On the least prime congruent to 1 modulo \( n \)

Jackson S. Morrow
On the least prime congruent to 1 modulo $n$

Jackson S. Morrow

(Communicated by Kenneth S. Berenhaut)

For any integer $n > 1$, there are infinitely many primes congruent to 1 (mod $n$). In this note, the elementary argument of Thangadurai and Vatwani is modified to improve their upper estimate of the least such prime when $n$ itself is a prime greater than or equal to 5.

**Preliminaries**

For any integer $n \geq 1$, the $n$-th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{1 \leq m \leq n \atop \gcd(m,n) = 1} (x - e^{2\pi im/n}).$$

This is a monic polynomial of degree $\varphi(n)$, where $\varphi$ denotes Euler’s phi function, and the roots of this polynomial are the primitive complex $n$-th roots of unity. It is well-known that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, with integer coefficients, and $x^n - 1 = \prod_{d|n} \Phi_d(x)$. From the last equation, we have

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n \atop d|n} \Phi_d(x)}. \quad (1)$$

It is a consequence of a well-known result of Dirichlet [1889] that for each integer $n > 0$, there are infinitely many primes of the form $kn + 1$, where $k$ is a positive integer. The problem of determining, or estimating, the smallest prime $p^*(n) \equiv 1 \mod n$ has attracted interest. In [Heath-Brown 1992; Linnik 1944a; 1944b; Xylouris 2009], estimates of the form $p^*(n) \leq c_1 n^{c_2}$, with $c_1, c_2$ constants independent of $n$, are proven using highly nonelementary methods of analytic number theory. Recently, elementary proofs of weaker bounds on $p^*(n)$ have been given. In [Sabia and Tesauri 2009], it is shown that $p^*(n) \leq (3^n - 1)/2$; in [Thangadurai and Vatwani 2011], this is improved to $p^*(n) \leq 2^{\varphi(n)+1} - 1$. Here

**MSC2010:** 11B25, 11N13.

**Keywords:** primes in progressions, arithmetic progressions.

This work was supported by NSF grant no. 1262930, and was completed during the 2013 Research Experience for Undergraduates Program in Algebra and Discrete Mathematics at Auburn University.
we adapt the methods of [Thangadurai and Vatwani 2011] (which were adapted from [Sabia and Tesauri 2009]) to prove the following theorem.

**Theorem.** Let $n \geq 5$ be a prime. The smallest prime $p^*(n) \equiv 1 \pmod{n}$ satisfies the bound

$$p^*(n) \leq \frac{(2^n + 1)}{3}.$$

**Main result**

From (1), we see that if $n$ is a prime, then

$$\Phi_n(X) = \frac{X^n - 1}{X - 1} = X^{n-1} + \cdots + 1,$$

and if $n$ is an odd prime,

$$\Phi_{2n}(X) = \frac{X^{2n} - 1}{\Phi_1(X)\Phi_2(X)\Phi_n(X)} = \frac{X^{2n} - 1}{(X - 1)(X + 1)\Phi_n(X)}$$

$$= \frac{X^{2(n-1)} + X^{2(n-2)} + \cdots + 1}{X^{n-1} + X^{n-2} + \cdots + 1}$$

$$= X^{n-1} - X^{n-2} + \cdots - X + 1$$

$$= \sum_{i=0}^{n-1} (-X)^i.$$  \hspace{1cm} (3)

The main result will follow from (3) and the following lemma.

**Lemma 1** [Sabia and Tesauri 2009]. For any integers $m, b \geq 2$, any prime divisor of $\Phi_m(b)$ is either a divisor of $m$ or is congruent to 1 (mod $m$).

Suppose that $n \geq 5$ is prime. By Lemma 1 and (3),

$$\Phi_{2n}(2) = \sum_{i=0}^{n-1} (-2)^i = \frac{(-2)^n - 1}{-3} = \frac{2^n + 1}{3}$$

has prime divisors of $2n$ or primes congruent to 1 (mod $2n$). The prime divisors of $2n$ are 2 and $n$. Since $2^n + 1$ is odd and $2^n + 1 \equiv 3 \pmod{n}$, neither 2 nor $n$ divides $(2^n + 1)/3$. Therefore,

$$p^*(n) \leq \frac{(2^n + 1)}{3}.$$

**Acknowledgments**

The author thanks Dr. Peter Johnson, Jr. for his advice on this project during the Auburn REU in Algebraic and Discrete Mathematics and Dr. David Zureick-Brown for his guidance and encouragement over the past year.
ON THE LEAST PRIME CONGRUENT TO 1 MODULO $n$

References


Received: 2013-11-28 Revised: 2014-03-09 Accepted: 2014-03-20

jmorro2@emory.edu Emory University, Druid Hills, GA 30306, United States
Enhancing multiple testing: two applications of the probability of correct selection statistic
   **ERIN IRWIN AND JASON WILSON**

On attractors and their basins
   **ALEXANDER ARBIETO AND DAVI OBATA**

Convergence of the maximum zeros of a class of Fibonacci-type polynomials
   **REBECCA GRIDER AND KRISTI KARBER**

Iteration digraphs of a linear function
   **HANNAH ROBERTS**

Numerical integration of rational bubble functions with multiple singularities
   **MICHAEL SCHNEIER**

Finite groups with some weakly $s$-permutably embedded and weakly $s$-supplemented subgroups
   **GUO ZHONG, XUANLONG MA, SHIXUN LIN, JIAYI XIA AND JIANXING JIN**

Ordering graphs in a normalized singular value measure
   **CHARLES R. JOHNSON, BRIAN LINS, VICTOR LUO AND SEAN MEEHAN**

More explicit formulas for Bernoulli and Euler numbers
   **FRANCESCA ROMANO**

Crossings of complex line segments
   **SAMULI LEPPÄNEN**

On the $\varepsilon$-ascent chromatic index of complete graphs
   **JEAN A. BREYTTENBACH AND C. M. (KIEKA) MYNHArdT**

Bisection envelopes
   **NOAH FECHTOR-PRADINES**

Degree 14 2-adic fields
   **CHAD AWTREY, NICOLE MILES, JONATHAN MILSTEAD, CHRISTOPHER SHILL AND ERIN STROSNIDER**

Counting set classes with Burnside’s lemma
   **JOSHUA CASE, LORI KOBAN AND JORDAN LEGRAND**

Border rank of ternary trilinear forms and the $j$-invariant
   **DEREK ALLUMS AND JOSEPH M. LANDSBERG**

On the least prime congruent to 1 modulo $n$
   **JACKSON S. MORROW**