International Journal of Number Theory
Vol. 1, No. 4 (2005) 499–512
© World Scientific Publishing Company

IRRATIONAL FACTORS SATISFYING THE LITTLE FERMAT THEOREM

SIMON LITSYN
School of Electrical Engineering
Tel Aviv University, 69978 Tel Aviv, Israel
litsyn@eng.tau.ac.il

VLADIMIR SHEVELEV
Department of Mathematics
Ben Gurion University, 84105 Beer Sheva, Israel
shevelev@bgu.ac.il

Received 13 May 2005
Accepted 5 September 2005

We study possible generalizations of the little Fermat theorem when the base of the exponentiation is allowed to be a non-integer. Such bases we call Fermat factors. We attempt classification of Fermat factors, and suggest several constructions.

Keywords: Congruences; Fermat theorem; Pisot numbers.

Mathematics Subject Classification: 11A07

1. Introduction

The fundamental "little" Fermat theorem claims that for any integer m and prime p,

$$m^p \equiv m \bmod p. \tag{1.1}$$

A natural question is if this theorem can be generalized by allowing the base on the left-hand side of (1.1) to be non-integer. Indeed, it is easy to check that if we keep the integrality of the base then the only possible generalization is

$$\forall m, k \in \mathbf{N}, p \text{ prime}: \quad (m(kp+1))^p \equiv m \bmod p. \tag{1.2}$$

Thus non-integer bases should be considered. Let $nint[m]$ stand for the integer closest to m.

Definition 1.1. A number $\xi(m)$ is called a Fermat factor of integer m if for every sufficiently large prime p,

$$nint[(m\xi(m))^p] \equiv m \bmod p. \tag{1.3}$$

For instance, as it will be shown later, $\xi(m) = \frac{1}{2m}(m + \sqrt{m^2+4})$ is a Fermat factor. In fact, for this $\xi(m)$ we will prove that (1.3) is valid for all odd p. To see that this is a non-trivial generalization, let us consider a numerical example.

Example 1.2. Let $p = 23$, $m = 5$, then $m\xi(m) = \frac{5+\sqrt{29}}{2} = 5.19258\cdots$. Then

$$5^{23} = 11920928955078125 \equiv 5 \bmod 23,$$

and, at the same time,

$$nint[(5.19258\cdots)^{23}] = 28432702285107160 \equiv 5 \bmod 23.$$

We will be searching for Fermat factors explicitly given by expressions depending on m of algebraic degree not exceeding 3 (i.e. containing only square and cubic roots). The main result of our paper is given in the following theorem.

Theorem 1.3. (*a*) *The number* 1 *has an infinite number of Fermat factors of arbitrary large algebraic degree.*

(*b*) *The number* 2 *has at least three Fermat factors of algebraic degree at most* 3.

(*c*) *Every natural number greater than* 2 *has at least four Fermat factors of algebraic degree at most* 3.

2. Auxiliary Results

We will need the following simple results.

Lemma 2.1. *Let $P(x)$ be a polynomial. Then*

$$\mathrm{Coef}_{x^{n-1}}\big((P(x))^{k-1} \cdot P'(x)\big) = \frac{n}{k}\,\mathrm{Coef}_{x^n}(P(x))^k. \tag{2.1}$$

Proof. Straightforward. □

The next reults follow from the Cauchy residues formula.

Lemma 2.2. *Let $P(x)$ be a polynomial of degree k. Then for small enough ρ,*

$$\frac{1}{2\pi i}\oint_{|w|=\rho} \frac{P'(w)}{1-P(w)}\frac{dw}{w^n} = \sum_{i=1}^{n} \xi_i^n,$$

where $\xi_i, i = 1, 2, \ldots, k$, are the roots (*with multiplicities*) *of the adjoint polynomial*

$$P^*(x) = x^k\left(1 - P\left(\frac{1}{x}\right)\right). \tag{2.2}$$

Proof. Follows from the Cauchy theorem since for small enough ρ the function $\frac{P'(w)}{1-P(w)}$ has the poles outside the circle of radius ρ, and all of them are simple. □

Lemma 2.3. *Let $P(x)$ be a polynomial, and $P(0) = 0$. Then*

$$\sum_{j\geq 1} \mathrm{Coef}_{x^{n-1}}(P(x))^{j-1}P'(x) = \frac{1}{2\pi i}\oint_{|w|=\rho} \frac{P'(w)}{1-P(w)}\frac{dw}{w^n}.$$

