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.

$b \equiv a'^2 \pmod{p}$, and we consider $u_{n+2} = 2a'u_{n+1} - a'^2 u_n$, giving $u_n = a'^{n-1}(a'u_0 + (u_1 - a'u_0)n)$. Now $a'u_0 \not\equiv 0 \pmod{p}$. Hence u_n can be divisible by p if $u_1 - a'u_0 \not\equiv 0 \pmod{p}$, but not if $u_1 - a'u_0 \equiv 0 \pmod{p}$, that is, if $2u_1 - au_0 \equiv 0 \pmod{p}$.

CASE 6.

$$p \mid \begin{vmatrix} u_0 & u_1 \\ u_1 & u_2 \end{vmatrix} = -u_1^2 + au_1u_0 - bu_0^2, \qquad p \nmid u_0, u_1.$$

Here

$$\frac{u_0}{u_1} \equiv \frac{u_1}{u_2} \equiv s \not\equiv 0 \pmod{p} \qquad \text{and} \qquad u_n \equiv s^n u_0 \pmod{p},$$

and u_n is never divisible by p.

3. *The General Case.* The characteristic polynomial of (1), $f(x) = x^2 - ax + b = (x - \alpha_1)(x - \alpha_2)$, has distinct roots, since p does not divide the discriminant $(\alpha_2 - \alpha_1)^2 = a^2 - 4b$. Hence we may write

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n, \quad \text{where } c_1 = \frac{u_0\alpha_2 - u_1}{\alpha_2 - \alpha_1}, \quad c_2 = \frac{u_1 - u_0\alpha_1}{\alpha_2 - \alpha_1}.$$

In the field $K(\alpha_1)$, which is either the rational or a quadratic field, the conjugate α_2 is included as $\alpha_2 = a - \alpha_1$. In this field let P be a prime ideal dividing p. Now

$$N(P) = p^2 \quad \text{if} \quad \left(\frac{a^2 - 4b}{p}\right) = -1, \quad \text{and}$$

$$N(p) = p \quad \text{if} \quad \left(\frac{a^2 - 4b}{p}\right) = +1.$$

We note that in this field P does not divide either α_1 or α_2 as p does not divide $\alpha_1\alpha_2 = b$, nor does P divide either the numerator or denominator of c_1 or c_2, as p does not divide $(\alpha_2 - \alpha_1)^2 = a^2 - 4b$ or $(u_1 - u_0\alpha_1)(u_0\alpha_2 - u_1) = -u_1^2 + au_1u_0 - bu_0^2$. This will permit us to take indices of these quantities with respect to a primitive root modulo P.

LEMMA. *μ has the value* $(N(P) - 1)/(\text{Ind } (\alpha_1/\alpha_2),\ N(P) - 1)$.

It is well known that μ is the rank of apparition of p in the sequence $u_n = (\alpha_1^n - \alpha_2^n)/(\alpha_1 - \alpha_2)$, that is, the least positive n for which $u_n \equiv 0 \pmod{p}$. For this it is sufficient that $u_n \equiv 0 \pmod{P}$, since a rational number divisible by P is also divisible by p.

This yields $\alpha_1^n \equiv \alpha_2^n \pmod{P}$, whence taking indices, $n\text{Ind}\ \alpha_1 \equiv n\text{Ind}\ \alpha_2 (\text{mod}\ (N(P)-1))$, or $n\text{Ind}\ (\alpha_1/\alpha_2) \equiv 0 (\text{mod}(N(P)-1))$. The least positive value of n that satisfies this condition is $(N(P)-1)/(\text{Ind}(\alpha_1/\alpha_2),\ N(P)-1)$, and consequently μ must have this value.

THEOREM. *The number p will divide some u_n of the sequence (u_n) satisfying (1) if and only if μ, the restricted period of (1), divides M, the restricted period of*

$$U_{n+2} = (au_0 - 2u_1)U_{n+1} - (u_1^2 - au_1u_0 + bu_0^2)U_n.$$

If $c_1\alpha_1^n + c_2\alpha_2^n \equiv 0 \pmod{P}$, then

$$n\text{Ind}\left(\frac{\alpha_1}{\alpha_2}\right) \equiv \text{Ind}\left(\frac{-c_2}{c_1}\right) (\text{mod}\ (N(P) - 1)),$$

and conversely. Now a congruence $An \equiv B \pmod{C}$ has a solution n if and only if $(A,\ C) \mid (B,\ C)$. This becomes

$$\left(\text{Ind}\left(\frac{\alpha_1}{\alpha_2}\right), N(P) - 1\right) \Bigg| \left(\text{Ind}\left(\frac{-c_2}{c_1}\right), N(P) - 1\right).$$

By the lemma

$$\left(\text{Ind}\left(\frac{\alpha_1}{\alpha_2}\right), N(P) - 1\right) = \frac{N(P) - 1}{\mu}.$$

The lemma also yields

$$\left(\text{Ind}\left(\frac{-c_2}{c_1}\right), N(P) - 1\right) = \frac{N(P) - 1}{M},$$

since $-c_2/c_1 = (u_0\alpha_2 - u_1)/(u_0\alpha_1 - u_1)$, and $u_0\alpha_1 - u_1$ and $u_0\alpha_2 - u_1$ are the roots of $x^2 - (au_0 - 2u_1)x + (u_1^2 - au_1u_0 + bu_0^2) = 0$, which is the characteristic of the recurrence for U_n. By substitution we obtain as a necessary and sufficient condition that p divide some u_n:

$$\frac{N(P) - 1}{\mu} \Bigg| \frac{N(P) - 1}{M} \qquad \text{or} \qquad M \mid \mu.$$

We note that the exceptional cases are those in which p divides any one of u_0, u_1, the coefficients of the two recurrences, and the discriminant of (1).

YALE UNIVERSITY