REMARKS ON THE FIBONACCI SERIES MODULO m

S. E. MAMANGAKIS, International Business Machines Corporation
Research Center, Yorktown Heights, N. Y.

In a recent paper D. D. Wall [1] was concerned with determining the length of the period of the recurring series obtained by reducing a Fibonacci series modulo m. In this paper we will use the same notation as in [1].

Thus, u_n denotes the Fibonacci series with $u_0=0$ and $u_1=1$, where $u_{n+1}=u_n+u_{n-1}$. Also, $k(m)$ denotes the length of the period of u_n mod m and as in [1] we let $m=p^e$, where p is a prime number. In [1] Wall poses a question that has so far remained unanswered: "The most perplexing problem we have met in this study concerns the hypothesis $k(p^2)\neq k(p)$. We have run a test on a digital computer which shows that $k(p^2)\neq k(p)$ for all p up to 10,000; however, we cannot yet prove that $k(p^2)=k(p)$ is impossible." This paper furnishes a proof of the hypothesis $k(p^2)\neq k(p)$ under certain mild conditions.

THEOREM 1. *If c and p are relatively prime and cp occurs in u_n, then $k(p^2)\neq k(p)$.*

Proof. Let $u_j=cp$ and consider the sequences

$$u_n, \text{ mod } p \text{ which we will denote by } {}_1u_n; \tag{1}$$

$$u_n, \text{ mod } p^2 \text{ which we will denote by } {}_2u_n \tag{2}$$

which begin, respectively, $0, 1, 1, 2, \cdots, {}_1u_{j-1}=Rp+Q, {}_1u_j=cp\equiv 0, {}_1u_{j+1}\equiv Q, \cdots \pmod p$ and $0, 1, 1, 2, \cdots, {}_2u_{j-1}=Rp+Q, {}_2u_j=cp\equiv cp, {}_2u_{j+1}\equiv(c+R)p+Q, \cdots \pmod{p^2}$, where $0<Q<p$. It can be shown by mathematical induction that

$$ {}_1u_{tj-1}\equiv Q^t, \qquad {}_1u_{tj}\equiv 0 \pmod p; \tag{3}$$

$$ {}_2u_{tj-1}\equiv tRpQ^{t-1}+Q^t, \qquad {}_2u_{tj}\equiv ctpQ^{t-1} \pmod{p^2}. \tag{4}$$

To see that (4) holds, we note that for $t=1$, the formulas hold. Next, assume the formulas hold for $t\leqq i$, then ${}_2u_{ij-1}\equiv iRpQ^{i-1}+Q^i$ and ${}_2u_{ij}\equiv cipQ^{i-1} \pmod{p^2}$. Now consider the new sequence U_n with $U_0=iRpQ^{i-1}+Q^i\equiv{}_2u_{ij-1}$ and $U_1=cipQ^{i-1}\equiv{}_2u_{ij} \pmod{p^2}$. But, by the well-known formula for a Fibonacci series in [1], $f_n=u_nb+u_{n-1}a$, where $f_1=a$, $f_2=b$ and $f_{n+1}=f_n+f_{n-1}$, we have $U_j=u_j(cipQ^{i-1})+u_{j-1}(iRpQ^{i-1}+Q^i)$ or $U_j\equiv(i+1)RpQ^i+Q^{i+1}\equiv{}_2u_{(i+1)j-1} \pmod{p^2}$, and $U_{j+1}=u_{j+1}(cipQ^{i-1})+u_j(iRpQ^{i-1}+Q^i)$ or $U_{j+1}\equiv(i+1)cpQ^i\equiv{}_2u_{(i+1)j} \pmod{p^2}$. Hence (4) holds; and (3) is implied by (4).

We will, therefore, obtain in the series (1) $\cdots, {}_1u_{tj-1}\equiv Q^t, {}_1u_{tj}\equiv 0 \pmod p$, and in (2) $\cdots, {}_2u_{tj-1}\equiv tRpQ^{t-1}+Q^t, {}_2u_{tj}\equiv ctpQ^{t-1} \pmod{p^2}$.

Now series (1) will first repeat when Q belongs to t mod p. (In other words t is the smallest number satisfying $Q^t\equiv 1$ mod p.) In this case, p^2 does not divide ${}_2u_{tj}\equiv ctpQ^{t-1}$ since t divides $p-1$, which means series (2) does not repeat with sequence (1). This proves our theorem.

THEOREM 2. *Let c and p be relatively prime, $e \leqq d$, and $u_j = cp^d$ be the first multiple of p to occur in u_n. Then $k(p^e) = k(p)$ if and only if u_{j-1} has the same order* mod p *and* mod p^e.

Proof. Since u_j is the first multiple of p to occur in u_n, the period of u_n mod p will be jt where u_{j-1} belongs to t mod p. But u_j is also the first multiple of p^e to occur in u_n and so its period is equal to js where u_{j-1} belongs to s mod p^e. Therefore if $k(p) = k(p^e)$ we have $k(p) = jt = js = k(p^e)$ which implies $t = s$. Conversely, under the same hypotheses, if u_{j-1} has the same order mod p and mod p^e it is obvious that $k(p^e) = k(p)$.

Remarks. In [2] Kraitchik has a table of u_n in their prime factorization for odd n up to $n = 129$, with a few missing entries, and none of the u_n listed satisfy the hypothesis of Theorem 2 for $1 < e \leqq d$ in this paper. Furthermore, I have computed all of the u_n up to $n = 50$ using Lehmer's prime and factor tables plus the tables in [2] as a check and, again, none of the u_n satisfy the hypothesis of our Theorem 2 for $1 < e \leqq d$. Could it be that the mild conditions of Theorem 1 are strong enough to apply to all prime numbers? That is to say, one would like to make Theorem 1 read: *If c and p are relatively prime, then cp occurs in u_n and $k(p^2) \neq k(p)$.*

References

1. D. D. Wall, Fibonacci series modulo m, this MONTHLY, vol. 67, 1960, pp. 525–532.
2. M. Kraitchik, Recherches sur la Théorie des Nombres, vol. 1, Paris, 1924, pp. 77–80.

NOTE ON THE DISTRIBUTIVE LAWS (Supplement)

TÔRU SAITÔ, Tokyo Gakugei University, Japan

J. L. Kelley [1] defines a ring to be a system which we called a c-ring in [2]. Then he defines a field to be a system which is a ring (in his sense) such that the set of all nonzero elements forms a multiplicative commutative group. In this supplementary note, we show that the definition of a field in Kelley's sense coincides with that in the ordinary sense.

We use terminologies and results in [2] freely.

We define a *w-division ring* (*c-division ring*) to be a w-ring (c-ring) F such that F has at least two elements and $F - \{0\}$ forms a multiplicative group. When the multiplicative group is commutative, it is called a *w-field* (*c-field*). Hence a field in Kelley's sense is a c-field in our definition.

THEOREM 1. *If a w-division ring F contains an element which is neither zero nor the defining element, then F is a division ring* (*in the ordinary sense*).

Proof. It suffices to show that F is a ring. By [2] Lemma 3, we have, in F, $e^2 = e$, where e is the defining element of F. If e were not 0, e would be an idempotent element of the multiplicative group $F^* = F - \{0\}$, and so e would be the identity element of F^*. Then for any $x \in F^*$, we have, using [2] Lemma 3 again,