Proof. By the Cauchy theorem for ρ small enough we have

$$\sum_{j\geq 1} \mathrm{Coef}_{x^{n-1}}(P(x))^{j-1}P'(x) = \frac{1}{2\pi i}\oint_{|w|=\rho} \sum_{j\geq 1}(P(w))^{j-1}P'(w)\frac{dw}{w^n}.$$

Notice that the summation under the integral is possible since by $P(0) = 0$ the summands in the left sum are zero starting from some index j. Choose ρ small enough such that

$$\{w : |w| = \rho\} \subset \left\{w : |P(w)| \leq \frac{1}{2}\right\}.$$

This is again possible since $P(0) = 0$. Then the series $\sum_{j\geq 1}(P(w))^{j-1}$ converges uniformly on the integration contour to the function $\frac{1}{1-P(w)}$. □

Lemma 2.4. *Let* $P(x) = x + \sum_{r=2}^{k} a_r x^r$, *then*

$$\sum_{j=1}^{n-1} \frac{n}{j}\,\mathrm{Coef}_{x^n}(P(x))^j = -1 + \sum_{j=1}^{k} \xi_j^n,$$

where ξ_j *are the roots of* $P^*(x)$ (*see* (2.2)) *with their multiplicities.*

Proof. By Lemma 2.1

$$\sum_{j=1}^{n} \mathrm{Coef}_{x^{n-1}}(P(x))^{j-1}P'(x) = \sum_{j=1}^{n} \frac{n}{j}\,\mathrm{Coef}_{x^n}(P(x))^j = 1 + \sum_{j=1}^{n} \frac{n}{j}\,\mathrm{Coef}_{x^n}(P(x))^j.$$

Then using Lemmas 2.2 and 2.3 we have

$$\begin{aligned}\sum_{j=1}^{n} \frac{n}{j}\,\mathrm{Coef}_{x^n}(P(x))^j &= -1 + \sum_{j=1}^{n} \mathrm{Coef}_{x^{n-1}}(P(x))^{j-1}P'(x)\\ &= -1 + \frac{1}{2\pi i}\oint_{|w|=\rho} \frac{P'(w)}{1-P(w)}\frac{dw}{w^n} = -1 + \sum_{j=1}^{k} \xi_j^n.\end{aligned}$$ □

3. Polynomials with Special Properties

Definition 3.1. A sequence of polynomials P_n, $n = 1, 2, \ldots$, with integer coefficients is said to possess $\mathcal{P}$-property if for every prime p all the coefficients of P_p are divisible by p.

The next theorem provides a simple method to generate polynomials having $\mathcal{P}$-property.

Theorem 3.2. *Let*

$$T_x(z) = z^k - z^{k-1} - a_2(x)z^{k-2} - \cdots - a_k(x) \tag{3.1}$$

satisfy

$$T_x(0) \neq 0, \quad T_x(1) \neq 0, \tag{3.2}$$

and $a_i(x), i = 2, \dots, k$, be polynomials with integer coefficients. Let there exist an infinite set E of values x on which $T_x(z)$ has only simple roots $\xi_1(x), \xi_2(x), \dots, \xi_k(x)$. Let moreover the sequence of polynomials $R_n(x)$ be defined by recurrence

$$R_n(x) = R_{n-1}(x) + a_2(x)R_{n-2}(x) + \cdots + a_k(x)R_{n-k}(x) + a_2(x) + \cdots + a_k(x), \tag{3.3}$$

with the initial conditions

$$R_i(x) = s_i(x) - 1, \quad i = 1, 2, \dots, k, \tag{3.4}$$

where

$$s_i(x) = \sum_{j=1}^{k} \xi_j^i(x), \tag{3.5}$$

i.e. $s_i(x)$ are power sums of the roots of $T_x(z)$.

Then $R_n(x)$ possess $\mathcal{P}$-property.

Proof. By (3.2), $R_n(x) = -1$ is a particular solution to (3.3)–(3.4). Let now $x \in E$. Since $T_x(z)$ is the characteristic polynomial of (3.3) with no multiple roots, the general solution to (3.3) has form

$$R_n(x) = -1 + \sum_{j=1}^{k} c_j \xi_j^n(x), \quad x \in E. \tag{3.6}$$

By (3.4)–(3.6), we have

$$-1 + \sum_{j=1}^{k} c_j \xi_j^n(x) = -1 + \sum_{j=1}^{k} \xi_j^n(x).$$

Since a system of linear equations defined by the Vandermonde matrix (notice that $\xi_j \neq 0$ by (3.2) and all ξ_j's are pair-wise distinct) has a unique solution, this yields that $c_j = 1$ for $j = 1, 2, \dots, k$. Thus

$$R_n(x) = -1 + \sum_{j=1}^{k} \xi_j^n(x), \quad x \in E. \tag{3.7}$$

Notice now that $T(z) = P^*(z)$, where

$$P(z) = z + a_2(x)z^2 + \cdots + a_k(x)z^k. \tag{3.8}$$

Therefore, by Lemma 2.4 and (3.7),

$$R_n(x) = \sum_{i=1}^{n-1} \frac{n}{i} \operatorname{Coef}_{z^n}(P(z))^i, \quad x \in E. \tag{3.9}$$

