a démontré la formule de récurrence suivante.

THÉORÈME. Pour $n \geq 3, s(p^n) = q(p^n) + s(p^{n-2})$.

Puissances de nombres premiers impairs. Pour obtenir des formules explicites pour les fonctions $q(p^n)$ et $s(p^n)$, il est utile de traiter le cas $p = 2$ séparément. L'argument pour les puissances d'un nombre premier impair p dépend de l'existence d'une racine primitive pour p^n pour tout n. En langage algébrique, cela dit que les unités de $\mathbb{Z}_{p^*}$ forment un groupe cyclique selon la multiplication et par conséquent ont un générateur [1, p. 62]. Puisque cela n'est pas vrai pour les puissances de 2 supérieures ou égales à 3, notre approche et nos résultats devront être un peu modifiés pour cette situation.

Si p est un nombre premier impair, la fonction indicatrice d'Euler fournit le nombre d'unités de $\mathbb{Z}_{p^n}$, qui est $p^n - p^{n-1}$. Il y a une racine primitive de p^n. Les puissances paires de cette racine primitive sont clairement des résidus quadratiques distincts, et la formule suivante est démontrée.

THÉORÈME. *Si p est un nombre premier impair, alors $q(p^n) = (p^n - p^{n-1})/2$, pour tout $n \geq 1$.*

Dans le but de compter tous les carrés dans $\mathbb{Z}_{p^n}$, il est utile de regarder les deux premiers cas séparément. Puisque 0 est le seul élément non unité dans $\mathbb{Z}_p$, clairement $s(p) = q(p) + 1 = (p + 1)/2$. Dans $\mathbb{Z}_{p^2}$, les non-unités sont des multiples de p, et ont des carrés égaux à 0. Ainsi $s(p^2) = q(p^2) + 1 = (p^2 - p + 2)/2$.

Maintenant, supposons $n \geq 3$ et n pair. Par des applications répétées de la formule de récurrence,

on obtient

$$\begin{aligned} s(p^n) &= \frac{p^n - p^{n-1}}{2} + \frac{p^{n-2} - p^{n-1}}{2} + \ldots + \frac{p^4 - p^3}{2} + \frac{p^2 - p + 2}{2} \\ &= \frac{p^{n+1} - p^n + p^n - p^{n-1} + p^{n-1} - \ldots + p^3 - p^2 + 2p + p^2 - p + 2}{2(p+1)} \\ &= \frac{p^{n+1} + p + 2}{2(p+1)} \end{aligned}$$

Si n est impair, on obtient

$$\begin{aligned} s(p^n) &= \frac{p^n - p^{n-1}}{2} + \frac{p^{n-2} - p^{n-1}}{2} + \ldots + \frac{p^4 - p^3}{2} + \frac{p^2 - p + 2}{2} \\ &= \frac{p^{n+1} - p^n + p^n - p^{n-1} - \ldots + p^2 + 2p + 1}{2(p+1)} \\ &= \frac{p^{n+1} + 2p + 1}{2(p+1)} \end{aligned}$$

Nos résultats sont résumés dans le théorème suivant.

THÉORÈME. *Supposons que p est un nombre premier impair. Alors*

$$s(p) = \frac{p+1}{2} \quad \text{et} \quad s(p^2) = \frac{p^2 - p + 2}{2}$$

Si $n \geq 3$, alors

$$s(p^n) = \begin{cases} \dfrac{p^{n+1} + p + 2}{2(p+1)} & n \ \textit{pair} \\ \dfrac{p^{n+1} + 2p + 1}{2(p+1)} & n \ \textit{impair.} \end{cases}$$

Puissances de deux. Maintenant on procède au cas restant : les puissances de 2. On a besoin d'un résultat préliminaire avant de nous consacrer à notre but principal.

Supposons $n \geq 3$, et $\text{pgcd}(a, 2^n) = 1$. Considérons l'équation $x^2 = a$ dans $\mathbb{Z}_2$. Supposons que b est une solution. Alors, clairement, $-b$ est également une solution. Aussi $b \neq -b$, puisque sinon $2b = 0$, ce qui implique $\text{pgcd}(b, 2^n) \neq 1$ alors qu'on sait que $\text{pgcd}(b^2, 2^n) = 1$. Une autre paire de solutions facilement vérifiable est $2^{n-1} \pm b$. On voit que ces valeurs sont distinctes par l'argument ci-dessus.

