Suryanarayana, D. & V. Siva Rama Prasad. "The Number of Pairs of Generalized Integers with L.C.M. $\leq x$." *J. Austral. Math. Soc.* 13 (1972):411-416.

_____. "The Number of k-ary Divisors of a Generalized Integer." *Portugal. Math.* 33 (1974):85-92.

Tuljaganova, M. "Distribution of Values of Euler's Function Deiuned on a Normalized Semigroup." *Izv. Akad. Nauk USSR Ser. Fiz.-Mat. Nauk* 12, No. 5 (1968):33-37 (in Russian).

Wegmann, H. "Beiträge zur Zahlentheorie auf freien Halbgruppen, I-II." *J. Reine Angew. Math.* 221 (1966):20-43, 150-159.

_____. "Über k-freie Elemente in Halbgruppen reeller Zahlen." *J. Reine Angew. Math.* 212 (1963):180-182.

Zlatopolskii, M. V. "The Distribution of the Elements of Free Semi-groups with Regular Normalization." Taskent Gos. Univ. Naucn. Trudy Vyp. 460 (in Russian). *Voprosy Mat.* (1974):62-66, 173.

*****

THE NUMBER OF PRIMES IS INFINITE

S. P. MOHANTY
Indian Institute of Technology, Kanpur 208016, U.P. India

For the theorem used as the title of this paper, many proofs exist, some simple, some erudite. For earlier proofs, we refer to [1]. We present here three interesting proofs of the above theorem, and believe that they are new in some sense.

Theorem 1: Let $A_0 = \alpha + m$, where α and m are positive integers with $(\alpha, m) = 1$. Let A_n be defined recursively by

$$A_{n+1} = A_n^2 - mA_n + m.$$

Then each A_i is prime to every A_j, $j \neq i$.

Proof: By definition,

$$A_1 = A_0^2 - mA_0 + m = \alpha A_0 + m.$$

Again,

$$A_2 = A_1^2 - mA_1 + m = A_1(A_1 - m) + m = \alpha A_0 A_1 + m.$$

Assume that

$$A_k = \alpha A_0 A_1 \ldots A_{k-1} + m.$$

By hypothesis, we have

$$A_{k+1} = A_k^2 - mA_k + m = A_k(A_k - m) + m.$$

Now, substituting $\alpha A_0 A_1 \ldots A_{k-1}$ for $A_k - m$ in the preceding line, we obtain

$$A_{k+1} = \alpha A_0 A_1 \ldots A_k + m.$$

So, by induction hypothesis, we get

$$A_n = \alpha A_0 A_1 \ldots A_{n-1} + m \text{ for all } n.$$

Again, from $A_0 \equiv \alpha \pmod{m}$, it follows that $A_1 \equiv \alpha^2 \pmod{m}$. Suppose that

$$A_k \equiv \alpha^{2^k} \pmod{m}.$$

Since we have $A_{k+1} = A_k^2 - mA_k + m$, we have

$$A_{k+1} \equiv (\alpha^{2^k})^2 \pmod{m},$$

that is,

$$A_{k+1} = \alpha^{2^{k+1}} \pmod{m}.$$

Hence, by induction,

$$A_i \equiv \alpha^{2^i} \pmod{m}.$$

Next, let $d = (A_i, A_j)$, $j > i$. Since

$$A_j = \alpha A_0 A_1 \ldots A_{j-1} + m,$$

we have $d|m$. But d divides $A_i \equiv \alpha^{2^i} \pmod{m}$. Now $d|A_i$ and $d|m$ together imply $d = 1$ for $(\alpha, m) = 1$. Hence,

$$(A_i, A_j) = 1, \; j > i,$$

and the theorem is proved.

Corollary 1: The number of primes is infinite.

Proof: It is easy to see that $A_1, A_2, \ldots$ are all odd. Since each A_i is prime to every A_j by Theorem 1, each of the numbers $A_1, A_2, \ldots$ is divisible by an odd prime which does not divide any of the others, and hence there are at least n distinct primes $\leq A_n$. This proves the corollary.

We note that Pólya's proof of the theorem using Fermat numbers [2] is a particular case of the above theorem. Taking $\alpha = 1$, $m = 2$ in the above theorem, we have $A_0 = 3$, $A_1 = 5$, $A_2 = 17$, etc. These are Fermat numbers defined by $F_n = 2^{2^n} + 1$, satisfying $F_{n+1} = F_n^2 - 2F_n + 2$ with $F_0 = 3$. Again, the theorem in [3] is obtained when we put $\alpha = 1$ and $m = 1$.

