Also solved by B. M. Ábrego , S. Amghibech (Canada), F. Boca, R. Chapman (U. K.), O. P. Lossers (Netherlands), B. Mixon, V. Pambuccian, A. Stadler (Switzerland), R. Tauraso (Italy), L. Zhou, BSI Problems Group (Germany), Szeged Problem Solving Group "Fejéntaláltuka" (Hungary), and NSA Problems Group.

Modular Sequences Defined by Polynomials

11047 [2003, 956]. *Proposed by Syrous Marivani, Louisiana State University at Alexandria, Alexandria, LA.* For integers a, b, c, and d, define a sequence $\langle f_n \rangle$ 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), $f_n = c_1\gamma_1^n + c_2\gamma_2^n$, where γ_1 and γ_2 are the roots of the equation $x^2 = ax + b$. In case (1), γ_1 and γ_2 are in $\mathbb{F}_p$, so $\gamma_i^p = \gamma_i$, and hence $f_p = f_1 = d = R(a, b, c, d)$. In case (2), γ_1 and γ_2 are in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ 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 γ is the double root of $x^2 = ax + b$, with $\gamma = a/2$. Substitution yields $f_p = c_1\gamma = ca/2 = D(a, b, c, d)$.

Also solved by B. S. Burdick, R. Chapman (U. K.), P. P. Dályay (Hungary), A. Nakhash, N. C. Singer, A. Stadler (Switzerland), R. Stong, C. Wengchang & D. C. L. Veliana (Italy), BSI Problems Group (Germany), GCHQ Problem Solving Group (U. K.), NSA Problems Group, and the proposer.

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

$$1998^2x^2 + 1997x + 1995 - 1998x^{1998} = 1998y^4 + 1993y^3 - 1991y^{1998} - 2001y.$$

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.