



On Quadruples of Consecutive k th Power Residues

Author(s): R. L. Graham

Source: *Proceedings of the American Mathematical Society*, Vol. 15, No. 2 (Apr., 1964), pp. 196-197

Published by: [American Mathematical Society](#)

Stable URL: <http://www.jstor.org/stable/2034033>

Accessed: 01/04/2011 17:07

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=ams>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



American Mathematical Society is collaborating with JSTOR to digitize, preserve and extend access to *Proceedings of the American Mathematical Society*.

<http://www.jstor.org>

ON QUADRUPLES OF CONSECUTIVE k th POWER RESIDUES

R. L. GRAHAM

In a recent paper of D. H. and Emma Lehmer [2], the function $\Lambda(k, m)$ was defined (for arbitrary integers k and m) as follows:

Let p be a sufficiently large prime and let $r = r(k, m, p)$ be the least positive integer such that

$$r, r + 1, r + 2, \dots, r + m - 1$$

are all congruent modulo p to k th powers of positive integers. Define

$$\Lambda(k, m) = \limsup_{p \rightarrow \infty} r(k, m, p).$$

In [2] it was shown that $\Lambda(k, 4) = \infty$ for $k \leq 1048909$ and it was conjectured that $\Lambda(k, 4) = \infty$ for all k . In this paper we establish this conjecture with the following

THEOREM. $\Lambda(k, 4) = \infty$.

PROOF. It suffices to prove the theorem for values of k which are prime. The proof makes use of the following proposition which is a special case of a result of Kummer [1] (see also [3]).

PROPOSITION. *Let k be a prime and let $\gamma_1, \dots, \gamma_n$ be an arbitrary sequence of k th roots of unity. Then there exist infinitely many primes p with corresponding k th power character χ modulo p such that*

$$\chi(p_i) = \gamma_i, \quad 1 \leq i \leq n,$$

where p_i denotes the i th prime.

Thus, for any n and prime k , there exists a prime p with corresponding k th power character χ modulo p such that

$$\begin{aligned} \chi(2) &\neq 1, \\ \chi(p_i) &= 1, \quad 2 \leq i \leq n. \end{aligned}$$

Now consider any four consecutive positive integers all less than p_n . It is clear that exactly one of these integers must equal $2(2d+1)$ for some integer d . But we have

$$\chi(2(2d+1)) = \chi(2)\chi(2d+1) = \chi(2) \cdot 1 \neq 1$$

since $2d+1$ is the product of odd primes less than p_n . Therefore

Received by the editors December 29, 1962.

$2(2d+1)$ is not a k th power residue modulo p . Since n was arbitrary then $\Lambda(k, 4) = \infty$. This proves the theorem.

REFERENCES

1. E. Kummer, Abh. K. Akad. Wiss. Berlin (1859).
2. D. H. and E. Lehmer, *On runs of residues*, Proc. Amer. Math. Soc. **13** (1962), 102-106.
3. W. H. Mills, *Characters with preassigned values*, Canad. J. Math. **15** (1963), 169-171.

BELL TELEPHONE LABORATORIES

ON DECOMPOSITIONS OF PARTIALLY ORDERED SETS

E. S. WOLK

1. Introduction. Let P be a set which is partially ordered by a relation \leq . A *decomposition* \mathfrak{D} of P is a family of mutually disjoint non-empty chains in P such that $P = \cup \{C : C \in \mathfrak{D}\}$. Two elements x, y of P are *incomparable* if and only if $x \not\leq y$ and $y \not\leq x$. A *totally unordered* set in P is a subset in which every two different elements are incomparable. We denote the cardinal number of a set S by $|S|$.

Dilworth [1] has proved the following well-known decomposition theorem.

THEOREM 1 (DILWORTH). *Let P be a partially ordered set, and suppose that n is a positive integer such that*

$$n = \max \{ |A| : A \text{ is a totally unordered subset of } P \}.$$

Then there is a decomposition \mathfrak{D} of P with $|\mathfrak{D}| = n$.

It is natural to ask whether, in this theorem, the positive integer n may be replaced by an infinite cardinal number. However, the theorem is no longer valid in this case, as is shown by an example in [3] which is due in essence of Sierpinski [2]. In this example P is a set of pairs which represents a 1-1 mapping from ω_1 , the first uncountable ordinal, into the real numbers. $(x_1, y_1) \leq (x_2, y_2)$ is defined by: $x_1 \leq x_2$ (as ordinals) and $y_1 \leq y_2$ (as real numbers). The purpose of this note is to show that a similar idea leads, given any infinite cardinal k , to