PRIME NUMBERS AND CYCLOTOMY

Panayiotis G. Tsangaris (Athens, Greece)

Abstract. First, an explicite expression for \((1 - \zeta^k)^{-1}\), where \(\zeta = \exp(2\pi i/n)\), is given, in the form of a polynomial in \(\zeta\), with rational coefficients. Then a new primality criterion is obtained, which involves the greatest integer function. Further, using a result due to Yu.I. Vološin [10], we transform this criterion into a series of criteria involving rational expressions of \(\zeta\) [one of these criteria involves the numbers \((1 - \zeta^k)^{-1}, 1 \leq k \leq n - 1\)]. Finally, these criteria are refined to a trigonometric primality criterion, that involves only sums of cosines.

AMS Classification Number: 11A51, 11R18

Introduction

Denote by \(F_n(x)\) the \(n\)-th cyclotomic polynomial, while \(\phi\) will denote Euler’s function and \(\zeta = \exp(2\pi i/n)\). Given two polynomials \(f(v), g(v)\) in variable \(v\), denote by \(R_v(f(v), g(v))\) their resultant.

In Section 1 we express \((1 - \zeta^k)^{-1}\), explicitly, in the form of a polynomial in \(\zeta\), by employing a series of new properties of the cyclotomic polynomial (Theorems 1.1 and 1.2).

In Section 2 a new primality criterion is obtained. Our primality criterion (Theorem 2.1) extends a previous result of author [7] which improves upon classical result of Hacks [5].

In Section 3 the result of (Section 2) is given in “cyclotomic” form by using roots of unity and trigonometric functions. The key result for such a “cyclotomic” modification is a Theorem of Yu. I. Vološin [10] expressing \([a/n]\) by means of a primitive root of 1 of order \(n\). Specifically, our Theorem 3.1 is a first primality criterion for \(n\) formulated in terms of \(\zeta\) and involving \((1 - \zeta^k)^{-1}, 1 \leq k \leq n - 1\). To calculate the inverse of \((1 - \zeta^k)\) (Corollary 1.4), we thus obtain a second “cyclotomic” primality criterion (Theorem 3.2). The “trigonometric elaboration” of this result leads to our final Theorem 3.4, which is a “trigonometric” primality criterion.

1. Expressing \((1 - \zeta^k)^{-1}\) as a polynomial in \(\zeta\)

Theorem 1.1. Let \(n, s\) be natural numbers and let \(d = (n, s)\). Then
\[ R_v(v^s - x^s, F_n(v)) = \begin{cases} F_{n/d}(x^s)^{\phi(n)/\phi(n/d)} & \text{for } n > 1 \text{ except for } d = n = 2, \\ -F_1(x^s) = 1 - x^s & \text{for } d = n = 2, \\ (-1)^{s+1}F_1(x^s) = (-1)^{s+1}(x^s - 1) & \text{for } n = 1. \end{cases} \]

**Proof.** Let \( R(x) = R_v(v^s - x^s, F_n(v)) \), \( G(x) = F_{n/d}(x^s)^{\phi(n)/\phi(n/d)} \) and \( \rho_1, \rho_2, \ldots, \rho_s \) be the \( s \)-th roots of unity. Then \( \rho_1x, \rho_2x, \ldots, \rho_sx \) are the roots of \( v^s - x^s \) (for \( x \) fixed). Hence

\[ R(x) = F_n(\rho_1x) \cdots F_n(\rho_sx). \]

Let \( \xi \) be a root of \( R(x) \). Hence, \( F_n(\rho_k\xi) = 0 \) for some \( k \), with \( 1 \leq k \leq s \), i.e. \( \rho_k\xi \) is a root of \( F_n(v) \). Thus, \( \rho_k\xi \) is a primitive \( n \)-th root of unity. Set \( \rho_k\xi = \zeta \), then \( \xi^s = \zeta^s \). But the order of \( \zeta^s \) is \( n/d \). Hence \( \xi^s \) is a primitive \( n/d \)-th root of unity, i.e.

\[ F_{n/d}(\xi^s) = 0. \]

