



## A Limit of Periods: 10603

Yury J. Ionin; Robin R. Lewis

*The American Mathematical Monthly*, Vol. 106, No. 6. (Jun. - Jul., 1999), p. 590.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9890%28199906%2F07%29106%3A6%3C590%3AALOP1%3E2.0.CO%3B2-Q>

*The American Mathematical Monthly* is currently published by Mathematical Association of America.

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. 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/journals/maa.html>.

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.

---

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

*Editorial comment.* Other solvers used generating functions, inductive arguments, and various identities and transformations. Joe Howard and Heinz-Jürgen Seiffert independently observed that the result follows fairly quickly from a result proved by the proposer in his solution to Problem 4427, *School Science and Mathematics* 95 (1995) 221.

Solved also by E. S. Andersen & M. E. Larsen (Denmark), J. C. Binz (Switzerland), P. Bracken, D. Bradley (Canada), E. Braune (Austria), D. Callan, R. J. Chapman (U. K.), D. A. Darling, V. Dwivedi (India), E. Hertz, M. Hoffman, J. Howard, A. Kaplan (France), A. A. Kelzon (Russia), R. A. Kopas, O. Krafft & M. Schaefer (Germany), J. H. Lindsey II, J. Lorch, P. McCartney, D. K. Nester, A. Pechtl (Germany), F. Qi (China), E. Schmeichel, L. Scribani (South Africa), H.-J. Seiffert (Germany), A. Sinefakopoulos (Greece), I. Sofair, R. Sprugnoli (Italy), A. Stadler (Switzerland), A. Stenger, J. Van hamme (Belgium), M. Vowe (Switzerland), Z. Wu, GCHQ Problems Group (U. K.), WMC Problems group, and the proposer.

### A Limit of Periods

**10603** [1997, 567]. *Proposed by Yury J. Ionin and Robin R. Lewis, Central Michigan University, Mt. Pleasant, MI.* Let  $a$ ,  $b$ , and  $k$  be positive integers, and let  $P_k(a, b)$  be the period of the sequence  $\{a^n \bmod b^k\}_{n=1}^{\infty}$ . Find  $\lim_{k \rightarrow \infty} P_{k+1}(a, b)/P_k(a, b)$ .

*Solution by the proposers.* The limit equals the largest divisor of  $b$  that is relatively prime to  $a$ .

Suppose first that  $a$  and  $b$  are relatively prime. Fixing  $a$  and  $b$ , let  $P_k = P_k(a, b)$ . We have  $a^{P_k} \equiv 1 \pmod{b^k}$ , so  $a^{P_k} = 1 + q_k b^k$  for some integer  $q_k$ . Note that  $P_k$  divides  $P_{k+1}$ . Thus  $P_{k+1} = u_k P_k$ , where  $u_k$  is the smallest positive integer  $u$  such that  $a^{u P_k} \equiv 1 \pmod{b^{k+1}}$ . Since

$$a^{u P_k} = (1 + q_k b^k)^u \equiv (1 + u q_k b^k) \pmod{b^{k+1}},$$

we have  $u_k = b/d_k$ , where  $d_k = \gcd(q_k, b)$ . Thus  $P_{k+1} = b P_k / d_k$ .

If  $k \geq 2$ , then the equalities  $a^{P_{k+1}} = 1 + q_{k+1} b^{k+1} = (1 + q_k b^k)^{b/d_k}$  imply that  $q_{k+1} = (q_k/d_k) + t_k q_k^2/b$ , where  $t_k$  is an integer. Therefore, if  $p$  is a common prime divisor of  $b$  and  $q_k$ , then  $p$  occurs in the prime factorization of  $q_{k+1}$  with an exponent smaller than its exponent in the prime factorization of  $q_k$ . If  $p$  is a prime divisor of  $b$  that does not divide  $q_k$ , then  $p$  also does not divide  $q_{k+1}$ . If  $k$  is sufficiently large, this implies that  $q_k$  and  $b$  are relatively prime, so  $d_k = 1$  and  $P_{k+1} = b P_k$ . It follows that the desired limit is  $b$ .

Suppose now that  $a$  and  $b$  are not relatively prime. Let  $r$  be the largest divisor of  $b$  that is relatively prime to  $a$ , and let  $b = rs$ . Now  $P_k(a, b)$  is a period of the sequence  $\{a^n \bmod r^k\}_{n=1}^{\infty}$ , and thus  $P_k(a, r)$  divides  $P_k(a, b)$ .

On the other hand, consider the expression  $a^{P_k(a, r)+m} - a^m$ . This is divisible by  $r^k$ , and for large  $m$  it is divisible by  $s^k$ . Since  $\gcd(r, s) = 1$ , it must therefore be divisible by  $b^k$ , and we discover that  $P_k(a, r)$  is a period of the sequence  $\{a^n \bmod b^k\}_{n=1}^{\infty}$ . Hence  $P_k(a, b)$  divides  $P_k(a, r)$ . We conclude that  $P_k(a, b) = P_k(a, r)$ . Since  $a$  and  $r$  are relatively prime, the claim follows from the previous case.

Solved also by D. A. Callan, R. J. Chapman (U. K.), J. H. Lindsey II, A. N. 't Woord (The Netherlands), GCHQ Problems Group, and NCCU Problems Group.

### Avoiding the Identity

**10606** [1997, 664]. *Proposed by Thomas Zaslavsky, Binghamton University, Binghamton, NY.* Given a positive integer  $m$ , show that there is a positive integer  $n$  such that, for every group  $G$  of order at least  $n$ , it is possible to choose  $m$  elements  $g_1, g_2, \dots, g_m$  so that no product of the form  $g_{i_1}^{\pm 1} g_{i_2}^{\pm 1} \dots g_{i_k}^{\pm 1}$  with  $1 \leq k \leq m$  and distinct subscripts  $i_1, i_2, \dots, i_k$  in  $\{1, 2, \dots, m\}$  equals the identity.

*Solution by Stephen M. Gagola, Jr., Kent State University, Kent, OH.* Let a signed product be a product of distinct group elements or their inverses in a specified order. A set  $S$  is *admissible* if the identity is not expressible as a signed product of elements of  $S$ . We prove