LETTER TO THE EDITOR

February 15, 1974

Dear Dr. Hoggatt:

I have discovered the theorem below and was advised to forward it to you as being the most suitable publisher, should it turn out to be original.

Consider the function

$$F_x(n) = 1 + \sum_{i=1}^{i=\frac{2n+(-1)^{(n+1)}-3}{4}} \left\{ \left(\frac{x^i}{i!}\right) \prod_{j=i+1}^{j=2i} (n-j) \right\} .$$

We make the convention that $F_x(1) = 1$ for all x.

It is easily established that for all ℓ the coefficient of $x^{(\lambda-1)}$ in $F_x(n)$ added to the coefficient of x^{λ} in $F_x(n+1)$ gives the coefficient of x^{λ} in $F_x(n+2)$, and thus we have:

$$xF_x(n) + F_x(n+1) = F_x(n+2) .$$

$F_1(n)$ is the Fibonacci series.

Theorem. Any prime factor of $F_x(P)$, where P is prime, is congruent to ± 1 or 0 (mod P). (We assume $P \neq 2$ since if $P = 2$ the theorem is trivial.)

Lemma 1. For any ℓ,

$$(\ell+1)(\ell+2)\cdots(2\ell) = (2)(6)\cdots(4\ell-2) .$$

This is easily proved by induction.

Lemma 2. The coefficient of x^{ℓ} in $F_x(p)$ is congruent to the coefficient of x^{ℓ} in the binomial expansion of

$$\left[x + \left(\frac{p+1}{4}\right)\right]^{\left(\frac{p-1}{2}\right)} \pmod{p},$$

where p is prime, and $p \neq 2$.

Since $p \neq 2$, p is odd and $F_x(p)$ is of order

$$\frac{2p+(-1)^{p+1}-3}{4} = \left(\frac{p-1}{2}\right) \quad \text{in } x.$$

From Lemma 1 we have

$$\frac{(\ell+1)(\ell+2)\cdots(2\ell)}{\ell!} = \frac{(2)(6)\cdots(4\ell-2)}{\ell!} .$$

Thus

$$\frac{(p-(\ell+1))(p-(\ell+2))\cdots(p-2\ell)}{\ell!} \equiv \frac{(2p-2)(2p-6)\cdots(2p-(4\ell-2))}{\ell!} \equiv 4^{\ell}\,\frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-1\right)\cdots\left(\frac{p-1}{2}-(\ell-1)\right)}{\ell!}$$

(mod p). But

$$4^{\ell} \equiv \left(\frac{p+1}{4}\right)^{(-\ell)} \pmod{p}$$

and by Fermat's Theorem

$$\left(\frac{p+1}{4}\right)^{(p-1)} \equiv 1 \pmod{p},$$

moreover

$$\left(\frac{p+1}{4}\right)^{\left(\frac{p-1}{2}\right)} \equiv 1 \pmod p$$

since

$$\left(\frac{p+1}{4}\right)^{\left(\frac{p-1}{2}\right)} \equiv -1 \pmod p$$

would imply

$$\left(\frac{1}{4}\right)^{\left(\frac{p-1}{2}\right)} = 4^{\left(\frac{1-p}{2}\right)} \equiv -1 \pmod p$$

or

$$4^{\left(p-1-\left(\frac{1-p}{2}\right)\right)} \equiv -1 \pmod p,$$

applying Fermat's theorem again, and this gives

$$2^{(p-1)} \equiv -1 \pmod p$$

which is absurd since $p \neq 2$. Thus

$$4^{\lambda} \equiv \left(\frac{p+1}{4}\right)^{\left(\frac{p-1}{2}-\ell\right)} \pmod p,$$

and so:

$$\frac{(p-(\ell+1)(p-(\ell+2))\cdots(p-2\ell)}{\ell!} \equiv \left(\frac{p+1}{4}\right)^{\left(\frac{p-1}{2}-\ell\right)} \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-\ell\right)\cdots\left(\frac{p-1}{2}-(\ell-1)\right)}{\ell!}$$

$\pmod p$ which is equivalent to the lemma.

Lemma 3. $F_x(p) \equiv \pm 1$ or $0 \pmod p$, where p is prime and $p \neq 2$.

From Lemma 2, it follows that

$$F_x(p) \equiv \left(x + \frac{p+1}{4}\right)^{\left(\frac{p-1}{2}\right)} \pmod p.$$

Thus by Fermat's theorem, either

$$x \equiv -\left(\frac{p+1}{4}\right) \mod p$$

in which case $F_x(p) \equiv 0 \pmod p$, or

$$\left\{F_x(p)\right\}^2 - 1 \equiv 0 \pmod p$$

in which case $F_x(p) \equiv \pm 1 \pmod p$.

Lemma 4. $\left\{F_x(n)\right\}^2 - \left\{F_x(n-1)\right\}\left\{F_x(n+1)\right\} = -x^{(n-1)}$ for all n.

This is easily proved by induction on n using the relationship

$$xF_x(n) + F_x(n+1) = F_x(n+2).$$

Lemma 5. When $x \not\equiv 0 \pmod p$, at least one of $F_x(p)$, $F_x(p-1)$, $F_x(p+1)$ is congruent to $0 \pmod p$, where p is prime and $p \neq 2$.

