Ajouter des unités mod n

Marian Deaconescu

Marian Deaconescu est originaire de Roumanie, mais il travaille maintenant à l'étranger, au Koweit. Ses principaux centres d'intérêt en mathématiques sont reliés à la théorie des groupes. Ses deux petites filles, la photographie noir et blanc, la pêche et le temps passé à nourrir son chien sont les raisons qui font qu'il fait moins de mathématiques qu'il ne devrait.

dédié à Nicolae Popescu

Soit un entier $n \geq 2$ et dénotons par $U(Z_n)$ le groupe des unités de l'anneau Z_n des classes résiduelles modulo n. Ainsi $U(Z_n) = \{k \in Z | (k, n) = 1\}$. $U(Z_n)$ n'est pas clos par addition ; par exemple, $1 \in U(Z_2)$, mais $1 + 1 = 0 \notin U(Z_2)$.

Si l'on joue un peu avec les tables d'*addition* pour $U(Z_n)$, on observe que si n est impair, alors tout élément de Z_n apparaît dans la table comme un résultat. Dit autrement, l'équation $x + y = k$ semble avoir des solutions $x, y \in U(Z_n)$ pour tout $k \in Z_n$.

Si n est pair, pourtant, on observe rapidement que les classes de résidus impairs ne sont jamais sommes d'unités dans $U(Z_n)$; la raison est simple à voir ; n étant pair, les classes résiduelles sont contraintes d'être impaires et donc la somme de deux unités n'est jamais une classe résiduelle impaire.

Il est bien connu que pour un nombre premier p, la congruence $x + y = 0 \pmod{p}$ a exactement p solutions qui peuvent être représentées par les couples $(0, 0), (1, p - 1), ..., (p - 1, 1)$. À part la solution triviale $(0, 0)$, les composantes des solutions restantes sont toutes des classes de résidus non nulles dans le corps F_p à p éléments. [...][1] Dans le présent article, M. Deaconescu traite la variante suivante du problème décrit au début : il répond à la question du nombre de solutions x qui sont des nombres premiers à n et de la congruence $x + y = k \pmod{n}$, où k, n sont des nombres naturels quelconques.

Ces remarques élémentaires suggèrent le problème naturel de trouver, étant donnée une classe $k \in Z_n$, combien de fois cette classe k apparaît comme résultat dans la table d'addition de $U(Z_n)$. Selon une terminologie différente : fixons un certain entier naturel $n \geq 2$ et pour tout entier naturel k tel que $0 \leq k \leq n - 1$, déterminer le nombre $s(k)$ défini comme suit :

$$s(k) = |\{(x, y) \in U(Z_n) \times U(Z_n) \mid x + y = k\}|.$$

Bien sûr, ça n'est pas tout à fait un exercice évident. Car si on essaie de construire les tables d'addition des $U(Z_n)$ pour des nombres n de plus en plus compliqués (utiliser un ordinateur aide

Elem. Math. 55 (2000) 123-127, © Birkhäuser Verlag. Basel, 2000, Elemente der Mathematik.

Pendant l'écriture de cet article, l'auteur était financé par la subvention de recherche K.U. SM177.

[1] Je ne peux vérifier la traduction de l'allemand proposée par Google : "*En particulier, cela prouve que le nombre de points F_p-rationnels de l'espace projectif à une dimension est p. La question analogue pour les systèmes de polynômes de degré supérieur à plusieurs variables conduit aux conjectures d'A. Weil, résolues par P. Deligne dans les années 1970.*

à réaliser cette tâche fastidieuse), de plus en plus insaisissables, une conjecture de travail semble apparaître.

La réponse à notre question semble dépendre, de façon inattendue, de considérations liées au nombre de points fixes des automorphismes du groupe additif $(Z_n, +)$.

Théorème. *Soit $n \geq 2$ un entier naturel, soit k tel que $0 \leq k \leq n-1$, et dénotons par $s(k)$ le nombre de solutions $(x, y) \in U(Z_n) \times U(Z_n)$ de l'équation $x + y = k$. Alors*

$$s(k) = \frac{\varphi(n)}{\varphi(n/d)} \Psi(d, n)$$

où $d = (k, n)$ et $\Psi(d, n)$ est le nombre de ces automorphismes du groupe additif Z_n ayant exactement d points fixes.

Dans l'énoncé du théorème, (k, n) désigne le plus grand commun diviseur de k et n, alors que $\varphi(n)$ est la valeur de la fonction indicatrice d'Euler de n.

