Avoiding the Identity: 10606

Thomas Zaslavsky; Stephen M. Gagola, Jr.

The American Mathematical Monthly, Vol. 106, No. 6. (Jun. - Jul., 1999), pp. 590-591.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28199906%2F07%29106%3A6%3C590%3AATI1%3E2.0.CO%3B2-8

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.

http://www.jstor.org
Sat Dec 22 05:29:17 2007

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 $\lim_{k\to\infty} P_{k+1}(a, b)/P_k(a, b)$.

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 $a^{P_k} \equiv 1 \bmod b^k$, 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 $a^{uP_k} \equiv 1 \bmod b^{k+1}$. Since

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

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

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 $P_{k+1} = bP_k$. 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 $g_1, g_2, \ldots, g_m$ so that no product of the form $g_{i_1}^{\pm 1} g_{i_2}^{\pm 1} \cdots g_{i_k}^{\pm 1}$ with $1 \leq k \leq m$ and distinct subscripts $i_1, i_2, \ldots, i_k$ in $\{1, 2, \ldots, m\}$ 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 that every group of order at least $f(m) = \lceil 2^{m-1}(m-1)!\sqrt{e}\,\rceil$ has an admissible subset of size m.

For $S \subseteq G$, let S^* be the set of signed products of elements of S. Let $g(m) = f(m+1)-2$. When $|S| = m$, we claim that $|S^*| \le g(m)$. A signed product is formed by choosing an ordered nonempty subset of S with exponents ± 1. Thus $|S^*| \le \sum_{k=1}^{m} \binom{m}{k} k! 2^k$. We can rewrite the bound as $2^m m! T_{m-1}(1/2)$, where $T_{m-1}(x) = \sum_{j=0}^{m-1} x^j/j!$ is the Maclaurin polynomial of degree $m-1$ for e^x. The next term in the series expansion of $2^m m! e^{1/2}$ contributes 1, while the remainder after that is at most 1. Thus $|S^*| \le f(m+1) - 2$.

Note that S^* and $G - S^*$ are closed under taking inverses. If a signed product equals the identity, then each of its elements can be expressed as a signed product of the other elements in the product. If S is admissible and x is a nonidentity element of $G - S^*$, it therefore follows that $S \cup \{x\}$ is also admissible. Thus S can be enlarged until $G - S^*$ contains only the identity element.

We now use induction on m to prove the claim that every group of order at least $f(m)$ has an admissible subset of size m. When $m = 1$, every nontrivial group has a nonidentity element, and this forms an admissible set of size 1. This agrees with $f(1) = 2$. When $m > 1$, the monotonicity of f and the induction hypothesis imply that every group of order at least $f(m)$ has an admissible subset S of size $m-1$. Since $g(m-1) = f(m) - 2$, there is a nonidentity element in $G - S^*$, and S can be enlarged by one element.

Solved also by P. J. Anderson (Canada), R. Barbara (France), D. Beckwith, G. L. Body (U. K.), R. J. Chapman (U. K.), J. H. Lindsey II, S. C. Locke, J. Merickel, K. A. Ross, M. C. Slattery, GCHQ Problems Group (U. K.), NCCU Problems Group, NSA Problems Group, and the proposer.

Some Sums Require Care

10638 [1998, 69]. *Proposed by Brian Conolly, Cambridge, U. K.* For $0 \le \lambda \le 1$ and $m \ge 0$, let $S_m(\lambda) = \sum_{n\ge 1} e^{-\lambda n}(\lambda n)^{n-m}/n!$. Show that $S_0(\lambda) = \lambda/(1-\lambda)$, $S_1(\lambda) = 1$, $S_2(\lambda) = 1/\lambda - 1/2$, and $S_3(\lambda) = 1/\lambda^2 - 3/(4\lambda) + 1/6$.

Solution I by Allen Stenger, Tustin, CA. Let

$$T_m(\lambda) = \lambda^m S_m(\lambda) = \sum_{n\ge 1} \frac{(\lambda e^{-\lambda})^n n^{n-m}}{n!}.$$

By Stirling's formula the summand is asymptotic to $(2\pi)^{-1/2} n^{-m-1/2}(\lambda e^{1-\lambda})^n$. Thus, this sum converges absolutely for $|\lambda e^{1-\lambda}| < 1$. Therefore it represents a continuous function on $[0, 1)$. Furthermore, if $m \ge 1$, it converges uniformly for $|\lambda e^{1-\lambda}| \le 1$ and therefore is continuous on $[0, 1]$. For $m = 0$ it diverges at $\lambda = 1$.

First consider the case $m = 1$. We want to show that $\sum_{n\ge 1} (\lambda e^{-\lambda})^n n^{n-1}/n! = \lambda$. Euler showed that this holds for $0 \le \lambda \le 1$. It can be derived by applying the Lagrange inversion formula to $\lambda e^{-\lambda}$ (G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, Volume 1, Springer, 1972, Part 3, Exercise 209).

The formulas for other values of m can be derived from the case $m = 1$ by integration or differentiation. Observe that $T_m(0) = 0$ and that by uniform convergence

$$\begin{aligned}\frac{d}{d\lambda} T_m(\lambda) &= \frac{d}{d\lambda} \sum_{n\ge 1} \frac{\lambda^n e^{-n\lambda} n^{n-m}}{n!} \\ &= \sum_{n\ge 1} \frac{\lambda^{n-1} e^{-n\lambda} n^{n-(m-1)}}{n!} - \sum_{n\ge 1} \frac{\lambda^n e^{-n\lambda} n^{n-(m-1)}}{n!} = \frac{1-\lambda}{\lambda} T_{m-1}(\lambda),\end{aligned}$$