Hence,

\[ F_{n/d}(\xi^s)^{\phi(n)/\phi(n/d)} = 0, \]

i.e. \( \xi \) is a root of \( G(x) \). Hence, every root of \( R(x) \) is a root of \( G(x) \), i.e.

\[ R(x) \mid G(x). \quad (1) \]

Also

\[ \deg G(x) = \deg R(x) = s\phi(n). \quad (2) \]

From (1) and (2) we have:

\[ G(x) = cR(x), \quad \text{where } c \text{ is a (rational) constant.} \quad (3) \]

Hence \( G(0) = cR(0) \), that is

\[ F_{n/d}(0)^{\phi(n)/\phi(n/d)} = cF_n(0)^s. \quad (4) \]

To derive the sought formula it suffices now to evaluate the constant \( c \). We have to examine two cases:

(a) If \( n > 1 \). In case \( d \neq n \), then \( n/d > 1 \). Also \( F_n(0) = 1 \) and \( F_1(0) = -1 \). Then, in view of (4) we have \( c = 1 \). In case \( d = n > 1 \), we have in view of (4) that

\[ c = (-1)^{\phi(n)} = \begin{cases} -1, & \text{if } n = 2, \\ 1, & \text{if } n > 2. \end{cases} \]
(b) If $n = 1$, then (4) implies that

$$c = \begin{cases} 
1, & \text{if } s \text{ is odd}, \\
-1, & \text{if } s \text{ is even}.
\end{cases}$$

**Remark.** Theorem 1.2 should be considered as closely related to a corresponding Theorem of T. Apostol [1] on the resultant of the cyclotomic polynomials $F_n(ax)$ and $F_n(bx)$.

**Theorem 1.2.** Let $n, s$ be natural numbers. Denote by $\rho_1, \rho_2, \ldots, \rho_s$ all the $s$-th roots of unity, and let

$$K_n^s(x) \equiv F_n(\rho_1 x) \cdots F_n(\rho_s x) - F_n(\rho_1) \cdots F_n(\rho_s).$$

Then:

(i) $(x^s - 1)|K_n^s(x)$.

(ii) If $n \nmid s$, then

$$(1 - \zeta^s)^{-1} = L_n^s(\zeta)/R(v^s - 1, F_n(v)),$$

where

$$L_n^s(x) = K_n^s(x)/(x^s - 1).$$

**Proof.** The numbers $\rho_1, \rho_2, \ldots, \rho_s$ form a cyclic group. Hence

$$K_n^s(\rho_k) = F_n(\rho_1 \rho_k) \cdots F_n(\rho_s \rho_k) - F_n(\rho_1) \cdots F_n(\rho_s) = 0 \text{ for } k = 1, 2, \ldots, s.$$ 

Also $\rho_1 x, \ldots, \rho_s x$ are the roots of $v^s - x^s = 0$ (for $x$ fixed). Thus

$$K_n^s(x) = R_v(v^s - x^s, F_n(v)) - R(v^s - 1, F_n(v))$$

is a polynomial of $x$ with integer coefficients. Since every $\rho_k$ is a root of $K_n^s(x)$, part (i) follows immediately. Then

$$L_n^s(\zeta) = K_n^s(\zeta)/(\zeta^s - 1)$$

and so

$$K_n^s(\zeta) = -F_n(\rho_1) \cdots F_n(\rho_s) = -R(v^s - 1, F_n(v)).$$

In conclusion

$$(1 - \zeta^s)^{-1} = L_n^s(\zeta)/R(v^s - 1, F_n(v)).$$

**Theorem 1.3.** Let $n, k$ be natural numbers such that $n > 1$, $n \nmid k$ and let $d = (n, k)$. Define

$$K_n^k(x) = F_n/d(x^k)^{\phi(n)/\phi(n/d)} - F_n/d(1)^{\phi(n)/\phi(n/d)}.$$
Then $x^k - 1$ is a divisor of $K_n^k(x)$, and

$$(1 - \zeta^k)^{-1} = L_n^k(\zeta)/F_{n/d}(1)^{\phi(n)/\phi(n/d)},$$

where

$L_n^k(x) = K_n^k(x)/(x^k - 1)$.

