triangle ABC; similarly K belongs to the three other ninepointcircles. The four of them will then have K as their common point.

COROLLARY. *The orthopole is the circumcenter of the ninepoint-quadrilateral.*

The four ninepointcircles have the same radius, half the circumradius of the quadrilateral. Half the circumradius of the quadrilateral is also the circumradius to the ninepoint-quadrilateral, according to our Theorem III. Its circumcenter is therefore $\frac{1}{2}R$ (R the circumradius of the quadrilateral) away from the points N_A, N_B, N_C, N_D. And Theorem V here says that these four points are at that distance from K.

Note 1. Two by two the ninepointcircles have a second common point, the ${}_4C_2=6$ midpoints of the sides of the quadrilateral.

Note 2. K is not only common to the four ninepointcircles of the original quadrilateral $ABCD$, but also to the ninepointcircles of the ortho-quadrilateral. But the same must be said for all the pairs of quadrilaterals of Theorem II. Hence there would be 32 ninepointcircles, but Lemma 1b reduces this number to one quarter of it: for the same ninepointcircle (as on the fig.) serves for four triangles, scattered over the four pairs. Hence there will be only eight ninepointcircles, the original ones of pair (1).

To summarize we can say that the ninepointcircle becomes a tenpointcircle thanks to an eightcirclepoint.

The author wishes to thank the referee for valuable suggestions.

Reference

1. Solution of Problem E1740, Four concyclic points, this MONTHLY, 72(1965) 1026.

A NOTE ON LINEAR RECURRENT SEQUENCES MODULO m

D. W. ROBINSON, Brigham Young University

A linear recurrent sequence of integers modulo m is periodic. (See for example [**1**, **6**].) The particular case of the Fibonacci sequence was discussed recently in this MONTHLY, (see [**3**, **5**]). In this note we generalize the results of [**3**], using essentially the notation of [**5**].

Let (u): $u_0, u_1, \cdots, u_n, \cdots$ be the Lucas' sequence of degree r associated with the characteristic polynomial

$$f(x) = x^r - a_1x^{r-1} - \cdots - a_r,$$

where $a_1, \cdots, a_r$ are integers and $a_r \neq 0$. That is, (u) is the sequence of integers that satisfy the linear recurrence

$$u_{n+r} = a_1u_{n+r-1} + \cdots + a_ru_n$$

for $n \geqq 0$ with $u_0=0, \cdots, u_{r-2}=0$, $u_{r-1}=1$. (For $r=1$ it is understood that

$u_0=1$.) Also, let m be a positive integer which is relatively prime to a_r. The least positive integer k such that $u_k\equiv 0, \cdots, u_{k+r-2}\equiv 0, u_{k+r-1}\equiv 1 \pmod{m}$ is called the period $k(m)$ of (u) modulo m, and the least positive integer d such that $u_d\equiv 0, \cdots, u_{d+r-2}\equiv 0 \pmod{m}$ is called the restricted period $d(m)$ of (u) modulo m. (See for example [**1**, **6**].)

The existence of the period, and thus the restricted period, may be established as follows. Let

$$A=\begin{bmatrix} 0 & \cdots & 0 & a_r \\ 1 & \cdots & 0 & a_{r-1} \\ & \cdots & & \\ 0 & \cdots & 1 & a_1 \end{bmatrix}$$

be the companion matrix of $f(x)$, and let U_n be the row matrix $[u_n, \cdots, u_{n+r-1}]$, $n=0, 1, \cdots$. Clearly $U_n=U_0A^n$. Since the integers modulo m form a finite system, there exist k and n such that A^{k+n} is congruent (elementwise) to A^n modulo m with $k+n>n\geqq 0$. In fact, since $\det A=(-1)^{r-1}a_r$ is a unit modulo m, A^k is congruent to the identity matrix I modulo m. Consequently, $U_k\equiv U_0 \pmod{m}$, which provides the conclusion, (see also [**2**, **4**]).

The results of this note depend upon the following

LEMMA. *Let (u) be the Lucas' sequence of degree r associated with the polynomial $f(x)$ above, and let m be a positive integer which is relatively prime to a_r. Let $k(m)$ and $d(m)$ be the period and the restricted period of (u) modulo m, and let $s(m)$ be the order of the unit $(-1)^{r-1}a_r$ modulo m. Then $u_{d(m)+r-1}$ is a unit modulo m of order $k(m)/d(m)$, and $k(m)/d(m)$ divides $r\cdot s(m)$.*

Proof. We first show that the period $k(m)$ of (u) modulo m is precisely the order modulo m of the matrix A above. Indeed, suppose $U_k\equiv U_0 \pmod{m}$ and let M_n be the r-by-r matrix with U_{n+i-1} for its ith row. Since $U_{k+i}\equiv U_i \pmod{m}$, it follows that $M_k=M_0A^k\equiv M_0 \pmod{m}$. But, since $\det M_0=(-1)^{r-1}$, M_0 is a unit and $A^k\equiv I \pmod{m}$. That is, $A^k\equiv I \pmod{m}$ if and only if $U_k\equiv U_0 \pmod{m}$. Consequently, $k(m)$ is the order of A modulo m.

