involve
a journal of mathematics

On the least prime congruent to 1 modulo n

Jackson S. Morrow

msp

2015 vol. 8, no. 2

INVOLVE 8:2 (2015)
dx.doi.org/10.2140/involve.2015.8.357

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 $1 \pmod n$. 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

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

This is a monic polynomial of degree $\varphi(n)$, where φ 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

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

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 $p^*(n) \equiv 1 \bmod n$ 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*

$$p^*(n) \leq (2^n + 1)/3.$$

Main result

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

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

and if n is an odd prime,

$$\begin{aligned} \Phi_{2n}(X) &= \frac{X^{2n} - 1}{\Phi_1(X)\Phi_2(X)\Phi_n(X)} = \frac{X^{2n} - 1}{(X-1)(X+1)\Phi_n(X)} \\ &= \frac{X^{2(n-1)} + X^{2(n-2)} + \cdots + 1}{X^{n-1} + X^{n-2} + \cdots + 1} \\ &= X^{n-1} - X^{n-2} + \cdots - X + 1 \\ &= \sum_{i=0}^{n-1} (-X)^i. \end{aligned} \tag{3}$$

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 $1 \pmod m$.*

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

$$p^*(n) \leq (2^n + 1)/3.$$

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.

References

[Dirichlet 1889] G. L. Dirichlet, *Dirichlet Werke*, G. Reimer, Berlin, 1889. JFM 21.0016.01

[Heath-Brown 1992] D. R. Heath-Brown, "Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression", *Proc. London Math. Soc.* (3) **64**:2 (1992), 265–338. MR 93a:11075 Zbl 0739.11033

[Linnik 1944a] U. V. Linnik, "On the least prime in an arithmetic progression, I: The basic theorem", *Rec. Math. [Mat. Sbornik] N.S.* **15(57)** (1944), 139–178. MR 6,260b Zbl 0063.03584

[Linnik 1944b] U. V. Linnik, "On the least prime in an arithmetic progression, II: The Deuring–Heilbronn phenomenon", *Rec. Math. [Mat. Sbornik] N.S.* **15(57)** (1944), 347–368. MR 6,260c Zbl 0063.03585

[Sabia and Tesauri 2009] J. Sabia and S. Tesauri, "The least prime in certain arithmetic progressions", *Amer. Math. Monthly* **116**:7 (2009), 641–643. MR 2549382 Zbl 1229.11012

[Thangadurai and Vatwani 2011] R. Thangadurai and A. Vatwani, "The least prime congruent to one modulo *n*", *Amer. Math. Monthly* **118**:8 (2011), 737–742. MR 2012i:11089 Zbl 1269.11007

[Xylouris 2009] T. Xylouris, *Über die Linniksche Konstante*, Ph.D. dissertation, Diplomarbeit, Universität Bonn, 2009. arXiv 0906.2749

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

jmorro2@emory.edu *Emory University, Druid Hills, GA 30306, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2015 is US $140/year for the electronic version, and $190/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2015 vol. 8 no. 2

1944-4176(2015)8:2;1-5