It is well known that a polynomial is uniquely defined by its values at a set of points of size greater than the degree. Therefore, since E is an infinite set, (3.9) holds for all x.

It is left to notice that since $a_i(x), i = 2, \dots, k$, are polynomials with integer coefficients, the power sums of their roots, $s_i(x)$, are as well polynomials with integer coefficients (it follows e.g. from the Newton formulas for power sums). Then from (3.3) and (3.4) it follows that $\{R_n(x)\}$ are polynomials with integer coefficients. If now n is a prime, then all $i \le n-1$ do not divide n. Therefore,

$$\frac{R_n(x)}{n} = \sum_{i=1}^{n-1} \frac{1}{i} \operatorname{Coef}_{z^n}(P(z))^i,$$

is a polynomial with integer coefficients. □

Theorem 3.3. *Let k be an integer greater than 1. The sequence of polynomials $\{R_n(x)\}$ defined by the recurrence*

$$R_n(x) = R_{n-1}(x) + xR_{n-2}(x) + \cdots + xR_{n-k}(x) + (k-1)x, \quad n \ge k+1, \tag{3.10}$$

with initial conditions

$$R_i(x) = 2\sum_{h=1}^{\lfloor \frac{i}{2} \rfloor} \binom{i}{2h} x^h, \quad i = 1, 2, \ldots, k, \tag{3.11}$$

possesses $\mathcal{P}$-property.

Proof. For $x \ne 0$ consider the polynomial

$$T_x(z) = z^k - z^{k-1} - xz^{k-2} - \cdots - xz - x, \tag{3.12}$$

being the characteristic polynomial of (3.10). Condition (3.2) clearly holds for it. It is easy to see that $T_x(z)$ can have multiple roots on an at most finite set of x's. Indeed, the system

$$\begin{cases} T_x(z) = 0 \\ \dfrac{d}{dz}T_x(z) = 0 \end{cases},$$

for $z \ne 1$ is equivalent to

$$\begin{cases} z^{k+1} - 2z^k - (x-1)z^{k-1} + x = 0 \\ kz^{k+1} - (3k-1)z^k + ((3-x)k + 2x - 2)z^{k-1} + (k-1)(x-1)z^{k-2} - x = 0 \end{cases}. \tag{3.13}$$

Dividing the sum of the equations by $(z-1)$ we get

$$(k+1)z^2 - 2kz - (k-1)(x-1) = 0.$$

Plugging the roots of this quadratic equation into (3.13) we arrive at an equation in x of finite degree. Thus all the conditions of Theorem 3.2 are valid, and (3.10) plays the role of (3.3) for the polynomial $T_x(z)$ (3.12). It is left to check the coincidence of conditions (3.11) and (3.4). Notice that the power sums of the roots of the first equation from (3.13) are $s_i(x) + 1$ where $s_i(x)$ are power sums of the roots of (3.12),

$i = 1, \ldots, k$. On the other hand the symmetric polynomials $\sigma_i(x)$ of the roots of the first equation of (3.13) are

$$\sigma_1(x) = 2, \quad \sigma_2(x) = 1 - x, \quad \sigma_3(x) = \cdots = \sigma_k(x) = 0.$$

Using the Newton formulas expressing the power sums via the symmetric sums we get

$$s_i(x) + 1 - 2(s_{i-1}(x) + 1) + (1 - x)(s_{i-2}(x) + 1) = 0, \quad i = 1, 2, \ldots, k,$$

or

$$s_i(x) - 2s_{i-1}(x) + (1 - x)s_{i-2}(x) - x = 0.$$

Solving this recurrence with initial conditions $s_1(x) = 1, s_2(x) = 1+2x$, we find that

$$\begin{aligned} s_i(x) &= (1 + \sqrt{x})^i + (1 - \sqrt{x})^i - 1 \\ &= 1 + 2\sum_{h=1}^{\lfloor \frac{i}{2} \rfloor} \binom{i}{2h} x^h, \quad i = 1, \ldots, k. \end{aligned} \tag{3.14}$$

Comparing (3.11) and (3.14) we conclude that

$$R_i(x) = s_i(x) - 1,$$

that coincides with (3.4). Thus by Theorem 3.2 $\{R_n(x)\}$ possesses the $\mathcal{P}$-property. □

4. Fermat Factors of Natural Numbers

Theorem 4.1. (*a*) *The number*

$$\xi_1 = \frac{1}{2}\left(1 + \sqrt{1 + \frac{4}{m^2}}\right) \tag{4.1}$$

is a Fermat factor of any natural m.