Preuve. Soit α un automorphisme du groupe additif Z_n. Alors $Fix(\alpha) = \{k \in Z_n \mid \alpha(k) = k\}$ est un sous-groupe de Z_n, et par conséquent, par le théorème de Lagrange, $|Fix(\alpha)|$ est un diviseur de n. Pour un diviseur d de n, $\Psi(d, n)$ dénote le nombre de ces automorphismes du groupe cyclique (additif) Z_n, qui ont d points fixes.

Observons d'abord que

$$\Psi(d, n) = |\{u \in U(Z_n) | (u–1, n) = d\}|. \tag{1}$$

Dans le but de prouver (1), notons qu'on peut identifier tout automorphisme $\alpha \in Aut(Z_n, +)$ avec une unité fixée $u \in U(Z_n)$ de telle façon que $\alpha(k) = ku$. Par conséquent

$$|Fix(\alpha)| = |Fix(u)| = |\{k \in Z_n \mid ku = k\}| = |\{k \in Z_n \mid n|k(u-1)\}| = (u-1, n).$$

Cela prouve l'hypothèse. □

Rappelons que nous voulons compter le nombre $s(k)$ de solutions dans $U(Z_n)$ de l'équation

$$x + y = k. \tag{*}$$

Soit $d = (k, n)$, de telle façon que $k = dt^{-1}$ pour une certaine unité $t \in U(Z_n)$ fixée. Transformons maintenant (*) dans des formes successives (et de plus en plus horribles) :

$$\begin{aligned} x + y = dt^{-1} &\iff xt + yt = d \iff x + y = d \iff xy^{-1} + 1 = dy^{-1} \\ &\iff xy + 1 = dy \iff -xy + 1 = dy. \end{aligned}$$

On doit ici attirer l'attention : quand on passe d'une équation à une autre, le signe d'équivalence est utilisé pour indiquer que les deux équations ont le même nombre de solutions.

Revenons à la longue liste d'équivalences : la première équation a le même nombre de solutions que (*), mais elle a deux avantages. Notons d'abord que $d = (dy, n) = (xy - 1, n)$. Ensuite, observons

que lorsque y parcourt $U(Z_n)$, l'expression dy prend exactement $\varphi(n/d)$ valeurs distinctes dans Z_n. En combinant ces remarques avec la formule (1), on voit que $s(k) = \dfrac{\varphi(n)}{\varphi(n/d)}\Psi(d,n)$, comme affirmé.

Supposons qu'on peut trouver la première décomposition de n (facile à supposer, mais habituellement difficile à réaliser en pratique - un fait sur lequel on devrait toujours insister !), i.e. $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ et soit $d = \prod_{i=1}^{s} p_i^{\beta_i}$ un diviseur de n. Il a été déterminé dans [1] que

$$\Psi(d,n) = \prod_{\substack{p_i \mid n/d \\ p_i \mid d}} p_i^{\alpha_i - \beta_i - 1}(p_i - 1) \prod_{\substack{p_j \mid n/d \\ p_j \nmid d}} p_j^{\alpha_j - 1}(p_j - 2) \tag{2}$$

Selon le théorème et selon la formule (2), les nombres $s(k)$ peuvent être effectivement calculés en supposant qu'on dispose d'une décomposition en facteurs premiers de n. La formule (2) permet également de dériver une première conséquence immédiate du théorème :

Corollaire 1 : *Soit $n \geq 2$ un entier naturel ;*

i) *Si n est impair, alors tout élément de Z_n est une somme de deux unités.*

ii) *Si n est pair, alors $k \in Z_n$ est une somme de deux unités si et seulement si k est pair.*

Preuve.

i) Si n est impair, la formule (2) indique que $\Psi(d,n) \neq 0$ pour tous les diviseurs d de n et le résultat découle du théorème.

ii) Par (2) et par le théorème, $s(k) \neq 0 \iff \Psi(d,n) \neq 0$, où $d = (k,n) \iff d$ est pair $\iff k$ est pair.

Le théorème a une autre conséquence moins évidente dans le domaine des entiers positifs - une inégalité qui identifie les nombres premiers comme une "empreinte digitale" dans son cas extrême.

De telles inégalités ne sont pas du tout courantes. Considérons juste celle-ci : si $n \geq 2$ est un entier naturel, alors $\varphi(n) \leq n-1$ et l'égalité a lieu si et seulement si n est un nombre premier. Certes, ces résultats sont jolis, mais ils ont une valeur pratique limitée et on se demande pourquoi en ajouter un de plus à la collection de ceux existant déjà.

Voici quelques raisons : l'inégalité suivante fait intervenir une fonction arithmétique moins habituelle, notamment $\Psi(1,n)$, cela suggère une conjecture naturelle que je pense être vraie, mais qui est très difficile à démontrer et sa preuve utilise les nombres $s(k)$.

