PROOF OF A SPECIAL CASE OF DIRICHLET'S THEOREM

BARRY POWELL
195 Lake Ave. West, Kirkland, Washington 98033

For any prime p I give a simple proof that there are infinitely many primes $q \equiv -1 \bmod p$, a special case of Dirichlet's Theorem that if g.c.d. $(a,m) = 1$ there are infinitely many primes $\equiv a \pmod m$. The proof is of interest in that it utilizes several number-theoretic properties of the Fibonacci Numbers, which are also developed herein.

In this paper F_n represents the Pseudo-Fibonacci Numbers, defined as $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = aF_n + bF_{n-1}$, where a and b are non-zero relatively prime integers.

F_n may then be written non-recursively as

$$F_n = \frac{\left(\frac{a+\sqrt{a^2+4b}}{2}\right)^n - \left(\frac{a-\sqrt{a^2+4b}}{2}\right)^n}{\sqrt{a^2+4b}} \tag{1}$$

For a derivation of this result see Niven and Zuckerman [1].

We will need the following lemmas:

Lemma 1. For any positive integer r that divides F_n for some n, let h be the smallest positive integer such that r divides F_h. Then h is a divisor of n.

Lemma 2. For any positive integer n, g.c.d. $(F_n, b) = 1$.

These results are noted in a paper by Hoggatt and Long [2].

Lemma 3. For any odd prime q,

$$F_q \equiv (a^2+4b)^{\frac{q-1}{2}} \pmod q \tag{2}$$

$$2F_{q+1} \equiv a(a^2+4b)^{\frac{q-1}{2}} + a \pmod q \tag{3}$$

$$2bF_{q-1} \equiv -a(a^2+4b)^{\frac{q-1}{2}} + a \pmod q. \tag{4}$$

Proof of Lemma 3. Replacing n by q in (1), expanding the right-hand side by the binomial expansion, and multiplying by 2^{q-1} we get modulo q,

$$2^{q-1}F_q \equiv (a^2+4b)^{\frac{q-1}{2}}.$$

This gives (2) because $2^{q-1} \equiv 1 \bmod q$.

Similarly, if we replace n by $q+1$ in (1) and expand, noting that $\binom{q+1}{i} \equiv 0 \bmod q$ for $2 \leqslant i \leqslant q-1$, and then multiply by 2^q, we get

$$2^qF_{q+1} \equiv (q+1)a(a^2+4b)^{\frac{q-1}{2}} + (q+1)a^q \pmod q.$$

this reduces to (3) by use of $a^q \equiv a \bmod q$. Then (4) follows from (2) and (3) and the equality

$$2F_{q+1} = 2aF_q + 2bF_{q-1}.$$

Theorem (Dirichlet). For any prime p there exist infinitely many primes $q \equiv -1 \pmod p$.

Proof. If $p = 2$ every odd prime satisfies $q \equiv -1 \pmod 2$. So henceforth let p be a fixed odd prime. Suppose there are only finitely many primes $q_1, q_2, \cdots, q_m$ satisfying the congruence. By Theorem 2.27, Chapter 2 of Niven and Zuckerman [3], there exist $(p-1)/2$ positive integers $k \leq p-1$ satisfying $k^{(p-1)/2} \equiv 1 \bmod p$. Hence there also exist $(p-1)/2$ positive integers $j \leq p-1$ satisfying $j^{(p-1)/2} \equiv -1 \bmod p$. Let λ be one of these positive integers j and define the positive integers $a = 2$,

$$\theta = \lambda \prod_{j=1}^{m} q_j^2, \qquad b = 4\theta - 1.$$

It follows that

$$(5) \qquad a^2 + 4b = 16\theta, \qquad \frac{a \pm \sqrt{a^2+4b}}{2} = 1 + 2\sqrt{\theta}\ .$$

Using these values of a and b in (1) and using (2) from Lemma 3 with q replaced by p, we see that

$$(6) \qquad F_p \equiv (a^2+4b)^{\frac{p-1}{2}} \equiv (16\theta)^{\frac{p-1}{2}} \equiv 4^{p-1}(\Pi q_j)^{p-1}\lambda^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Also from (1) and (5) we see that

$$(7) \qquad F_p = \frac{(1+2\sqrt{\theta})^p - (1-2\sqrt{\theta})^p}{4\sqrt{\theta}}, \qquad F_p \equiv p \pmod{4\theta},$$

where the second result here is obtained by expanding the first result and taking everything modulo 4θ.

Now let q be a prime factor of F_p. From (6) we see that $q \neq p$, and from the second part of (7) we see that q is not a divisor of 4θ, so q is different from the primes $2, q_1, q_2, \cdots, q_m$.

We note that

$$(a^2+4b)^{\frac{q-1}{2}} \equiv (16\theta)^{\frac{q-1}{2}} \equiv 4^{q-1}(\Pi q_j)^{q-1}\lambda^{\frac{q-1}{2}} \equiv \lambda^{\frac{q-1}{2}} \equiv \epsilon \bmod q,$$

where $\epsilon = +1$ or $\epsilon = -1$.

If $\epsilon = +1$ we use (4) from Lemma 3 to conclude that q is a divisor of $2bF_{q-1}$. But q is odd and by Lemma 2 is not a divisor of b, since $(F_p, b) = 1$ and q is a divisor of F_p, and so q is a divisor of F_{q-1}. By Lemma 1, with n replaced by $q-1$, h replaced by p, and r by q, we see that p is a divisor of $q-1$ and so $q \equiv 1 \bmod p$. Now if this congruence holds for every prime divisor q of F_p it would follow from the multiplication of such congruences that $F_p \equiv 1 \bmod p$, contrary to (6). Hence we must have $\epsilon = -1$ for at least one prime divisor q of F_p.