(*b*) *The number*

$$\xi_2 = \frac{1}{2}\left(1 + \sqrt{1 - \frac{4}{m^2}}\right) \tag{4.2}$$

is a Fermat factor of any natural $m \geq 3$.

Proof. (a) Consider the sequence of polynomials $\{R_n(x)\}$ defined in (3.10)–(3.11) and possessing the $\mathcal{P}$-property. Using induction we obtain that

$$\deg R_n(x) = \left\lfloor \frac{n}{2} \right\rfloor. \tag{4.3}$$

Evidently that along with $\{R_n(x)\}$ the sequence $\left\{x^{\lfloor \frac{n}{2} \rfloor} R_n\left(\frac{1}{x}\right)\right\}$ possesses the $\mathcal{P}$-property. Furthermore, by (3.7),

$$R_n(x) = -1 + \sum_{j=1}^{k} \eta_j^n(x), \tag{4.4}$$

where $\{\eta_j(x)\}$ are the roots of $T_x(z)$, see (3.12). Let $k = 2$. Then

$$\eta_{1,2}(x) = \frac{1}{2}\big(1 \pm \sqrt{1+4x}\big), \quad x > 0.$$

By (4.4)

$$x^{\lfloor \frac{n}{2} \rfloor} R_n\left(\frac{1}{x}\right) = x^{\lfloor \frac{n}{2} \rfloor}\left(\left(\frac{1}{2}\left(1+\sqrt{1+\frac{4}{x}}\right)\right)^n + \left(\frac{1}{2}\left(1-\sqrt{1+\frac{4}{x}}\right)\right)^n - 1\right). \tag{4.5}$$

Let $x = m^2$, $n = p$, an odd prime, and m be not divisible by p. Then,

$$m^{p-1} R_p\left(\frac{1}{m^2}\right) = m^{p-1}\left(\left(\frac{1}{2}\left(1+\sqrt{1+\frac{4}{m^2}}\right)\right)^p + \left(\frac{1}{2}\left(1-\sqrt{1+\frac{4}{m^2}}\right)\right)^p\right) - m^{p-1} \equiv 0 \bmod p. \tag{4.6}$$

Multiplying both sides of this congruence by m and using the Fermat theorem we get

$$\left(\frac{m+\sqrt{m^2+4}}{2}\right)^p + \left(\frac{m-\sqrt{m^2+4}}{2}\right)^p \equiv m \bmod p.$$

Since $\sqrt{m^2+4} - m$ decreases in m, we have

$$\left(\frac{\sqrt{m^2+4}-m}{2}\right)^p \leq 0.62^p < \frac{1}{2}.$$

Therefore, given p does not divide m,

$$nint\big[m\xi_1^p\big] \equiv m \bmod p. \tag{4.7}$$

If $m \equiv 0 \bmod p$, the left-hand side of (4.6) is a polynomial in m^2 (here it is essential that $p \neq 2$) with all coefficients divisible by p. Therefore, also

$$m^p R_p\left(\frac{1}{m^2}\right) - m^p \equiv 0 \bmod p,$$

and (4.7) follows.

(b) The proof is analogous but instead of $x = m^2$ in (4.5) we set $x = -m^2$. □

It follows from Theorem 4.1 that every natural m possesses a Fermat factor of algebraic degree 2 for every odd p. Let us consider now Fermat factors of degree 3.

Theorem 4.2. *The numbers*

$$\xi_1 = \frac{1}{3}\left(1 + \sqrt[3]{1+\frac{18}{m^2}+\frac{3}{m^3}\sqrt{3m^4+33m^2-3}} + \sqrt[3]{1+\frac{18}{m^2}-\frac{3}{m^3}\sqrt{3m^4+33m^2-3}}\right), \tag{4.8}$$

$$\xi_2 = \frac{1}{3}\left(1 + \sqrt[3]{1 + \frac{45}{2m^2} + \frac{3}{2m^3}\sqrt{12m^4 + 177m^2 - 96}} + \sqrt[3]{1 + \frac{45}{2m^2} - \frac{3}{2m^3}\sqrt{12m^4 + 177m^2 - 96}}\right), \tag{4.9}$$

are Fermat factors of any natural m.