Corollaire 2 : Soit $n \geq 2$ un entier naturel et soit $\Psi(1,n)$ le nombre d'automorphismes sans point fixe du groupe additif Z_n. Alors

$$\varphi(n)(\varphi(n) - 1) \geq (n-1)\Psi(1,n)$$

et l'égalité est vérifiée si et seulement si n est un nombre premier.

Preuve. Comme le suggère la notation $\Psi(1,n)$, un automorphisme sans point fixe du groupe additif Z_n est un automorphisme qui fixe seulement la classe identité 0.

Prenons $d=1$ dans la formule (2) pour obtenir

$$\Psi(1,n)=\prod_{i=1}^{s} p_i^{\alpha_i-1}(p_i-1). \tag{3}$$

Observons alors que, par définition de $s(k)$, on obtient :

$$\sum_{k=0}^{n-1} s(k)=\varphi(n)^2. \tag{4}$$

En effet, $U(Z_n)$ a $\varphi(n)$ éléments et sa table d'addition a $\varphi(n)^2$ entrées.

Appliquons le théorème deux fois pour obtenir :

$$s(0)=\varphi(n) \tag{5}$$

et

$$s(k)=\Psi(1,n) \qquad \text{à chaque fois que } (k,n)=1. \tag{6}$$

Maintenant, utilisons (2) et (3) pour obtenir, après un calcul plutôt long - mais élémentaire, que

(7) Pour n impair et pour d un diviseur propre de n, $\varphi(n)\Psi(d,n)>\varphi(n/d)\Psi(1,n)$.

Après cette préparation, on est prêt à prouver le corollaire 2. Soit d'abord n pair ≥ 4, de telle façon que par (3), $\Psi(1,n)=0$. L'énoncé est correct dans ce cas.

Supposons ensuite que n est impair et composé ; alors il existe un certain k, $0<k<n-1$ avec $(k,n)>1$ et on obtient :

$$\varphi(n)(\varphi(n)-1)=\varphi(n)^2-\varphi(n)= \qquad \text{(par (4) et (5))}$$

$$\sum_{k=1}^{n-1} s(k)=\sum_{(k,n)=1} s(k)+\sum_{(k,n)>1} s(k)= \qquad \text{(par (6))}$$

$$\varphi(n)\Psi(1,n)+\sum_{(k,n)>1} s(k)> \qquad \text{(par (7) et par théorème)}$$

$$\varphi(n)\Psi(1,n)+(n-1-\varphi(n))\Psi(1,n)=(n-1)\Psi(1,n).$$

Finalement, soit n un nombre premier. Alors (3) donne que $\Psi(1,n)=n-2$ et puisque clairement $\varphi(n)=n-1$, on vérifie aisément que l'égalité est vérifiée dans ce cas. La preuve est complète. □

Remarque. L'inégalité dans le corollaire 2 peut être prouvée directement, par des inégalités de force brute, mais c'est un peu bizarre de faire ça.

Il devrait être clair à partir de maintenant que les nombres $\Psi(1,n)$ ont une forte ressemblance avec $\varphi(n)$: considérons juste leur valeur si n est un nombre premier ou un nombre sans carré. Une conjecture bien connue (et autant que je sache non résolue à ce jour) de D.H. Lehmer [3] affirme

que si $n \geq 2$ et si $\varphi(n)$ divise $n-1$, alors n doit être un nombre premier.

Par analogie et inspiré par le corollaire 2, on peut conjecturer que les entiers $n \geq 2$ pour lesquels $\Psi(1,n)$ divise $\varphi(n)-1$ doivent être des nombres premiers. Je m'attends à ce que cette conjecture soit aussi difficile que celle de Lehmer. Le lecteur qui souhaite lire davantage de résultats partiels en lien avec la conjecture de Lehmer devrait consulter [2] pour une bibliographie partielle.

Je voudrais ici étendre mes remerciements à mon bon ami Vali Filip. Infirmier de formation et vocation, avec la patience d'un ange, il a été capable de comprendre la plupart de ce matériau, bien qu'à l'occasion j'aie dû lui expliquer ce qu'est un groupe et un automorphisme de groupe.

Bibliographie

[1] M. Deaconescu and H.K. Du, *Counting similar automorphisms of finite cyclic groups*, Math. Japonica 46 (1997), 345-348.

[2] R.K. Guy, *Unsolved problems in Number Theory*, Springer Verlag, 1981.

[3] D.H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. 38 (1932), 745-751.

Marian Deaconescu
Département de mathématiques et informatique
Université du Koweit
P.O. Box 5969
Safat 13060
Kuwait
e-mail: DEACON@math-1.sci.kuniv.edu.kw