

involve

a journal of mathematics

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

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

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

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

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 $p^*(n) \equiv 1 \pmod{n}$ 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

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

and if n is an odd prime,

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

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 $2^n + 1 \equiv 3 \pmod{n}$, 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

EDITORS

MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, berenhks@wfu.edu

BOARD OF EDITORS

Colin Adams	Williams College, USA colin.c.adams@williams.edu	David Larson	Texas A&M University, USA larson@math.tamu.edu
John V. Baxley	Wake Forest University, NC, USA baxley@wfu.edu	Suzanne Lenhart	University of Tennessee, USA lenhart@math.utk.edu
Arthur T. Benjamin	Harvey Mudd College, USA benjamin@hmc.edu	Chi-Kwong Li	College of William and Mary, USA ckli@math.wm.edu
Martin Bohner	Missouri U of Science and Technology, USA bohner@mst.edu	Robert B. Lund	Clemson University, USA lund@clemson.edu
Nigel Boston	University of Wisconsin, USA boston@math.wisc.edu	Gaven J. Martin	Massey University, New Zealand g.j.martin@massey.ac.nz
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA budhiraj@email.unc.edu	Mary Meyer	Colorado State University, USA meyer@stat.colostate.edu
Pietro Cerone	La Trobe University, Australia P.Cerone@latrobe.edu.au	Emil Minchev	Ruse, Bulgaria eminchev@hotmail.com
Scott Chapman	Sam Houston State University, USA scott.chapman@shsu.edu	Frank Morgan	Williams College, USA frank.morgan@williams.edu
Joshua N. Cooper	University of South Carolina, USA cooper@math.sc.edu	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran moslehian@ferdowsi.um.ac.ir
Jem N. Corcoran	University of Colorado, USA corcoran@colorado.edu	Zuhair Nashed	University of Central Florida, USA znashed@mail.ucf.edu
Toka Diagana	Howard University, USA tdiagana@howard.edu	Ken Ono	Emory University, USA ono@mathcs.emory.edu
Michael Dorff	Brigham Young University, USA mdorff@math.byu.edu	Timothy E. O'Brien	Loyola University Chicago, USA tbriell@luc.edu
Sever S. Dragomir	Victoria University, Australia sever@matilda.vu.edu.au	Joseph O'Rourke	Smith College, USA orourke@cs.smith.edu
Behrouz Emamizadeh	The Petroleum Institute, UAE bemamizadeh@pi.ac.ae	Yuval Peres	Microsoft Research, USA peres@microsoft.com
Joel Foisy	SUNY Potsdam foisyjs@potsdam.edu	Y.-F. S. Pétermann	Université de Genève, Switzerland petermann@math.unige.ch
Errin W. Fulp	Wake Forest University, USA fulp@wfu.edu	Robert J. Plemmons	Wake Forest University, USA rplemmons@wfu.edu
Joseph Gallian	University of Minnesota Duluth, USA kgallian@d.umn.edu	Carl B. Pomerance	Dartmouth College, USA carl.pomerance@dartmouth.edu
Stephan R. Garcia	Pomona College, USA stephan.garcia@pomona.edu	Vadim Ponomarenko	San Diego State University, USA vadim@sciences.sdsu.edu
Anant Godbole	East Tennessee State University, USA godbole@etsu.edu	Bjorn Poonen	UC Berkeley, USA poonen@math.berkeley.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	James Propp	U Mass Lowell, USA jpropp@cs.uml.edu
Andrew Granville	Université Montréal, Canada andrew.andrew@dms.umontreal.ca	József H. Przytycki	George Washington University, USA przytyck@gwu.edu
Jerrold Griggs	University of South Carolina, USA griggs@math.sc.edu	Richard Rebarber	University of Nebraska, USA rrebarbe@math.unl.edu
Sat Gupta	U of North Carolina, Greensboro, USA sgupta@uncg.edu	Robert W. Robinson	University of Georgia, USA rwr@cs.uga.edu
Jim Haglund	University of Pennsylvania, USA jhaglund@math.upenn.edu	Filip Saidak	U of North Carolina, Greensboro, USA f_saidak@uncg.edu
Johnny Henderson	Baylor University, USA johnny_henderson@baylor.edu	James A. Sellers	Penn State University, USA sellersj@math.psu.edu
Jim Hoste	Pitzer College jhoste@pitzer.edu	Andrew J. Sterge	Honorary Editor andy@ajsterge.com
Natalia Hritonenko	Prairie View A&M University, USA nahritonenko@pvamu.edu	Ann Trenk	Wellesley College, USA atrenk@wellesley.edu
Glenn H. Hurlbert	Arizona State University, USA hurlbert@asu.edu	Ravi Vakil	Stanford University, USA vakill@math.stanford.edu
Charles R. Johnson	College of William and Mary, USA crjohnso@math.wm.edu	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy antonia.vecchio@cnr.it
K. B. Kulasekera	Clemson University, USA kk@ces.clemson.edu	Ram U. Verma	University of Toledo, USA verma99@msn.com
Gerry Ladas	University of Rhode Island, USA gladas@math.uri.edu	John C. Wierman	Johns Hopkins University, USA wierman@jhu.edu
		Michael E. Zieve	University of Michigan, USA zieve@umich.edu

PRODUCTION


Silvio Levy, Scientific Editor

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/>

© 2015 Mathematical Sciences Publishers

involve

2015

vol. 8

no. 2

Enhancing multiple testing: two applications of the probability of correct selection statistic	181
ERIN IRWIN AND JASON WILSON	
On attractors and their basins	195
ALEXANDER ARBIETO AND DAVI OBATA	
Convergence of the maximum zeros of a class of Fibonacci-type polynomials	211
REBECCA GRIDER AND KRISTI KARBER	
Iteration digraphs of a linear function	221
HANNAH ROBERTS	
Numerical integration of rational bubble functions with multiple singularities	233
MICHAEL SCHNEIER	
Finite groups with some weakly s -permutably embedded and weakly s -supplemented subgroups	253
GUO ZHONG, XUANLONG MA, SHIXUN LIN, JIAYI XIA AND JIANXING JIN	
Ordering graphs in a normalized singular value measure	263
CHARLES R. JOHNSON, BRIAN LINS, VICTOR LUO AND SEAN MEEHAN	
More explicit formulas for Bernoulli and Euler numbers	275
FRANCESCA ROMANO	
Crossings of complex line segments	285
SAMULI LEPPÄNEN	
On the ε -ascent chromatic index of complete graphs	295
JEAN A. BREYTENBACH AND C. M. (KIEKA) MYNHARDT	
Bisection envelopes	307
NOAH FECHTOR-PRADINES	
Degree 14 2-adic fields	329
CHAD AWTREY, NICOLE MILES, JONATHAN MILSTEAD, CHRISTOPHER SHILL AND ERIN STROSNIDER	
Counting set classes with Burnside's lemma	337
JOSHUA CASE, LORI KOBAN AND JORDAN LEGRAND	
Border rank of ternary trilinear forms and the j -invariant	345
DEREK ALLUMS AND JOSEPH M. LANDSBERG	
On the least prime congruent to 1 modulo n	357
JACKSON S. MORROW	