Proof. Set in (4.4) $k = 3$. We have

$$R_n(x) = \eta_1^n(x) + \eta_2^n(x) + \eta_3^n(x) - 1, \tag{4.10}$$

where $\eta_i, i = 1, 2, 3$, are the roots of $T_x(z)$ (3.12),

$$T_x(z) = z^3 - z^2 - xz - x. \tag{4.11}$$

Therefore,

$$x^{\lfloor \frac{n}{2} \rfloor} R_n\left(\frac{1}{x}\right) = x^{\lfloor \frac{n}{2} \rfloor}\big(\zeta_1^n(x) + \zeta_2^n(x) + \zeta_3^n(x) - 1\big), \tag{4.12}$$

where

$$\zeta_i(x) = \eta_i\left(\frac{1}{x}\right), \quad i = 1, 2, 3, \ldots, \tag{4.13}$$

are the roots of $T_{\frac{1}{x}}(z)$ (4.11),

$$T_{\frac{1}{x}}(z) = z^3 - z^2 - \frac{1}{x}z - \frac{1}{x}. \tag{4.14}$$

Moreover, the polynomials $\left\{x^{\lfloor \frac{n}{2} \rfloor} R_n\left(\frac{1}{x}\right)\right\}$ are integer-valued for integer x, and possess the $\mathcal{P}$-property.

Let us show that for $x \geq 1$ the polynomial $T_{\frac{1}{x}}(z)$ (4.14) has the unique real root, $\zeta_1 > 1$. Indeed,

$$\frac{d}{dz}T_{\frac{1}{x}}(z) = 3z^2 - 2z - \frac{1}{x},$$

and $T_{\frac{1}{x}}(z)$ has a local maximum in $z = \frac{1}{3}\big(1 - \sqrt{1 + \frac{3}{x}}\big)$. However, for $x \geq 1$,

$$\begin{aligned} T_{\frac{1}{x}}\left(\frac{1}{3}\left(1 - \sqrt{1 + \frac{3}{x}}\right)\right) &= \frac{1}{27x}\left((2x + 15)\sqrt{1 + \frac{3}{x}} - 2x - 45\right) \\ &< \frac{1}{27x}\left((2x + 15)\left(1 + \frac{3}{2x}\right) - 2x - 45\right) \\ &= \frac{5}{6x^2} - \frac{1}{x} \leq -\frac{1}{6}. \end{aligned}$$

Thus $T_{\frac{1}{x}}(z)$ has the unique real root $\zeta_1(x)$, and since $T_{\frac{1}{x}}(1) = -\frac{2}{x} < 0$, we conclude that $\zeta_1(x) > 1$, and we are done.

Let now $x = m^2$, where m is a positive integer. If ζ_2 and $\bar{\zeta}_2$ are complex conjugate roots of $T_{\frac{1}{m^2}}(z)$ then by Vieta's theorem

$$|\zeta_2| = |\bar{\zeta}_2| = \sqrt{\frac{1}{m^2\zeta_1}} = \frac{1}{m}\frac{1}{\sqrt{\zeta_1}}. \tag{4.15}$$

Let $n = p \geq 3$, be a prime number, and p does not divide m. By (4.12)

$$m^{p-1}\big(\zeta_1^p + \zeta_2^p + \bar{\zeta}_2^p - 1\big) \equiv 0 \bmod p. \tag{4.16}$$

Multiplying by m and using the Fermat theorem we get

$$(\zeta_1 m)^p + (\zeta_2 m)^p + (\bar{\zeta}_2 m)^p \equiv m \bmod p. \tag{4.17}$$

Taking into account that $\zeta_1 > 1$ we can choose p such that

$$\left(\frac{1}{\sqrt{\zeta_1}}\right)^p < 0.25.$$

Then by (4.15)

$$\big|(\zeta_2 m)^p + (\bar{\zeta}_2 m)^p\big| < 0.5.$$

By (4.17) for the relevant p's we find that

$$nint\big[(\zeta_1 m)^p\big] \equiv m \bmod p. \tag{4.18}$$

It is left to notice that $\xi_1 = \zeta_1$ is indeed the positive root of $T_{\frac{1}{x}}(z)$ when $x = m^2$.

