Canad. Math. Bull. Vol. 21 (4), 1978

SUMS OF POWERS IN ARITHMETIC PROGRESSIONS

BY
CHARLES SMALL

The papers [2] and [3] study the function $g(k, n)$, defined for integers $k>1$ and $n>1$ as the smallest r with the property that every integer is a sum of r kth powers mod n. This note identifies $g'(k)$, defined as the maximum over all n of $g(k, n)$, with the function $\Gamma(k)$ studied by Hardy and Littlewood [1] fifty years ago in connection with Waring's problem.

I want to thank Professor Eric Milner for a push in the right direction.

Notation:

$\mathbb{Z}$ = rational integers = $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$.

$\mathbb{N}$ = natural numbers = $\{0, 1, 2, 3, \ldots\}$.

$\mathbb{N}_i = \{n \in \mathbb{N} \mid n > i\}$, for $i = 0, 1$.

$\mathbb{Z}/n\mathbb{Z}$ = ring of integers mod n, *for* $n \in \mathbb{N}_1$.

For r, $k \in \mathbb{N}_1$, $\mathbb{N}^r$ is the Cartesian product of r copies of $\mathbb{N}$, $\sum_r^k$ is the map $\mathbb{N}^r \to \mathbb{N}$ given by $(x_1, x_2, \ldots, x_r) \mapsto x_1^k + x_2^k + \cdots + x_r^k$, and I_r^k is the image of $\sum_r^k$.

For $k, n \in \mathbb{N}_1$, $g(k, n)$ and $g'(k)$ are defined as above.

For $a \in \mathbb{N}$ and $n \in \mathbb{N}_0$, $P_n(a)$ denotes the arithmetic progression $\{a + tn \mid t \in \mathbb{N}\}$ and $\widetilde{P_n(a)}$ denotes the complete arithmetic progression $\{a + tn \mid t \in \mathbb{Z}\} \cap \mathbb{N}$. Thus $P_n(a) \subseteq \widetilde{P_n(a)} \subseteq \mathbb{N}$.

We let ϕ denote the projection $\mathbb{N} \to \mathbb{Z}/n\mathbb{Z}$, and (as usual) write $\bar{a}$ instead of $\phi(a)$. Note that $\phi^{-1}(\bar{b}) = \widetilde{P_n(a)}$ for any $b \equiv a (\text{mod}\, n)$.

Now we make four definitions, for $k \in \mathbb{N}_1$:

$\Gamma_0(k)$ denotes the smallest $r \in \mathbb{N}_1$ with the property that every arithmetic progression contains a sum of r kth powers, i.e., the least r such that $\widetilde{P_n(a)} \cap I_r^k \neq \emptyset$, for all $a \in \mathbb{N}$ and $n \in \mathbb{N}_0$.

$\widetilde{\Gamma_0(k)}$ is the analogue, for complete arithmetic progressions, of $\Gamma_0(k)$, i.e. $\widetilde{\Gamma_0(k)}$ is the least r for which $\widetilde{P_n(a)} \cap I_r(k) = \emptyset$, for all $a \in \mathbb{N}$, $n \in \mathbb{N}_0$.

$\Gamma(k)$ denotes the smallest $r \in \mathbb{N}_1$ with the property that every arithmetic progression contains *infinitely many* sums of r kth powers, i.e., the least r such that $|P_n(a) \cap I_r^k| = \infty$, for all $a \in \mathbb{N}$ and $n \in \mathbb{N}_0$, where $|X|$, for a subset X of $\mathbb{N}$, denotes the cardinality of X; and $\widetilde{\Gamma(k)}$ is the analogue, for complete arithmetic progressions, of $\Gamma(k)$, i.e., $\widetilde{\Gamma(k)}$ is the least r for which $|\widetilde{P_n(a)} \cap I_r^k| = \infty$, for all $a \in \mathbb{N}$, $n \in \mathbb{N}_0$.

Received by the editors September 19, 1977.

https://doi.org/10.4153/CMB-1978-087-7 Published online by Cambridge University Press

We are going to show that the five functions g', Γ, $\tilde{\Gamma}$, Γ_0, and $\tilde{\Gamma}_0$ are in fact the *same* function. The function $\Gamma(k)$ of Hardy and Littlewood is defined differently, but they show (see [1], theorem 1) that for $k \neq 4$ it is the function considered here. (For $k=4$, $\Gamma(4)$ as defined here is 15, and $\Gamma(4)$ as defined by Hardy and Littlewood is 16.)

THEOREM. $g'=\Gamma=\tilde{\Gamma}=\Gamma_0=\tilde{\Gamma}_0$.

