A GENERALIZATION OF FERMAT'S LITTLE THEOREM

Frank S. Gillespie
Southwest Missouri State University, Springfield, MO 65804
(Submitted February 1987)

A rational number r is said to be divisible by a prime number p provided the numerator of r is divisible by p. Here it is assumed that all rational numbers are written in standard form. That is, the numerators and denominators are relatively prime integers and the denominators are positive.

Certain sequences $\{u_n\}_{n=1}^{\infty}$ of rational numbers have the property that if p is any prime number, then $u_p \equiv u_1 \pmod{p}$. A sequence $\{u_n\}_{n=1}^{\infty}$ having this property is said to be a *Fermat sequence* or to possess the *Fermat property*.

The obvious example of a sequence that has the Fermat property is $\{a^n\}_{n=1}^{\infty}$ with a being an integer. Indeed Fermat's Little Theorem states that if a is any integer and if p is a prime number, then $a^p \equiv a \pmod{p}$.

There are sequences $\{u_n\}_{n=1}^{\infty}$ that have the Fermat property other than $\{a^n\}_{n=1}^{\infty}$. An example of a sequence that has the Fermat property for odd primes is the sequence $\{T_n(x)\}_{n=1}^{\infty}$ where x is an integer and $T_n(x)$ is a Tchebycheff polynomial of the first kind.

It is the purpose of this paper to give a class of sequences (of rational numbers) all having the Fermat property. The following theorem is related to Newton's formulas. Let

$$f(x) = x^k + A_1x^{k-1} + \cdots + A_{k-1}x + A_k$$

be a polynomial with real or complex coefficients. The sequence $\{u_n\}_{n=1}^{\infty}$ is defined in the following way: The first k terms of the sequence are given by Newton's formulas, namely,

$$\begin{aligned}
&u_1 + A_1 = 0,\\
&u_2 + A_1u_1 + 2A_2 = 0,\\
&u_3 + A_1u_2 + A_2u_1 + 3A_3 = 0, \qquad (1)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\\
&u_k + A_1u_{k-1} + A_2u_{k-2} + \cdots + A_{k-1}u_1 + kA_k = 0.
\end{aligned}$$

After the initial k terms are given, the rest of the terms are generated by the difference equation

$$u_n + A_1u_{n-1} + A_2u_{n-2} + \cdots + A_ku_{n-k} = 0, \qquad (2)$$

for $n \ge k + 1$, which is formed from the polynomial $f(x)$. It is well known that the sequence $\{u_n\}_{n=1}^{\infty}$ given above is the sequence of the sum of the powers of the roots of $f(x)$. Thus, if

$$f(x) = (x - x_1)(x - x_2) \dots (x - x_k),$$

then

$$u_n = x_1^n + x_2^n + \cdots + x_k^n, \text{ for } n = 1, 2, 3, \dots .$$

In this paper it is supposed that $x_1x_2 \dots x_k \ne 0$. See [6], pages 260-262.

The Corollary to Theorem 1 solves the difference equation defined by (1) and (2) with appropriate adjustments in the way $f(x)$ is factored.

Theorem 1: Let $c_1, c_2, \ldots, c_k$ and $x_1, x_2, \ldots, x_k$ be any real or complex numbers. Let

$$\prod_{i=1}^{k}(1 + x_i x)^{c_i} = 1 + \sum_{i=1}^{\infty} A_i x^i. \tag{3}$$

Then

$$c_1x_1^n + c_2x_2^n + \cdots + c_kx_k^n \tag{4}$$

$$= \frac{n\displaystyle\sum_{j_1=0}^{n-1}(-1)^{j_1}\sum_{j_2=0}^{j_1}\binom{n-j_1}{j_2}A_1^{n-j_1-j_2}\sum_{j_3=0}^{j_2}\binom{j_2}{j_3}A_2^{j_2-j_3}\cdots}{n-j_1}$$

$$\frac{\displaystyle\sum_{j_{n-1}=0}^{j_{n-2}}\binom{j_{n-2}}{j_{n-1}}A_{n-2}^{j_{n-2}-j_{n-1}}\binom{j_{n-1}}{j_1-j_2-\cdots-j_{n-1}}A_{n-1}^{j_{n-1}-(j_1-j_2-\cdots-j_{n-1})}A_n^{j_1-j_2-\cdots-j_{n-1}}}{},$$

where n is a natural number.