The proof for ξ_2 (4.9) is quite analogous and uses the polynomial

$$T_x(z) = z^3 - z^2 - 2xz - x, \quad x \neq 0. \tag{4.19}$$

□

Example 4.3. For $m = 3$ by (4.9) we have $\xi_2 = 1.249115513\cdots$, and

$$nint\big[(3\xi_2)^p\big] \equiv 3 \bmod p,$$

is valid only for prime $p \geq 13$. Thus,

$$nint\big[(3\xi_2)^{11}\big] = 2046268 \equiv 4 \bmod 11,$$
$$nint\big[(3\xi_2)^{13}\big] = 28734930 \equiv 3 \bmod 13.$$

Indeed,

$$\left(\frac{1}{\xi_2}\right)^{11} = 0.29\cdots > 0.25, \quad \left(\frac{1}{\xi_2}\right)^{13} = 0.23\cdots < 0.25.$$

The Fermat factors of 1 will be considered in Sec. 6.

5. Simple Generalizations

In this section we will present some simple generalization of the previous results. If in Theorems 4.1 and 4.2 instead of $x = m^2$ we assume $x = m$, then with almost the same proof we arrive at the following generalization of the Euler congruence:

$$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \bmod p$$

valid for odd p's and all natural m not divisible by p. Here $\left(\frac{m}{p}\right)$ is the Legendre symbol,

$$\left(\frac{m}{p}\right) = \begin{cases} 1, & \text{if } \exists x : x^2 \equiv m \bmod p, \\ -1, & \text{otherwise.} \end{cases}$$

The Euler congruence can be reformulated as

$$\sqrt{m}(\lambda(m))^p \equiv m \left(\frac{m}{p}\right) \bmod p \tag{5.1}$$

where $\lambda(m) = \sqrt{m}$. Our goal is to find other options for $\lambda(m)$ satisfying (5.1) with the *nint* function used on the left-hand side.

Theorem 5.1. *We have*

$$nint[\sqrt{m}(\lambda(m))^p] \equiv m \left(\frac{m}{p}\right) \bmod p \tag{5.2}$$

if

(a) *for any natural m and every odd prime p,*

$$\lambda(m) = \frac{\sqrt{m} + \sqrt{m+4}}{2}; \tag{5.3}$$

(b) *for $m \geq 5$ and every odd prime p,*

$$\lambda(m) = \frac{\sqrt{m} + \sqrt{m-4}}{2}; \tag{5.4}$$

(c) *for any natural m and large enough prime p,*

$$\lambda(m) = \frac{1}{3}\left(\sqrt{m} + \sqrt[3]{m\sqrt{m} + 18\sqrt{m} + 3\sqrt{3(m^2+11m-1)}} + \sqrt[3]{m\sqrt{m} + 18\sqrt{m} - 3\sqrt{3(m^2+11m-1)}}\right); \tag{5.5}$$

(d) *for any natural m and large enough prime p,*

$$\lambda(m) = \frac{1}{3}\left(\sqrt{m} + \sqrt[3]{m\sqrt{m} + 45\sqrt{m} + \frac{3}{2}\sqrt{3(4m^2+59m-32)}} + \sqrt[3]{m\sqrt{m} + 45\sqrt{m} - \frac{3}{2}\sqrt{3(4m^2+59m-32)}}\right). \tag{5.6}$$

Well-known particular values of the Legendre symbol (see e.g. [3]) yield the following corollary.

Corollary 5.2. *For odd* p

$$nint\left[\sqrt{2}\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{p}\right] \equiv \begin{cases} 2 \bmod p & \text{if } p \equiv \pm 1 \bmod 8 \\ -2 \bmod p & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

$$nint\left[\sqrt{3}\left(\frac{\sqrt{3}+\sqrt{7}}{2}\right)^{p}\right] \equiv \begin{cases} 3 \bmod p & \text{if } p \equiv \pm 1 \bmod 12 \\ -3 \bmod p & \text{if } p \equiv \pm 5 \bmod 12 \end{cases}$$

$$nint\left[\sqrt{5}\left(\frac{\sqrt{5}+1}{2}\right)^{p}\right] \equiv nint\left[\sqrt{5}\left(\frac{\sqrt{5}+3}{2}\right)^{p}\right]$$

$$\equiv \begin{cases} 5 \bmod p & \text{if } p \equiv \pm 1 \bmod 5 \\ -5 \bmod p & \text{if } p \equiv \pm 2 \bmod 5 \end{cases}.$$

This list can be easily extended. Other interesting congruences can be derived from representations of primes, $p \equiv 1 \mod 4$, as a sum of two mutually prime squares. It is known (see e.g. [3]) that this representation is unique, and the square root of the odd summand is a quadratic residue modulo p.

