DIVISORS OF SECOND-ORDER SEQUENCES*

BY MARSHALL HALL

1. *Introduction.* Given a recurrence of second order

$$u_{n+2} = au_{n+1} - bu_n, \tag{1}$$

where a and b are integers, and the initial values u_0, u_1 (integers) are terms of a sequence (u_n) satisfying (1), it is an interesting problem to determine whether or not a given prime p will divide some u_n of the sequence. Morgan Ward† reduced this problem to the standard problem on recurrences of determining the restricted periods modulo p of (1) and an auxiliary recurrence of second order. His method is somewhat indirect and uses the assumption that μ, the restricted period of (1) modulo p, is even. This paper obtains a similar reduction of the problem by a somewhat more direct method and makes no assumption on μ.

2. *Some Exceptional Cases.* The appearance of p as a divisor of some u_n evidently depends solely upon the values of a, b, u_0, u_1, modulo p. If p stands in certain relations to these numbers, the theory of the sequence (u_n) modulo p is different from the general theory. It is convenient to treat these unusual cases separately, and then exclude them from further consideration.

CASE 1. $p \mid a,\ p \mid b$.

Here $p \mid u_n$ for $n \geqq 2$.

CASE 2. $p \nmid a,\ p \mid b$.

Here $u_n \equiv a^{n-1}u_1 \pmod{p}$ for all $n \geqq 2$. Hence either p divides all u_n for $n \geqq 1$ or none.

CASE 3. $p \mid a,\ p \nmid b$.

Here $u_{2n} \equiv (-b)^n u_0$, $u_{2n+1} \equiv (-b)^n u_1(p)$; and p divides all or none of u_{2n}, and all or none of u_{2n+1}.

CASE 4. $p \nmid a,\ p \nmid b$, p divides either u_0 or u_1.

Then p divides either $u_{n\mu}$ or $u_{n\mu+1}$, where μ is the restricted period of (u_n) modulo p.

CASE 5. $p \mid (a^2-4b)$, $p \nmid a, b, u_0, u_1$.

Then p cannot be 2 since $p \nmid a$. Let $a \equiv 2a' \pmod{p}$, then

* Presented to the Society, April 20, 1935.

† M. Ward, *An arithmetical property of recurring series of the second order*, this Bulletin, vol. 40 (1934), p. 825.