An Application of Fermat's Little Theorem: 11054
Author(s): Shahin Amrabov and Bernard M. Abrego
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/30037588
Accessed: 24/03/2010 21:28

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=maa.

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.

Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to The American Mathematical Monthly.
Modular Sequences Defined by Polynomials

11047 [2003, 956]. Proposed by Syros Marivani, Louisiana State University at Alexandria, Alexandria, LA. For integers $a, b, c,$ and $d,$ define a sequence $(f_n)$ by $f_n = af_{n-1} + bf_{n-2}$ for $n \geq 2,$ with $f_0 = c$ and $f_1 = d.$ Let $p$ be a prime. Find polynomial expressions $R, N,$ and $D$ in $a, b, c,$ and $d$ such that modulo $p$:

1. If $a^2 + 4b$ is a quadratic residue, then $f_p \equiv R(a, b, c, d);$
2. If $a^2 + 4b$ is a quadratic nonresidue, then $f_p \equiv N(a, b, c, d);$ and
3. If $p|(a^2 + 4b),$ then $f_p \equiv D(a, b, c, d).$

Solution by O. P. Lossers, Eindhoven University of Technology, Eindhoven, The Netherlands. For the special case $p = 2,$ we find $f_2 = ad + bc.$ For $p > 2,$ we work over $\mathbb{F}_p.$

In cases (1) and (2), $f_n = c_1\gamma^n + c_2\gamma^n,$ where $\gamma_1$ and $\gamma_2$ are the roots of the equation $x^2 = ax + b.$ In case (1), $\gamma_1$ and $\gamma_2$ are in $\mathbb{F}_p,$ so $\gamma_1^p = \gamma_1,$ and hence $f_p = f_1 = d = R(a, b, c, d).$ In case (2), $\gamma_1$ and $\gamma_2$ are in $\mathbb{F}_p \setminus \mathbb{F}_p$ and are conjugate, so $\gamma_1^p = \gamma_2$ and $\gamma_2^p = \gamma_1.$ Hence $f_p = c_1\gamma_2 + c_2\gamma_1.$ Using $c_1\gamma_1 + c_2\gamma_2 = d$ and $(c_1 + c_2)(\gamma_1 + \gamma_2) = ca,$ we obtain $f_p = ca - d = N(a, b, c, d).$

In case (3), $f_n = (c_1 + nc_2)\gamma^n,$ where $\gamma$ is the double root of $x^2 = ax + b,$ with $\gamma = a/2.$ Substitution yields $f_p = c_1\gamma = ca/2 = D(a, b, c, d).$

An Application of Fermat’s Little Theorem

11054 [2004, 64]. Proposed by Shahin Amrabov, ARI College, Ankara, Turkey. Determine the set of all solutions in integers to


Composite solution by Bernard M. Abrego, California State University, Northridge, CA and Pál Péter Dályay, Szeged, Hungary. There are no solutions in integers. Suppose that $(x, y)$ is such a solution. Since 1997 is prime, Fermat’s Little Theorem gives $x^{1997} \equiv x \pmod{1997}$ and $y^{1997} \equiv y \pmod{1997}.$ Hence $x^{1998} \equiv x^2 \pmod{1997}$ and $y^{1998} \equiv y^2 \pmod{1997}.$ Considering the given equation modulo 1997, we obtain

\[ x^2 + 0 - 2 - x^2 \equiv y^4 - 4y^3 + 6y^2 - 4y \pmod{1997}, \]

which simplifies to $-1 \equiv (y - 1)^4 \pmod{1997}.$ In particular, $y - 1$ is relatively prime to 1997. By Fermat’s Little Theorem, $(y - 1)^{1996} \equiv 1 \pmod{1997}.$ On the other hand, raising both sides of (1) to the power 499 yields $-1 \equiv (y - 1)^{1996} \pmod{1997}.$ Since these last two congruences are contradictory, the result follows.

Also solved by S. Amghibech (Canada), M. A. Carlton, W. C. Chu (Italy), K. T. Dale (Norway), R. S. Garibaldi, M. Goldenberg & M. Kaplan, S. Y. Jeon (Korea), C. H. Kwack (Korea), O. P. Lossers (Netherlands), S. Namli, M. Reid, A. E. Stadler (Switzerland), L. Zhou, the GCHQ Problem Solving Group (U. K.), the NSA Problems Group, and the proposer.