Example 5.3. Let $p = 53 = 7^2 + 2^2$. Therefore $\left(\frac{7}{53}\right) = 1$, and by the theorem

$$nint\left[\sqrt{7}\left(\frac{\sqrt{7}+\sqrt{11}}{2}\right)^{53}\right] \equiv nint\left[\sqrt{7}\left(\frac{\sqrt{7}+\sqrt{3}}{2}\right)^{53}\right] \equiv 7 \bmod 53.$$

6. Fermat Factors of 1

Lemma 6.1. (*a*) *For* $x \in (0,1)$, *and odd* k, $k \geq 3$,

$$T_x(z) = z^k - z^{k-1} - xz^{k-2} - \cdots - xz - x, \tag{6.1}$$

has the unique real root, $\xi_1 \in (1, 1+\sqrt{x})$.

(*b*) *For* $x \in (0,1)$, *and even* k, $k \geq 4$, $T_x(z)$ *has exactly two real roots*, $\xi_1 \in (1, 1+\sqrt{x})$, $\xi_2 \in (-x^{\frac{1}{k+1}}, 0)$.

Proof. (a) Let

$$U_x(z) = T_x(z)(z-1) = z^{k+1} - 2z^k + (1-x)z^{k-1} + x. \tag{6.2}$$

The derivative $\frac{dU_x(z)}{dz}$ has zero $z_1 = 0$ of odd multiplicity $(k-2)$, and two other zeros

$$z_{2,3} = \frac{1}{k+1}\left(k \pm \sqrt{(k^2-1)x+1}\right) > 0.$$

Moreover, $U_x(z)$ has local minimum at z_2, $z_2 > 1$, and local maximum at $z_3 \in (0,1)$. Since $U_x(1) = 0$, then $U_x(z_2) < 0$, $U_x(z_3) > 0$. Therefore, there exists a real root ξ_1 of $U_x(z)$, and thus of $T_x(z)$. Clearly $\xi_1 > z_2 > 1$. However, since $T_x(1+\sqrt{x}) = x > 0$,

$$\xi_1 \in (1, 1+\sqrt{x}). \tag{6.3}$$

At $z_1 = 0$ we have a local minimum of $U_x(z)$. However, $U_x(0) > 0$. This means that whence $z < 1$, $U_x(z) > 0$. Thus ξ_1 from (6.3) is the unique real root of $T_x(z)$.

(b) Again we have local minimum and maximum at z_2 and z_3. However, now $z_1 = 0$ is the root of even multiplicity. Therefore, to the left of z_3, $U_x(z)$ grows from $-\infty$ up to $U_x(z_3) > 0$. Thus, along with ξ_1 from (6.3), $U_x(z)$, as well as $T_x(z)$, has another real root ξ_2. Since $U_x(0) > 0$, and

$$U_x(-x^{\frac{1}{k+1}}) = -2x^{\frac{k}{k+1}} - (1-x)x^{\frac{k-1}{k+1}} < 0,$$

we deduce $\xi_2 \in (-x^{\frac{1}{k+1}}, 0)$. □

Lemma 6.2. *For small enough x, the absolute values of all roots of $T_x(z)$ defined in* (6.1) *but $\xi_1 > 1$, are less than* 1.

Proof. The roots of a polynomial are continuous functions of its coefficients. In our case the roots of $T_x(z)$ continuously depend on x. When $x \to +0$, by Lemma 6.1, $\xi_1 \to 1+0$, and (existing for even k) the second real root $\xi_2 \to 0$. At $x = 0$,

$$T_0(z) = z^k - z^{k-1}.$$

This polynomial has two zeros, $z_1 = \xi_1 = 1$ and $(k-1)$-fold root $z_2 = 0$. This means that all complex roots of $T_x(z)$ tend to 0. □

Theorem 6.3. *For large enough m and $k \geq 2$, the positive root $\xi = \xi(m)$ of*

$$T(z) = mz^k - mz^{k-1} - z^{k-2} - \cdots - z - 1 \tag{6.4}$$

is a Fermat factor of 1.