Proof: The argument is formal. Take $\ln x$ of both sides of (3). Then, for the left side,

$$\ln\prod_{i=1}^{k}(1 + x_i x)^{c_i} = \sum_{i=1}^{k} c_i \ln(1 + x_i x). \tag{4}$$

The expansion

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - + \cdots + \frac{(-1)^{n-1}x^n}{n} + \cdots, \tag{5}$$

$|x| < 1$ is well known.

Let $\mathrm{Coe}_{x^r} f(x)$ denote the coefficient of x^r when $f(x)$ is expanded as a power series in x. Then

$$\mathrm{Coe}_{x^n}\sum_{i=1}^{k} c_i \ln(1 + x_i x) = \sum_{i=1}^{k}\frac{c_i(-1)^{n-1}x_i^n}{n} \tag{6}$$

$$= \frac{(-1)^{n-1}[c_1x_1^n + c_2x_2^n + \cdots + c_kx_k^n]}{n}.$$

To find the coefficient of x^n on the right side of (3) after $\ln x$ is taken, the following argument is given. Since the coefficient of x^n is to be determined, it follows that only

$$\ln\left(1 + \sum_{i=1}^{n} A_i x^i\right)$$

need be considered. Thus, the required coefficient is

$$\mathrm{Coe}_{x^n}\ln\left(1 + \sum_{i=1}^{n} A_i x^i\right) \tag{7}$$

$$= \mathrm{Coe}_{x^n}\left[\frac{\displaystyle\sum_{i=1}^{n} A_i x^i}{1} - \frac{\left(\displaystyle\sum_{i=1}^{n} A_i x^i\right)^2}{2} + - \cdots + \frac{(-1)^{n-j-1}\left(\displaystyle\sum_{i=1}^{n} A_i x^i\right)^{n-j}}{n-j} + \cdots\right].$$

Since each term in this expansion has x as a factor, it is not necessary to consider terms for which $n - j > n$. Thus, $n - j \le n$ so that $j \ge 0$. Also, the only ones that are needed to be considered are those which do have some term with x^n in its expansion. Now each term that has x^n in its expansion satisfies $n(n - j) \geq n$ or $n - j \geq 1$ or $n - 1 \geq j$. Thus, the largest value for j needed is $n - 1$. Hence,

$$\mathrm{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{n} A_i x^i\right) = \mathrm{Coe}_{x^n} \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1}\left(\sum_{i=1}^{n} A_i x^i\right)^{n-j_1}}{n - j_1} \tag{8}$$

$$= \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1}\mathrm{Coe}_{x^{j_1}}\left(A_1 + \sum_{i=2}^{n} A_i x^{i-1}\right)^{n-j_1}}{n - j_1}$$

$$= \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1}\mathrm{Coe}_{x^{j_1}} \sum_{j_2=0}^{n-j_1} \binom{n - j_1}{j_2} A_1^{n-j_1-j_2}\left(\sum_{i=2}^{n} A_i x^{i-1}\right)^{j_2}}{n - j_1}$$

$$= \sum_{j_1=0}^{n-1} \frac{(-1)^{n-j_1-1} \sum_{j_2=0}^{n-j_1} \binom{n - j_1}{j_2} A_1^{n-j_1-j_2}\,\mathrm{Coe}_{x^{j_1-j_2}}\left(A_2 + \sum_{i=3}^{n} A_i x^{i-2}\right)^{j_2}}{n - j_1}.$$

Continuing this pattern with a simple induction completes the proof. □

An important special case of Theorem 1 occurs when $c_1 = c_2 = \cdots = c_k = 1$. In this case, in (7),

$$\mathrm{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{k} A_i x^i\right) = \mathrm{Coe}_{x^n} \ln\left(1 + \sum_{i=1}^{k} \sigma_i x^i\right), \tag{9}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_k$ are the elementary symmetric functions of $x_1, x_2, \ldots, x_k$. Thus,

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + \cdots + x_k,\\ \sigma_2 &= x_1x_2 + x_1x_3 + x_1x_4 + \cdots + x_2x_3 + \cdots\\ &\quad + \cdots + x_{k-1}x_k, \;\ldots,\; \sigma_k\\ &= x_1x_2 \ldots x_k.\end{aligned}$$

The only terms in the expansion (9) that need be considered are those which actually do have some term with x^n in its expansion. Now each term which has x^n in its expansion satisfies $k(n - j) \geq n$, or $(k - 1)n \geq kj$, [see line (8)]. Let $h_k(n)$ be the largest whole number t such that $(k - 1)n \geq kt$. Thus, $0 \leq j \leq h_k(n)$. With this change, the following is a corollary to Theorem 1.

