THE LAW OF REPETITION OF PRIMES IN AN ELLIPTIC DIVISIBILITY SEQUENCE

By Morgan Ward

1. Let

$$(U): \qquad U_n = (\alpha^n - \beta^n)/(\alpha - \beta) \qquad (n = 0, 1, \cdots)$$

be the Lucas sequence formed on the roots α and β of the polynomial $x^2 - Px + Q$ where P and Q are rational integers. (This last restriction may be weakened (see Lehmer [1]). If $\alpha = \beta$, we define U_n to be $n\alpha^{n-1}$.) Among the many arithmetical properties of (U) discovered by Lucas [2], [3], there are two which are of fundamental importance. The first property is Lucas' "law of apparition" of primes in (U). (We formulate Lucas' result in such a manner that it will apply to the more general elliptic sequences considered later.)

If p is a prime not dividing both of the initial values U_3 and U_4 of (U), then there exists a number $\rho = \rho(p)$ such that $U_n \equiv 0 \pmod p$ if and only if $n \equiv 0 \pmod \rho$.

ρ is called the rank of apparition, or simply the rank, of p in (U). It divides $p - (D/p)$ where D is the discriminant of $x^2 - Px + Q$, so that $\rho(p) \leq p + 1$.

The second property is the "law of repetition" of primes in (U) (see Lehmer [1] for a proof).

If ρ is the rank of a prime p in (U) not dividing both U_3 and U_4 and p^k is the highest power of p which divides U_ρ, then the rank of apparition of p^n in (U) is ρ or $p^{n-k}\rho$ according as $n \leq k$ or $n \geq k$.

k is usually one. It is easily seen that p^k is the highest power of p dividing $U_{p-(D/p)}$. Hence the determination of when k is greater than one is a generalization of the problem of finding when the quotient of Fermat $(c^{p-1} - 1)/p$ is divisible by p.

2. I have recently studied the arithmetical properties of a class of elliptic sequences which includes Lucas' sequences as a special case. (See [4]. The type of sequence considered in this paper is called a "general" elliptic divisibility sequence in [4].) An elliptic sequence (h): $h_0, h_1, h_2, \cdots, h_n$ is a particular solution of the functional equation

$$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2 \tag{2.1}$$

subject to the restrictions

$$h_0 = 0;\ h_1 = 1;\ h_2,\ h_3,\ h_4 \text{ rational integers;} \tag{2.2}$$

$$h_2 h_3 \neq 0; \tag{2.3}$$

$$h_2 \text{ divides } h_4. \tag{2.4}$$

Received May 17, 1948.