In the case $\epsilon = -1$ we use (3) from Lemma 3 to conclude that q is a divisor of $2F_{q+1}$, and so a divisor of F_{q+1}. By Lemma 1 we see that p is a divisor of $q+1$, so $q \equiv -1 \pmod p$, contrary to the assumption that $q_1, q_2, \cdots, q_m$ are the only primes satisfying this congruence. Q.E.D.

Corollary. From the same analysis used to establish the above result, with $a = 2$ and $b = 4\lambda - 1$ substituted into (1), $p \cdot 1$, for any prime p

$$F_p = \frac{(1+2\sqrt{\lambda})^p - (1-2\sqrt{\lambda})^p}{4\sqrt{\lambda}}$$

is divisible by a prime $q \equiv -1 \pmod p$. Since $\lambda \leq p-1$, a prime

$$q \equiv -1 \pmod p < (2\sqrt{p-1}+1)^p.$$

For a proof of the existence of infinitely many primes $q \equiv -1 \pmod m$, (m any positive integer ≥ 2) using polynomial theory, see Nagell [4]. For a simple proof of the existence of infinitely many primes $q \equiv 1 \pmod m$ see Ivan Niven and Barry Powell [5].

ADDITIONAL RESULTS

Theorem: Consider any odd prime p which does not divide (a^2+4b), where $(a,b) = 1$ as in (1), $p \cdot 1$. Then $F_p \equiv 0 \bmod q$, q prime, $\rightarrow q \equiv 1 \bmod p$ or $q \equiv -1 \bmod p$ if and only if

$$(a^2+4b)^{\frac{q-1}{2}} \equiv 1 \bmod q \qquad \text{or} \qquad (a^2+4b)^{\frac{q-1}{2}} \equiv -1 \bmod q.$$

[Co-discovered by Professor Verner E. Hoggatt, Jr., per telephone communication.]

Proof. We have, from (1), p. 1,

$$F_p = \frac{\left(\frac{a+\sqrt{a^2+4b}}{2}\right)^p - \left(\frac{a-\sqrt{a^2+4b}}{2}\right)^p}{\sqrt{a^2+4b}}$$

Multiplying both sides by 2^{p-1} and using the binomial expansion, we get

$$2^{p-1}F_p \equiv pa^{p-1} \bmod (a^2+4b). \tag{8}$$

$$F_p \equiv 0 \bmod q \to q \nmid (a^2+4b).$$

Otherwise

$$q \mid (a^2+4b) \to 2^{p-1}F_p \equiv pa^{p-1} \bmod q \quad \text{from (8)},$$

$$\to pa^{p-1} \equiv 0 \bmod q \to q \mid p \text{ or } q \mid a.$$

$$q \mid p \to q = p \to F_p \equiv 0 \bmod p \to p \mid (a^2+4b)$$

by (2) of Lemma 3, contradicting the assumption that $p \nmid (a^2+4b)$. $q \nmid a$, since

$$a = F_2 \equiv 0 \bmod q \to 2 \mid p$$

by Lemma 1, and p is odd.

Thus from Lemma 3, (3) and (4),

$$F_{q+1} \equiv 0 \bmod q \text{ iff } (a^2+4b)^{\frac{q-1}{2}} \equiv -1 \bmod q$$

and

$$2bF_{q-1} \equiv 0 \bmod q \text{ iff } (a^2+4b) \equiv 1 \bmod q.$$

$F_p \equiv 0 \bmod q$ and $F_{q+1} \equiv 0 \bmod q \to q \equiv -1 \bmod p$ by Lemma 1 with h replaced by p. Since

$$p \mid (q+1) \to F_p \mid F_{q+1}$$

Therefore $F_{q+1} \equiv 0 \bmod q$. Thus $F_{q+1} \equiv 0 \bmod q$ iff $q \equiv -1 \bmod p$. Hence $(a^2+4b)^{\frac{q-1}{2}} \equiv -1 \bmod q$ iff $q \equiv -1$ mod q.

Similarly $F_{q-1} \equiv 1 \bmod q$ iff $q \equiv 1 \bmod p$ and hence $(a^2+4b)^{\frac{q-1}{2}} \equiv 1 \bmod q$ iff $q \equiv 1 \bmod p$ follows from Lemma 1, Lemma 2, and the fact that $p \mid (q-1) \to F_p \mid F_{q-1}$.

Conjecture. For n any positive integer sufficiently large, there exists at least 1 prime $q \equiv \pm 1 \bmod n$ dividing F_n.

EXAMPLES. F_{15} of the Fibonacci sequence

$$= 610 = 61 \cdot 10 \text{ and } 61 \equiv 1 \bmod 15.$$

$$F_{18} = 136 \cdot 19 \text{ and } 19 \equiv 1 \bmod 18.$$

$$F_{20} = 165 \cdot 41 \text{ and } 41 \equiv 1 \bmod 20.$$

REFERENCES

1. Niven and Zuckerman, *An Introduction to the Theory of Numbers,* 3rd ed. (1972), pp. 96–99.
2. V. E. Hoggatt, Jr., and Calvin T. Long, "Generalized Fibonacci Polynomials," *The Fibonacci Quarterly,* Vol. 12, No. 2 (April 1974).
3. Niven and Zuckerman, *An Introduction to the Theory of Numbers,* 3rd ed. (1972), Ch. 2, Theorem 2.27.
4. T. Nagell, *An Introduction to Number Theory,* pp. 170–173, John Wiley, New York (1951).
5. Ivan Niven and Barry Powell, "Primes in Certain Arithmetic Progressions," *Amer. Math. Monthly,* Vol. 83, No. 6, June–July 1976, pp. 467–469.

****