Corollary to Theorem 1: Let n be a natural number and let $x_1, x_2, \ldots, x_k$ be a set of real or complex numbers.

Then,

$$x_1^n + x_2^n + \cdots + x_k^n = \frac{n \sum_{j_1=0}^{h_k(n)} (-1)^{j_1} \sum_{j_2=0}^{j_1} \binom{n - j_1}{j_2} \sigma_1^{n-j_1-j_2} \sum_{j_3=0}^{j_2} \binom{j_2}{j_3} \sigma_2^{j_2-j_3} \cdots \sum_{j_{k-1}=0}^{j_{k-2}} \binom{j_{k-2}}{j_{k-1}} \sigma_{k-2}^{j_{k-2}-j_{k-1}} \binom{j_{k-1}}{j_1 - j_2 - \cdots - j_{k-1}} \sigma_{k-1}^{j_{k-1}-(j_1-j_2-\cdots-j_{k-1})}\, \sigma_k^{j_1-j_2-\cdots-j_{k-1}}}{n - j_1}, \tag{10}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_k$ are the elementary symmetric functions of $x_1, x_2, \ldots, x_k$ and $h_k(n)$ is the largest whole number t such that $(k-1)n \geq kt$.

Using (10), with appropriate simplifications for $k = 2$ and $k = 3$, gives:

$$x_1^n + x_2^n = n \sum_{j=0}^{[n/2]} (-1)^j \frac{\binom{n-j}{j}}{n-j}(x_1 + x_2)^{n-2j}(x_1x_2)^j, \tag{11}$$

and

$$x_1^n + x_2^n + x_3^n \tag{12}$$
$$= \frac{n \sum_{j=0}^{[2n/3]} (-1)^j \sum_{\ell=[(j+1)/2]}^{j} \binom{n-j}{\ell}\binom{\ell}{j-\ell}(x_1 + x_2 + x_3)^{n-j-\ell}}{n-j}$$
$$\frac{(x_1x_2 + x_2x_3 + x_3x_1)^{2\ell-j}(x_1x_2x_3)^{j-\ell}}{},$$

where [ ] is the greatest integer function.

The identity (11) is known. It is reported on in [2], p. 80, in the article on G. Candido's use of this identity.
For a discussion of formal arguments, see [3].

Theorem 1 can now be used to establish

Theorem 2: Let $c_1, c_2, \ldots, c_k$ and $x_1, x_2, \ldots, x_k$ be any real or complex numbers and if the coefficients $A_1, A_2, A_3, \ldots$ in

$$\prod_{i=1}^{k}(1 + x_i x)^{c_i} = 1 + \sum_{i=1}^{\infty} A_i x^i$$

are all rational numbers, then:

(1) The sequence $\{u_n\}_{n=1}^{\infty}$, $u_n = c_1x_1^n + c_2x_2^n + \cdots + c_kx_k^n$, is a sequence of rational numbers; and

(2) If for any prime number p, p is relatively prime to each of the denominators of $A_1, A_2, \ldots, A_p$, then the sequence $\{u_n\}_{n=1}^{\infty}$ has the Fermat property.

Proof: From Theorem 1, it is clear that u_n is a rational number if $A_1, A_2, \ldots, A_n$ are all rationals. Also, if p is a prime number, from Theorem 1 and the fact that the denominators of $A_1, A_2, \ldots, A_p$ are all relatively prime to p, $u_p \equiv u_1 \pmod{p}$. Here, $u_1 = A_1$. □

L. E. Dickson established a result somewhat reminiscent of Theorem 2. He showed that if Z_n is the sum of the n^{th} powers of the roots of the polynomial

$$x^m + a_1x^{m-1} + \cdots + a_k = 0,$$

where $a_1 = 0$ and $a_1, a_2, \ldots, a_k$ are all integers, then $Z_p \equiv 0 \pmod{p}$ when p is a prime. See [1]. This result is of course a corollary of Theorem 2.