Pour montrer que ces quatre solutions sont les seules solutions, supposons que $\text{pgcd}(c, 2^n) = 1$ et que c est une solution en sus de b. Alors $b^2 = a = c^2$ dans $\mathbb{Z}_{2^n}$ implique $b^2 - c^2 = 0$ ou $(b-c)(b+c) = 0$ dans $\mathbb{Z}_{2^n}$. Puisque b et c sont tous les deux impairs, soit $(b-c)$ soit $(b+c)$ doit être de la forme $4m + 2 = 2(2m+1)$. Donc l'autre facteur est un multiple de 2^{n-1} ou bien 0. Par conséquent

$c = 2^{n-1} \pm b$ ou $c = \pm b$.

Ainsi on conclut que si $x^2 = a$ a une solution dans $\mathbb{Z}_{2^n}$, alors l'équation a exactement 4 solutions distinctes dans $\mathbb{Z}_{2^n}$.

On observe que le seul résidu quadratique soit dans $\mathbb{Z}_2$ soit dans $\mathbb{Z}_4$ est 1. Il en découle que $q(2) = q(4) = 1$.

Pour $n \geq 3$, il y a 2^{n-1} unités dans $\mathbb{Z}_{2^n}$, notamment les nombres impairs. Considérons que deux unités sont équivalentes si leurs carrés sont égaux. Alors les unités peuvent être séparés en classes d'équivalence de 4 unités chacune ; par conséquent, il y aura $2^{-2}2^{n-1} = 2^{n-3}$ résidus quadratiques dans $\mathbb{Z}_{2^n}$. Ainsi pour $n \geq 3, q(2^n) = 2^{n-3}$.

On est maintenant prêt à démontrer les dernières formules. Voici le résultat.

THÉORÈME.

$$s(2^n) = \begin{cases} \dfrac{2^{n-1}+4}{3} & n \textit{ pair} \\ \dfrac{2^{n-1}+5}{3} & n \textit{ impair}, n \geq 3. \end{cases}$$

Preuve. L'argument est par induction. En commençant avec $n = 2$, il est clair que $s(2^2) = 2$. Maintenant, supposons que la formule est vérifiée pour $n \leq k$. Il y a deux cas.

Cas I. $k+1$ est pair. Alors

$$\begin{aligned} s(2^{k+1}) &= q(2^{k+1}) + s(2^{k-1}) = 2^{(k+1)-3} + \frac{2^{(k-1)-1}+4}{3} \\ &= 2^{k-2} + \frac{2^{k-2}+4}{3} + \frac{4 \cdot 2^{k-2}+4}{3} = \frac{2^{(k+1)-1}+4}{3} \end{aligned}$$

Cas II. $k+1$ est impair. Alors

$$\begin{aligned} s(2^{k+1}) &= q(2^{k+1}) + s(2^{k-1}) = 2^{(k+1)-3} + \frac{2^{(k-1)-1}+5}{3} \\ &= 2^{k-2} + \frac{2^{k-2}+5}{3} + \frac{4 \cdot 2^{k-2}+5}{3} = \frac{2^{(k+1)-1}+5}{3} \end{aligned}$$

Les formules précédentes sont obtenables directement à partir de la formule de récurrence. Par exemple, si n est impair, des applications répétées amènent

$$\begin{aligned} s(2^n) &= q(2^n) + q(2^{n-2}) + \ldots + q(2^3) + s(2^1) \\ &= 2^{n-3} + 2^{n-5} + \ldots + 1 + 2. \end{aligned}$$

Donc on a besoin d'une formule pour la somme des puissances paires de 2. En posant $x_n =$

$1 + 2^2 + \ldots + 2^{2n}$, on a

$$\begin{aligned} x_n &= (2^2)^0 + (2^2)^1 + \ldots + (2^2)^n \\ &= \frac{(2^2)^{n+1} - 1}{2^n - 1} \end{aligned}$$

Donc $x_n = \dfrac{2^{2n+2} - 1}{3}$, et

$$\begin{aligned} s(2^n) &= x_{(n-3)/2} + 2 \\ &= \frac{2^{n-1} - 1}{3} + 2 = \frac{2^{n-1} + 5}{3}. \end{aligned}$$

Une formule pour la somme des puissances impaires de 2 s'obtient de x_n en factorisant, et alors $s(2^n)$ se calcule facilement.

Références

[1.] Ivan Niven, Herbert Zuckerman, *An Introduction to the Theory of Numbers*, 4ème édition, John Wiley and Sons, Inc., New York, 1980.

[2.] David M. Burton, *Elementary Number Theory*, 3ème édition, Wm. C. Brown, Dubuque, IA, 1994.

[3.] John Fraleigh, *A First Course in Abstract Algebra*, 3ème édition, Addison-Wesley, Reading, MA, 1982.