It follows from Lemma 4, using Fermat's theorem, that

$$\left\{F_x(p)\right\}^2 - \left\{F_x(p-1)\right\} \cdot \left\{F_x(p+1)\right\} \equiv 1 \pmod p.$$

Thus if $F_x(p) \not\equiv 0 \pmod p$, by Lemma 3,

$$\left\{F_x(p)\right\}^2 \equiv 1 \pmod p$$

in which case

$$\left\{F_x(p-1)\right\}\left\{F_x(p+1)\right\} \equiv 0 \pmod p,$$

and the lemma follows.

Now if $x \equiv 0 \pmod p$, $F_x(n) \equiv 1 \pmod p$ for all n, by the definition of $F_x(n)$.

If $x \not\equiv 0 \pmod p$, from Lemma 5 there exists a number α such that $F_x(\alpha) \equiv 0 \pmod p$, we assume that α is the least such number, and $\alpha > 1$ since $F_x(1) = 1$ for all x. It can be shown inductively that $F_x(n+\alpha) \equiv sF_x(n) \pmod p$ for all n, where $s \equiv F_x(\alpha+1) \pmod p$, and $s \not\equiv 0$ since $s \equiv 0$ would imply $F_x(\alpha-1) \equiv 0 \pmod p$. Then if $F_x(r) \equiv 0 \pmod p$, there exists r' such that

$$r' \equiv r \pmod \alpha, \quad 0 < r' \leqslant \alpha, \quad \text{and} \quad F_x(r') \equiv 0 \pmod p.$$

By the definition of α, $r' < \alpha$ is absurd, therefore $r' = \alpha$.

Let P be prime and p a prime factor of $F_x(P)$. Then

$$F_x(P) \equiv 0 \pmod p \quad \text{and} \quad x \not\equiv 0 \pmod p$$

since, if $x \equiv 0 \pmod p$, $F_x(n) \equiv 1 \pmod p$ for all n.

Thus $P \equiv 0 \pmod \alpha$ and since P is prime, $P = \alpha$. Let p' be either $p, p-1$, or $p+1$, such that

$$F_x(p') \equiv 0 \pmod p$$

(from Lemma 3). Then p' is an integral multiple of P and the theorem follows.

I mentioned this result to Dr. P.M. Lee of York University and he has pointed out to me that Lemma 3 can be derived from H. Siebeck's work on recurring series (L.E. Dickson, *History of the Theory of Numbers,* p. 394f). A colleague of his has also discovered a non-elementary proof of the above theorem.

I am myself only an amateur mathematician, so I would ask you to excuse any resulting awkwardnesses in my presentation of this theorem and proof.

Yours faithfully,
Alexander G. Abercrombie

[Continued from Page 146.]

****

There is room for considerable work regarding possible lengths of periods. For various values of p and q we found periods of lengths: 1, 2, 8, 9, 17, 25, 33, 35, 42, 43, 61, 69.

GENERALIZED PERIODS

For various sequence types, it is possible to arrive at generalized periods. Some examples are the following.

$(p, p-1)$: $2p-2, 2p-3, 2p-3, 2p-2, 2p, 2p+2, 2p+3, 2p+2, 2p$, where p is large enough to make all quantities positive.

(p,p): $2p, 2p+2, 2p, 2p+1, 2p-1, 2p, 2p-1, 2p+1$, where $p \geqslant 2$.
$2p-1, 2p+1, 2p-1, 2p+2, 2p, 2p+3, 2p, 2p+2$, where $p \geqslant 2$, and many others.

$(p+1, p)$: $2p-1, 2p, 2p+2, 2p+4, 2p+5, 2p+4, 2p+2, 2p, 2p-1$ fpr $p \geqslant 3$. (Period of length 9)
$2p, 2p+1, 2p+5, 2p+5, 2p+5, 2p+1, 2p, 2p-3, 2p-1, 2p-1, 2p+4, 2p+4, 2p+7, 2p+3,$
$2p+2, 2p-3, 2p-2, 2p-3, 2p+2, 2p+3, 2p+8, 2p+7, 2p+4, 2p+4, 2p-1, 2p-1, 2p-3,$
for $p \geqslant 24$ (Period of length 26), and many others.

A schematic method was used which made the work of arriving at these results somewhat less laborious.

NON-PERIODIC SEQUENCES

In studying the sequences (3,4), non-periodic sequences of a quasi-periodic type were found. They have the peculiar property that alternate terms form a regular pattern in groups of four, while the intermediate terms between these pattern terms become unbounded. This situation arises in sequences (p,q) for which q is greater than p.

As an example of such a non-periodic sequence in the case (4,7) the sequence beginning with 1,3,4, follows:

1, 3, 4, 37, 59, 124, 25, 17, 2, 6, 3, 27, 22, 93, 20, 34, 3, 13, 3, 35, 13, 99, 14, 58, 4, 31, 3, 58, 9, 148, 12, 121, 4, 72, 3, 129, 8, 312, 11, 279, 4, 179, 3, 317, 8, 751, 10, 663, 4, 466, 3, 819, 8, 1922, 10, 1687, 4, 1183, 3, 2074, 8, 4850, 10, 4249, 4, 2976, 3, 5211, 8, 12170, 10, ⋯.

Note the regular periodicidity of 3,8,10,4 with the sets of intermediate terms increasing as the sequence progresses.

The various types of non-periodic sequence for (4,7) are:

[Continued on Page 184.]