Example 1: For the Tchebycheff polynomials it is known that

$$2T_n(x) = (x + \sqrt{x^2 - 1})^n + (x - \sqrt{x^2 - 1})^n.$$

(See [5], p. 5.) Letting

$$y_1 = x + \sqrt{x^2 - 1}$$

and

$$y_2 = x - \sqrt{x^2 - 1}$$

and

$$(1 + y_1 y)(1 + y_2 y) = 1 + 2xy + y^2$$

so that, by Theorem 2, for x an integer $\{2T_n(x)\}_{n=1}^{\infty}$ is a Fermat sequence. Thus, if p is a prime number $2T_p(x) \equiv 2x \pmod{p}$. Hence, if $p > 2$, $\{T\ (x)\}_{n=1}^{\infty}$ has the Fermat property.

It is possible to give examples of sequences $\{u\ \}_{n=1}^{\infty}$ in (1) of Theorem 2 where the c's are irrational or even complex. However, if the x 's are irrational, then it is not obvious that $u_n \equiv u_1 \pmod{p}$ for p being a prime number. The position taken here is that no irrational number is divisible by any prime number. The arithmetic of this paper is the arithmetic of the real rational integers. Thus,

$$\left(\frac{1 + \sqrt{5}}{2}\right)^p \not\equiv \frac{1 + \sqrt{5}}{2} \pmod{p},$$

but as Theorem 2 shows

$$\left(\frac{1 + \sqrt{5}}{2}\right)^p + \left(\frac{1 - \sqrt{5}}{2}\right)^p \equiv \frac{1 + \sqrt{5}}{2} + \frac{1 - \sqrt{5}}{2} \pmod{p}.$$

Thus, for $x_1, x_2, \ldots, x_k$, the roots of a polynomial over the rationals

$$x_1^p + x_2^p + \cdots + x_k^p \equiv x_1 + x_2 + \cdots + x_k \pmod{p}$$

is a generalization of Fermat's Little Theorem.

From Theorem 1 it is clear that if the u's are all rational numbers, then all the A's in Theorem 2 are also rational. Thus, the following corollary is established.

Corollary to Theorem 2: Let $c_1, c_2, \ldots, c_k$ and $x_1, x_2, \ldots, x_k$ be any real or complex numbers. Then a necessary and sufficient condition for the coefficients $A_1, A_2, A_3, \ldots$ in

$$\prod_{i=1}^{k} (1 + x_i x)^{c_i} = 1 + \sum_{i=1}^{\infty} A_i x^i, \tag{13}$$

to be rational numbers is for the sequence

$$\{u_n\}_{n=1}^{\infty},\ u_n = c_1 x_1^n + c_2 x_2^n + \cdots + c_k x_k^n,$$

to be a sequence of rationals.

Example 3: Let a and b be rationals and suppose that b is not the square of a rational. Consider the power series

$$(1 + (a + \sqrt{b})x)^{a - \sqrt{b}} (1 + (a - \sqrt{b})x)^{a + \sqrt{b}} = 1 + \sum_{i=1}^{\infty} A_i x^i. \tag{14}$$

By the corollary, the power series will have rational coefficients provided

$$u_n = (a + \sqrt{b})(a - \sqrt{b})^n + (a - \sqrt{b})(a + \sqrt{b})^n,$$

is rational for $n = 1, 2, 3, \ldots$. Now

$$u_n = (a^2 - b)[(a - \sqrt{b})^{n-1} + (a + \sqrt{b})^{n-1}] \tag{15}$$

$$= (a^2 - b) \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-1-i} b^{i/2} [(-1)^i + 1],$$

which is clearly rational.

For example,

$$(1 + \omega x)^{\omega^2}(1 + \omega^2 x)^{\omega} = 1 + \sum_{i=1}^{\infty} A_i x^i, \tag{16}$$

is such that A_i is rational for $i = 1, 2, 3, \ldots$ when $1, \omega, \omega^2$ are the cube roots of unity.

Example 4: Define the sequence $\{u_n\}_{n=1}^{\infty}$ by the formula

$$u_n = \sum_{j=1}^{m} \sec^{2n}\frac{2j-1}{4m}\pi.$$

Here m is an arbitrary natural number. Then $\{u_n\}_{n=1}^{\infty}$ is a sequence of integers which has the Fermat property.