Proof. Fix $k \in \mathbb{N}_1$; we show $g'(k) \leq \widetilde{\Gamma_0(k)} \leq \widetilde{\Gamma(k)} \leq \Gamma(k) \leq \Gamma_0(k) \leq g'(k)$.

$g'(k) \leq \widetilde{\Gamma_0(k)}$: We have to show that for any $n \in \mathbb{N}_1$, every element of $\mathbb{Z}/n\mathbb{Z}$ is a sum of $\widetilde{\Gamma_0(k)}$ kth powers. But given $x \in \mathbb{Z}/n\mathbb{Z}$, $\phi^{-1}(x)$ is a complete arithmetic progression $\widetilde{P_n(a)}$ for some a; $\widetilde{P_n(a)}$ contains a sum of $\widetilde{\Gamma_0(k)}$ kth powers; and we need only apply ϕ.

$\widetilde{\Gamma_0(k)} \leq \widetilde{\Gamma(k)}$: This is trivial: if $|\widetilde{P_n(a)} \cap I_r^k| = \infty$ then surely $\widetilde{P_n(a)} \cap I_r^k \neq \emptyset$!

$\widetilde{\Gamma(k)} \leq \Gamma(k)$: This, too, is trivial: anything true for every arithmetic progression is true in particular for every complete arithmetic progression.

$\Gamma(k) \leq \Gamma_0(k)$: We have to show that if every arithmetic progression contains a sum of r kth powers then every arithmetic progression contains infinitely many sums of r kth powers. Given an arithmetic progression $P_n(a)$, choose $x_1 \in P_n(a) \cap I_r^k$. Now consider the arithmetic progression $P_n(x_1+n)$, and choose $x_2 \in P_n(x_1+n) \cap I_r^k$. Continuing in this way (choose $x_{i+1} \in P_n(x_i+n) \cap I_r^k$) we find a sequence of distinct numbers $x_1, x_2, x_3, \ldots$ in $P_n(a) \cap I_r^k$, for $P_n(a) \supseteq P_n(x_1+n) \supseteq P_n(x_2+n) \supseteq \cdots$.

$\Gamma_0(k) \leq g'(k)$: We have to show that every arithmetic progression $P_n(a)$ contains a sum of $g'(k)$ kth powers. In $\mathbb{Z}/n\mathbb{Z}$ we have $\bar{a} = \bar{x}_1^k + \cdots + \bar{x}_r^k$ for some $r \leq g(k, n) \leq g'(k)$. Choose representatives (pre-images under ϕ) $x_1, \ldots, x_r$ for $\bar{x}_1, \ldots, \bar{x}_r$ such that $x_i \geq a$ for all i $(1 \leq i \leq r)$. Then $a = x_1^k + \cdots + x_r^k - tn$ for some $t \in \mathbb{Z}$, and since $x_i^k \geq a$ for all i, $t \in \mathbb{N}$. Thus $a + tn \in P_n(a) \cap I_r^k$, and we are done.

$g'(k)$ can, in principle, be computed for any k by the methods of [3]. For computation of $\Gamma(k)$, see §§5 and 6 of [1].

REFERENCES

1. G. H. Hardy and J. E. Littlewood, *Some Problems of 'Partitio Numerorum' VIII: The Number $\Gamma(k)$ in Waring's Problem*, Proc. London Math. Soc. **28** (1927) 518–542.
2. C. Small, *Waring's Problem mod n*, Amer. Math. Monthly **84** (1977) 12–25.
3. C. Small, *Solution of Waring's Problem mod n*, Amer. Math. Monthly **84** (1977) 356–359.

DEPT. OF MATHEMATICS
QUEENS UNIVERSITY
KINGSTON, ONTARIO, CANADA K7L 3N6

https://doi.org/10.4153/CMB-1978-087-7 Published online by Cambridge University Press

MULLEN, KENNETH, *A note on Bernstein's bivariate inequality*
SANTHAKUMARI, C., *On quotient loops of normal subloops*
WANG, JAMES LI-MING, *Approximation on boundary sets*

ERRATA

Vol. **21** (1), 1978, pp. 21–30. In the paper "Reducible rational fractions of the type of Gaussian polynomials with only non-negative coefficients" the word "As" (p. 28, line 5(b) should read "If"; the word "Exactly" (p. 24, line 13(b)) should read "At least"; and the words "necessary and" (p. 24, lines 8/7(b)) should be omitted. The author's attention was called upon the need for these changes by M. Lewin, who will consider in detail the case $c > 1$ in a forthcoming paper.

https://doi.org/10.4153/CMB-1978-087-7 Published online by Cambridge University Press