We may prove in a similar manner that $A^d\equiv tI \pmod{m}$ if and only if $U_d\equiv tU_0 \pmod{m}$, where t is some integer. Thus the restricted period $d(m)$ generates the ideal of all d such that A^d is a scalar matrix modulo m. In particular, $d(m)\mid k(m)$. Also, since $U_0=[0, \cdots, 0, 1]$, if $U_d\equiv tU_0 \pmod{m}$ then $t\equiv u_{d+r-1} \pmod{m}$. Therefore,

$$A^{d(m)}\equiv u_{d(m)+r-1}I \pmod{m},$$

and it follows that $u_{d(m)+r-1}$ is a unit modulo m of order $k(m)/d(m)$. Finally, if $s(m)$ is the order of $\det A=(-1)^{r-1}a_r$ modulo m, then

$$1\equiv(\det A)^{s(m)\cdot d(m)}\equiv(\det A^{d(m)})^{s(m)}\equiv(u_{d(m)+r-1})^{r\cdot s(m)} \pmod{m}.$$

That is, the order of $u_{d(m)+r-1}$ modulo m divides $r\cdot s(m)$.

We now extend the first theorem of [3].

THEOREM. *Let the notation and conditions be as in the lemma. If p is a prime such that $p \nmid a_r$, then $k(p^e)=k(p)$ implies $d(p^e)=d(p)$.*

Proof. Since $A^{k(p)}=I+pB$ for some matrix B, it is clear that

$$A^{p^{e-1}k(p)} \equiv I \pmod{p^e}.$$

That is, $k(p^e)\,|\,p^{e-1}k(p)$. But it is obvious that $k(p)\,|\,k(p^e)$. Hence, $k(p^e)/k(p)$ is some nonnegative power of p. Similarly, $d(p^e)/d(p)$ is a nonnegative power of p. Also, since the unit group of integers modulo p is of order $p-1$, it follows by the first conclusion of the lemma that $k(p)/d(p)$ divides $p-1$. Thus, $p \nmid k(p)/d(p)$ and the theorem is a consequence of the fact that

$$\frac{d(p^e)}{d(p)}\cdot\frac{k(p^e)}{d(p^e)} = \frac{k(p^e)}{k(p)}\cdot\frac{k(p)}{d(p)}\,.$$

A corollary of these results is that if $p \nmid a_r$ and $k(p^e)=k(p)$, then $u_{d(p)+r-1}$ has the same order modulo p and modulo p^e. Indeed, we have the following generalization of the second theorem of [3].

COROLLARY 1. *Let the notation and conditions be as in the lemma. If p is a prime such that $p \nmid a_r$ and e is a positive integer such that $d(p^e)=d(p)$, then $k(p^e)=k(p)$ if and only if $u_{d(p)+r-1}$ has the same order modulo p and modulo p^e.*

Furthermore, by the final conclusion of the lemma, it is immediate that we also have the following

COROLLARY 2. *Let the notation and conditions be as in the lemma and let $a_r=\pm 1$. If p is a prime such that $p \nmid 2r$, then $k(p^e)/d(p^e)=k(p)/d(p)$ for every positive integer e.*

If $a_r=(-1)^{r-1}$ in this corollary, then it is sufficient to require only $p \nmid r$. This condition is necessary, however, as shown by the following example. If $f(x)=x^3-x^2-x-1$ and $p=3$, then $k(3)=d(3)=d(3^2)=13$, but $k(3^2)=39$.

This paper was written while the author was on sabbatical leave at the California Institute of Technology, where he was supported in part by the National Science Foundation.

References

1. R. D. Carmichael, On sequences of integers defined by recurrence relations, Quart. J. Math., 48 (1920) 343–372.

2. E. C. Dade, D. W. Robinson, O. Taussky, and M. Ward, Divisors of recurrent sequences, J. Reine Angew. Math., 214/215 (1964) 180–183.

3. S. E. Mamangakis, Remarks on the Fibonacci series modulo *m*, this MONTHLY, 68 (1961) 648–649.

4. D. W. Robinson, The Fibonacci matrix modulo *m*, The Fibonacci Quart., 1 (1963) 29–36.

5. D. D. Wall, Fibonacci series modulo *m*, this MONTHLY, 67 (1960) 525–532.

6. M. Ward, The characteristic number of a sequence satisfying a linear recursion relation, Trans. Amer. Math. Soc., 33 (1931) 153–165.