**Proof.** Immediate by using Theorems 1.1 and 1.2.

**Corollary 1.4.** If $n$ is a prime and $k < n$, then we have

$$(1 - \zeta^k)^{-1} = \frac{1}{n} \sum_{1 \leq w \leq n-1} w \zeta^{k(n-w-1)}.$$

**Proof.** Here $(n, k) = 1$ and $F_n(1) = n$, so by Theorem 1.3 we have

$L_n^k(x) = (F_n(x^k) - F_n(1))/(x^k - 1) = \sum_{1 \leq w \leq n-1} wx^{k(n-w-1)},$

which proves the corollary.

2. A Primality Criterion

The known formula of Hacks [5, p. 205] for the g.c.d. of two natural numbers

$$(n, j) = 2 \sum_{1 \leq i \leq n-1} [ji/n] - jn + j + n$$

together with the fact that $n$ is prime if and only if $\sum_{1 \leq j \leq m} (n, j) = m$ where $m = [\sqrt{n}]$ implies the following:

**Theorem 2.1.** Let $n$ be a natural number with $n > 1$, $m = [\sqrt{n}]$ and

$$g(n) = 4 \sum_{1 \leq j \leq m} \sum_{1 \leq i \leq n-1} [ji/n] - (m-1)m(n-1).$$

Then the following hold true:

(i) $n$ is prime if and only if $g(n) = 0$.

(ii) $n$ is composite if and only if $g(n) > 0$. 

3. Prime numbers, roots of unity, cyclotomy and trigonometry

By Vološin’s Theorem [10] we have:

\[
\left[ \frac{a}{n} \right] = \frac{a}{n} - \frac{n-1}{2n} - \frac{1}{n} \sum_{1 \leq s \leq n-1} \frac{\zeta^{s(a+1)}}{1 - \zeta^s}
\]  

(5)

for any pair of (positive) integers \(a, n\). Hence by (5) and Theorem 2.1 we have the following:

**Theorem 3.1.** Let \(n\) be a natural number with \(n > 1\) and \(m = [\sqrt{n}]\). Then, \(n\) is prime if and only if

\[
2 \sum_{1 \leq j \leq m} \frac{\zeta^{k(tj+1)}}{1 - \zeta^k} = m(n - 1).
\]

**Theorem 3.2.** Let \(n\) be a natural number with \(n > 1\) and \(m = [\sqrt{n}]\). Then \(n\) is prime if and only if

\[
2 \sum_{1 \leq j \leq m} \frac{\zeta^{tjk}(1 - \zeta^k)}{\zeta^{k(n-1)} + \zeta^k - 2} = m(n - 1).
\]

(6)

**Proof.** If \(n\) is a prime, by Theorem 3.1 and Corollary 1.4 we obtain:

\[
\frac{2}{n} \sum_{1 \leq j \leq m} \sum_{1 \leq t, k \leq n-1} \zeta^{(tj+1)k} w \zeta^{k(n-w-1)} = m(n - 1).
\]

(7)

Let \(\zeta^k = 1/z\). Clearly \(\zeta^k \neq 1\), i.e. \(z \neq 1\). Therefore

\[
\sum_{1 \leq w \leq n-1} w \zeta^{k(n-w-1)} = \frac{1}{z^{n-2}} \sum_{1 \leq w \leq n-1} w z^{w-1} = \frac{n(\zeta^{k(n-1)} - 1)}{\zeta^{k(n-1)} + \zeta^k - 2}.
\]

(8)

By (7) and (8) follows (6).

Assume now that (6) holds true. We have \(\zeta^{k(n-1)} + \zeta^k - 2 \neq 0\) and \(\zeta^{k(n-1)} \neq 1\) because \(\zeta^k \neq 1\). Also, the following hold true:

\[
\frac{1 - \zeta^k}{\zeta^{k(n-1)} + \zeta^k - 2} = \frac{1}{\zeta^{k(n-1)} - 1}.
\]

Hence

\[
\frac{\zeta^{tjk}(1 - \zeta^k)}{\zeta^{k(n-1)} + \zeta^k - 2} = \frac{\zeta^{k(tj+1)}}{1 - \zeta^k}.
\]
Hence by our assumption we have:

\[ m(n - 1) = 2 \sum_{1 \leq j \leq m} \frac{\zeta^{tjk}(1 - \zeta^k)}{\zeta^{k(n-1)} + \zeta^k - 2} = 2 \sum_{1 \leq j \leq m} \frac{\zeta^{k(tj+1)}}{1 - \zeta^k}. \]

Finally, by Theorem 3.1, \( n \) is prime Q.E.D.