To see this, consider the product

$$f(y) = \prod_{j=1}^{m}\left(1 - \left[\sec^2\frac{2j-1}{4m}\pi\right]y\right). \tag{17}$$

Multiply this by $\prod_{j=1}^{m}\cos^2\frac{2j-1}{4m}\pi$ so that

$$f(y)\prod_{j=1}^{m}\cos^2\frac{2j-1}{4m}\pi = \prod_{j=1}^{m}\left(\cos^2\frac{2j-1}{4m}\pi - y\right). \tag{18}$$

Replace y by x^2 so that

$$f(x^2)\prod_{j=1}^{m}\cos^2\frac{2j-1}{4m}\pi = \prod_{j=1}^{m}\left(\cos^2\frac{2j-1}{4m}\pi - x^2\right), \tag{19}$$

$$\left[(-1)^m\prod_{j=1}^{m}\cos^2\frac{2j-1}{4m}\pi\right]f(x^2) = \prod_{j=1}^{m}\left(x - \cos\frac{2j-1}{4m}\pi\right)\left(x + \cos\frac{2j-1}{4m}\pi\right). \tag{20}$$

Thinking of $\cos[(2j-1)/4m]\Pi$ along the unit circle for $j = 1, 2, \ldots, m$, it is in the first quadrant so that, by symmetry,

$$\left[(-1)^m\prod_{j=1}^{m}\cos^2\frac{2j-1}{4m}\pi\right]f(x^2) = \prod_{j=1}^{2m}\left(x - \cos\frac{2j-1}{4m}\pi\right). \tag{21}$$

A well-known identity is

$$x^{2n} + 1 = \prod_{j=1}^{n}\left(x^2 - 2x\cos\frac{2j-1}{2n}\pi + 1\right). \tag{22}$$

In (22), let $n = 2m$ and $x = i$ so that

$$2 = (-1)^m 2^{2m}\prod_{j=1}^{2m}\cos^2\frac{2j-1}{4m}\pi. \tag{23}$$

Now, by symmetry around the unit circle,

$$\prod_{j=1}^{2m}\cos\frac{2j-1}{4m}\pi = (-1)^m\prod_{j=1}^{m}\cos^2\frac{2j-1}{4m}\pi = \frac{(-1)^m}{2^{2m-1}}. \tag{24}$$

Using (24) and (21) yields

$$f(x^2) = (-1)^m 2^{2m-1} \prod_{j=1}^{2m}\left(x - \cos\frac{2j-1}{4m}\pi\right). \tag{25}$$

It is well known that

$$T_{2m}(x) = 2^{2m-1} \prod_{j=1}^{2m}\left(x - \cos\frac{2j-1}{4m}\pi\right),$$

where $T_{2m}(x)$ is the $2m^{\text{th}}$ Tchebycheff polynomial (see [4], pp. 86-90). This follows from the fact that $T_n(x) = \cos(n \arccos x)$. Now $x = \sqrt{y}$, so that

$$f(y) = (-1)^m T_{2m}(\sqrt{y}), \tag{26}$$

which is a polynomial in y with integer coefficients.

Since $\sec^2[(2j-1)/4m]\pi$ for $j = 1, 2, 3, \ldots, m$ are the roots of

$$(-1)^m y^m T_{2m}(1/\sqrt{y})$$

and the coefficients of this polynomial are all integers and the leading coefficient is $(-1)^m$, it follows from the corollary to Theorem 2 that $\{u_n\}_{n=1}^{\infty}$ is a sequence of integers satisfying the Fermat property.

References

1. *Amer. Math. Monthly* 15 (1908):209.
2. L. E. Dickson. *History of the Theory of Numbers*. Vol. I: *Divisibility and Primality*. New York: Chelsea, 1952.
3. Ian P. Goulden & David M. Jackson. *Combinatorial Enumeration*. New York: Wiley & Sons, 1983.
4. Kenneth S. Miller & John B. Walsh. *Advanced Trigonometry*. New York: Krieger, 1977.
5. Theodore J. Rivlin. *The Chebyshev Polynomials*. New York: Wiley-Interscience, 1974.
6. J. V. Uspensky. *Theory of Equations*. New York: McGraw-Hill, 1948.

*****