Proof. Consider the sequence of polynomials $\{R_n(x)\}$ defined in (3.10)–(3.11), possessing the $\mathcal{P}$-property. Then, as it was mentioned before, $\{x^{\lfloor \frac{n}{2} \rfloor} R_n(\frac{1}{x})\}$ also possesses the $\mathcal{P}$-property. Moreover,

$$R_n\left(\frac{1}{x}\right) = -1 + \sum_{j=1}^{k} \xi_j^n(x), \tag{6.5}$$

where $\xi_j(x)$ are the roots of $T_{\frac{1}{x}}(z)$ defined in (3.12), which for $x = m$ coincide with the roots of $T(z)$ defined in (6.4). On the other hand, by Lemma 6.2 for large enough m all the zeros of $T_{\frac{1}{m}}(z)$ but $\xi_1 > 1$ have absolute value less than 1. For $x = m$ and odd prime $n = p$, by (6.5),

$$m^{\frac{p-1}{2}}\left(-1 + \sum_{j=1}^{k} \xi_j^p(m)\right) \equiv 0 \bmod p. \tag{6.6}$$

Let p not divide m. Then (6.6) yields

$$\sum_{j=1}^{k} \xi_j^p(m) \equiv 1 \bmod p.$$

Notice that this also holds for m divisible by p, since the coefficients of $R_n\left(\frac{1}{x}\right)$ are divisible by p when $n = p$.

For large enough m, we have $|\xi_j| < 1$, $j = 2, 3, \ldots, k$, and for large enough p,

$$\left|\sum_{j=2}^{k} \xi_j^p(m)\right| \leq 0.5,$$

and

$$nint\left[\xi_1^p\right] \equiv 1 \bmod p. \qquad \square$$

The following result demonstrates that there exist Fermat factors of 1 of arbitrary large algebraic degree. We will use the following well-known statement, see e.g. [4, Sec. 8, Chap. 2, Sec. 3].

Lemma 6.4. *Let $P(x)$ be an integer-valued polynomial of degree k, and let there exist an integer ℓ satisfying*

(i) *the zeros of $P(x)$ lie in the half-plane $\Re e\, x < k - \frac{1}{2}$;*
(ii) $P(\ell - 1) \neq 0$;
(iii) *$P(\ell)$ is a prime.*

Then $P(x)$ is irreducible over rationals.

Theorem 6.5. *For any even $k \geq 4$, there exist arbitrary large m such that $T(z)$ from* (6.4) *is irreducible.*

Proof. We will show that $\ell = 3$ for some arbitrary large m satisfies all conditions of Lemma 6.4. Indeed, from Lemmas 6.1 and 6.2 it follows that for large enough m the zeros of $T(z)$ lie within the circle $|z| < 2$, belonging to half-plane $\Re e\, z < 4 - \frac{1}{2} \leq k - \frac{1}{2}$. Moreover,

$$T(2) = m2^{k-1} - 2^{k-2} - \cdots - 2 - 1 = (m-1)2^{k-1} + 1 \neq 0.$$

Finally, the numbers

$$T(3) = 2m\, 3^{k-1} - (3^{k-2} + 3^{k-3} + \cdots + 3 + 1),$$

constitute an arithmetic progression when m varies. The initial term of the progression is $a = 2 \cdot 3^{k-1} - (3^{k-2} + 3^{k-3} + \cdots + 3 + 1)$, and the difference is $d = 2 \cdot 3^{k-1}$. Since k is even, a is odd and not divisible by 3. Therefore a and d are mutually prime. Thus by the Dirichlet theorem there exists arbitrary large m for which $T(3)$ is prime. □

7. Open Problems

We suggest the following research problems on Fermat factors.

(i) The Pisot number is defined as a real root of a polynomial with integer coefficients with absolute value greater than 1, such that all its conjugates have absolute value strictly less than 1, see [1]. It is easy to check that all our examples of Fermat factors are Pisot numbers. Are there Fermat factors which are not Pisot numbers? Is it possible for every Pisot number to find an integer for which it is a Fermat factor?

(ii) Are there Fermat factors of numbers greater than 1 having algebraic degree more than 3? Do numbers exceeding 1 have an infinite number of Fermat factors?

(iii) There are many applications of the Fermat theorem in cryptography, see e.g. [2]. Are there interesting ways for use of the suggested generalization to cryptographic problems?

Acknowledgments

We are grateful to the anonymous referee for useful comments.

The first author's reasearch was supported in part by ISF Grant 553-03.

The second author's research was supported in part by the Giladi Foundation of the Israeli Ministry of Absorption.

References

[1] M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Huget, M. Pathiaux-Delefosse and J. P. Schreiber, *Pisot and Salem Numbers* (Birkhäuser-Verlag, 1992).

[2] G. J. Simmons (ed.), *Contemporary Cryptology* (IEEE Press, 1992).

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer-Verlag, 1982).

[4] G. Polya and G. Szegö, *Problems and Theorems in Analysis, II* (Springer-Verlag, New York, 1972).