Theorem 2: Every prime divisor of $\frac{1}{3}(2^p + 1)$, where p is a prime > 3, is greater than p.

Proof: First, we show that $\frac{1}{3}(2^p + 1)$ where p is a prime >3 is not divisible by 3. Now,

$$\frac{1}{3}(2^p + 1) = \frac{2^p + 1}{2 + 1} = 2^{p-1} - 2^{p-2} + \cdots + 1$$

is an integer. Again

$$\frac{1}{3}(2^p + 1) = (2^{p-1} + 2^{p-3} + \cdots + 1) - (2^{p-2} + 2^{p-4} + \cdots + 2)$$

$$\equiv \frac{p + 1}{2} - 2 \cdot \frac{p - 1}{2} \pmod 3 \equiv \frac{-p + 3}{2} \pmod 3.$$

Since p is a prime >3 we have $p = 6k + 1$ or $6k + 5$. Then,

$$\frac{1}{3}(2^p + 1) \equiv \frac{-6k - 1 + 3}{2} \equiv 1 \pmod 3$$

or

$$\frac{1}{3}(2^p + 1) \quad \frac{-6k - 5 + 3}{2} \quad -1 \pmod 3.$$

Next, suppose that $\frac{1}{3}(2^p + 1) \equiv 0 \pmod q$, where q is a prime $\leq p$. Clearly, q is odd and $q \neq 3$ when $p > 3$. Now, by Fermat's little theorem

$$2^{q-1} \equiv 1 \pmod q.$$

If $q = p > 3$, we have $2^{p-1} \equiv 1 \pmod q$, whence $2^p \equiv 2 \pmod q$. But

$$\frac{1}{3}(2^p + 1) \equiv 0 \pmod q$$

by assumption. Hence, we obtain $3 \equiv 0 \pmod q$, a contradiction. Therefore, $q < p$. Now, $(q - 1, p) = 1$ implies that there exist integers a and b such that $ap + b(q - 1) = 1$. Then

$$a \qquad 2 = 2^{ap+b(q-1)} = (2^p)^a \cdot (2^{q-1})^b \equiv (-1)^a(1)^b \pmod q \equiv -1 \pmod q$$

for a odd. Hence, $2 \equiv -1 \pmod q$ or $3 \equiv 0 \pmod q$. Since q is a prime and $q \neq 3$, we have again a contraction; hence, $q > p$. Therefore, every prime divisor of $\frac{1}{3}(2^p + 1)$ is greater than p. Now it is a corollary that the number of primes is infinite.

We note that "Every prime divisor of $2^p - 1$ where p is a prime is greater than p" was a problem in the *American Mathematical Monthly*.

Theorem 3: Let p be an odd prime > 5. Then every prime divisor of U_p is greater than p where U_p is the pth Fibonacci number.

The Fibonacci numbers are definable by $U_1 = U_2 = 1$ and $U_{n+1} = U_n + U_{n-1}$. We use the following facts to prove the theorem:

(1) $U_{n+m} = U_{n-1}U_m + U_nU_{m+1}$.

(2) If $m|n$ then $U_m|U_n$ and conversely.

(3) Neighboring Fibonacci numbers are relatively prime to each other.

(4) For any m, n we have $(U_m, U_n) = U_{(m,n)}$, where (a, b) means g.c.d. of a and b.

(5) If p is an odd prime, then $p|U_p$, $p|U_{p-1}$, or $p|U_{p+1}$, according as $p = 5$, $p = 10m \pm 1$, or $p = 10m \pm 3$.

Proof: For $p = 2$, $2|F_{p+1} = 2$. Let p be an odd prime > 5. Then U_p is odd since only U_{3t}'s are even. So, every divisor of U_p is odd. Let $q|U_p$ where q is a prime. If $q = p$, then $p|U_p$. This is impossible for $p > 5$. Suppose $q < p$. Now, $(U_p, U_q) = U_{(p,q)} = U_1 = 1$, $(U_{q-1}, U_p) = U_{(q-1,p)} = U_1 = 1$ and $(U_{q+1}, U_p) = U_{(q+1,p)} = U_1 = 1$. Hence, $q \nmid U_q$, $q \nmid U_{q-1}$, and $q \nmid U_{q+1}$. This contradicts (5). Therefore, $q > p$ and the theorem is proved.

Thus, it is a corollary that the number of primes is infinite.

A Request: The author is trying to collect all the proofs on infinitude of primes. Any information in this regard will be very much appreciated.

REFERENCES

1. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, pp. 413-415.

2. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, p. 14.

3. Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, Vol. 1 (Washington, D.C.: Spartan Books, 1962), p. 13.

*****