Our next Lemma 3.3 aims at transforming the above Theorem 3.2 into a “trigonometric” primality criterion.

**Lemma 3.3.** Let \( m, n \) be natural numbers with \( n > 1 \) and \( m = \lfloor \sqrt{n} \rfloor \). Then

\[ 2 \sum_{1 \leq j \leq m} \frac{\zeta^{tjk}(1 - \zeta^k)}{\zeta^{k(n-1)} + \zeta^k - 2} = - \sum_{1 \leq j \leq m} \cos \frac{2\pi tjk}{n}. \]

**Proof.** The following hold true

\[ \zeta^{tjk}(1 - \zeta^k) = 2 \sin \frac{\pi k(2tj + 1)}{n} \sin \frac{\pi k}{n} - 2i \sin \frac{\pi k}{n} \cos \frac{\pi k(2tj + 1)}{n}. \] \hspace{1cm} (9)

Also

\[ \zeta^{k(n-1)} + \zeta^k - 2 = -4 \sin^2 \frac{\pi k}{n}. \] \hspace{1cm} (10)

From (9) and (10) we obtain:

\[ 2 \sum_{1 \leq j \leq m} \frac{\zeta^{tjk}(1 - \zeta^k)}{\zeta^{k(n-1)} + \zeta^k - 2} = - \sum_{1 \leq j \leq m} \frac{\sin \frac{\pi k(2tj + 1)}{n}}{\sin \frac{\pi k}{n}} \]

\[ + i \sum_{1 \leq j \leq m} \frac{\cos \frac{\pi k(2tj + 1)}{n}}{\sin \frac{\pi k}{n}}. \] \hspace{1cm} (11)

Moreover

\[ - \sum_{1 \leq j \leq m} \frac{\sin \frac{\pi k(2tj + 1)}{n}}{\sin \frac{\pi k}{n}} = - \sum_{1 \leq j \leq m} \sin \frac{2\pi tjk}{n} \cot \frac{\pi k}{n} \]

\[ - \sum_{1 \leq j \leq m} \cos \frac{2\pi tjk}{n}. \] \hspace{1cm} (12)
On the other hand
\[
\sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \frac{\cos \frac{\pi k(2tj+1)}{n}}{\sin \frac{\pi k}{n}} = \sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \cos \frac{2\pi tk}{n} \cot \frac{\pi k}{n} - \sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \sin \frac{2\pi tk}{n}. \quad (13)
\]

The following hold true
\[
\sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \sin \frac{2\pi tk}{n} \cot \frac{\pi k}{n} = 0, \quad (14)
\]
\[
\sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \cos \frac{2\pi tk}{n} \cot \frac{\pi k}{n} = 0 \quad (15)
\]

and
\[
\sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \sin \frac{2\pi tk}{n} = 0. \quad (16)
\]

Finally, by (11) together with (12), (13), (14), (15) and (16) we obtain:
\[
2 \sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \frac{\zeta^{tk}(1 - \zeta^k)}{\zeta^{k(n-1)} + \zeta^k - 2} = - \sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \cos \frac{2\pi tk}{n}.
\]

It is now clear that Theorem 3.2 and Lemma 3.3 imply the following

**Theorem 3.4.** Let \( n \) be a natural number with \( n > 1 \) and \( m = \lfloor \sqrt{n} \rfloor \). Then \( n \) is prime if and only if
\[
\sum_{1 \leq j \leq m \atop 1 \leq t, k \leq n-1} \cos \frac{2\pi tk}{n} = -m(n - 1).
\]

**References**


---

**Panayiotis G. Tsangaris**  
Department of Mathematics  
Athens University  
Panepistimiopolis, 15784 Athens  
Greece  
E-mail: ptsagari@cc.uoa.gr