# The least prime congruent to one modulo $n$

R. Thangadurai and A. Vatwani

September 10, 2010

**Abstract**

It is known that there are infinitely many primes $\equiv 1\,(mod\,n)$ for any integer $n > 1$. In this paper, we use an elementary argument to prove that the least such prime satisfies $p \leq 2^{\phi(n)+1} - 1$, where $\phi$ is the Euler totient function.

## 1 Introduction

Dirichlet's well known prime number theorem [2] essentially states that, if $a$ and $n$ are relatively prime integers, there exist infinitely many primes in the arithmetic progression $a, a+n, a+2n, \cdots$. The proof of this theorem is not very elementary [16, 17]. However, many simpler proofs are known for the particular case $a = 1$ [3, 4, 5, 10, 12, 13, 14, 15, 19].

Linnik [8, 9] proved that, if $(a, n) = 1$, there are absolute constants $c_1$ and $c_2$, such that the least prime $\equiv a \pmod{n}$ satisfies $p \leq c_1 n^{c_2}$. His proof employs analytic methods. In 1992, it was proved by Heath-Brown [6] that the value of the constant $c_2$ could be taken as 5.5. Recently this value was improved to 5.2 by T.Xylouris [20]. The value can further be improved to $c_2 = 2 + \epsilon$, provided the Generalized Riemann Hypothesis is assumed. In a private communication, we learn that J. Oesterle proved, by assuming Generalized Riemann Hypothesis, that $p \leq 70n(\log(n))^2$, for all $n > 1$. These results are not elementary and involve a detailed study of zeroes of Dirichlet $L$-functions. Consequently, simpler proofs of bounds in special cases are sought after. Recently, Sabia and Tesauri [13] gave an elementary argument using divisibility properties of the $n$th cyclotomic polynomial to prove the bound $(3^n - 1)/2$ for the least prime $p \equiv 1 \pmod{n}$, $n \geq 2$. The bound $2^n + 1$ for the same was given by S.S Pillai [11], in 1944, using divisibility properties of the numbers $2^n + 1$, but this result did not receive much attention since it was mentioned as a lemma.

In this paper, we build upon the idea employed in [13] to prove the following result.

**Theorem 1.** *For a given integer $n \geq 2$, the least prime $p \equiv 1 \pmod{n}$ satisfies*

$$p \leq 2^{\phi(n)+1} - 1,$$

*where $\phi(n)$ is the Euler totient function.*

## 2 Preliminaries

For any integer $n \geq 1$, the $n$-th cyclotomic polynomial can be defined as:

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

This is a polynomial of degree $\phi(n)$ whose roots are the primitive $n$-th roots of unity. It is known that $\Phi_n(x)$ is a monic irreducible polynomial over $\mathbb{Q}$ with integer coefficients and that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

A suitable form for $\Phi_n(x)$ can be obtained using the Möbius function, $\mu(n)$, which is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^k & \text{if } n > 1 \text{ and } n = p_1 p_2 \cdots p_k \text{ for distinct primes } p_i; \\ 0 & \text{otherwise.} \end{cases}$$

It can be seen that $\mu$ is a multiplicative function, that is, $\mu(mn) = \mu(m)\mu(n)$ whenever $(m,n) = 1$. Some of the properties of the Möbius function are stated in the following Lemma.

**Lemma 2.** ([1, 18]) *Let $n \geq 1$ be a given integer. Then we have,*
*a)* $\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{if } n = 1, \\ 0 & \textit{otherwise.} \end{cases}$
*b)If $f$ and $g$ are two arithmetical functions such that, $f(n) = \sum_{d|n} g(d)$, then*

$$g(n) = \sum_{d|n} f(d)\mu(n/d)$$

*In particular, $n = \sum_{d|n} \phi(d)$ implies that $\phi(n) = \sum_{d|n} \mu(d)n/d$.*
*c)If $f(n) = \prod_{d|n} g(d)$, then*

$$g(n) = \prod_{d|n} f(d)^{\mu(n/d)}$$

*In particular, $x^n - 1 = \prod_{d|n} \Phi_d(x)$ implies that $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$.*

We state two more lemmas which will be useful. Their proofs can be found in the references cited.

**Lemma 3.** ([13]) *For any integer $b \geq 2$, the prime factors of $\Phi_n(b)$ are either prime divisors of $n$ or are $\equiv 1 \pmod{n}$. Moreover, if $n > 2$, any prime divisor of $n$ can divide $\Phi_n(b)$ only to the exponent 1, that is, $p^2$ does not divide $\Phi_n(b)$.*

This lemma was used by Sabia and Tesauri [13] to prove that the least prime $p \equiv 1 \pmod{n}$ satisfies $p \leq (3^n - 1)/2$.

**Lemma 4.** ([7]) *For every integer $n > 2$, $n \neq 6$, we have,*

$$\phi(n) \geq \sqrt{n}.$$

Also, we will use the following identity. For $x \in [0, 1)$, we have

$$-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \le x + x^2 + x^3 + \cdots = \frac{x}{1-x} \tag{1}$$

**Theorem 5.** *For any integers $n \ge 2$ and $b \ge 2$, we have,*

$$\frac{1}{2} \cdot b^{\phi(n)} \le \Phi_n(b) \le 2 \cdot b^{\phi(n)}$$

*Proof.* From Lemma 2, we know

$$\begin{aligned}
\Phi_n(b) &= \prod_{d|n} (b^d - 1)^{\mu(n/d)} \\
&= b^{\sum_{d|n} d \cdot \mu(n/d)} \prod_{d|n} \left(1 - \frac{1}{b^d}\right)^{\mu(n/d)} \\
&= b^{\phi(n)} \prod_{d|n} \left(1 - \frac{1}{b^d}\right)^{\mu(n/d)}
\end{aligned}$$

We define

$$S = \frac{\Phi_n(b)}{b^{\phi(n)}} = \prod_{d|n} \left(1 - \frac{1}{b^d}\right)^{\mu(n/d)}$$

Then,

$$\log S = \sum_{d|n} \mu(n/d) \log(1 - b^{-d}) \tag{2}$$

It is enough to show that $\frac{1}{2} \le S \le 2$, that is,

$$-\log 2 \le \log S \le \log 2$$

We shall first prove the upper bound:

**Case 1.** $\mu(n) \ge 0$

By the equation (2),

$$\begin{aligned}
\log S &= \mu(n) \log(1 - b^{-1}) + \sum_{d|n, d \ge 2} \mu(n/d) \log(1 - b^{-d}) \\
&\le -\mu(n) \log\left(\frac{b}{b-1}\right) + \sum_{d \ge 2} -\log(1 - b^{-d}) \\
&\le \sum_{d \ge 2} \left[b^{-d} + \frac{b^{-2d}}{2} + \frac{b^{-3d}}{3} + \cdots\right], \quad \text{(by (1))}
\end{aligned}$$

$$
\begin{aligned}
&\leq \sum_{d\geq 2}\left[b^{-d}+\frac{b^{-2d}}{2}(1+b^{-d}+b^{-2d}+\cdots)\right]\\
&=\sum_{d\geq 2}\left[b^{-d}+\frac{b^{-2d}}{2}(1-b^{-d})^{-1}\right]=\sum_{d\geq 2}\left(\frac{1}{b^d}+\frac{1}{2b^{2d}}\frac{b^d}{b^d-1}\right)\\
&\leq \sum_{d\geq 2}\left(\frac{1}{b^d}+\frac{1}{6b^d}\right)=\frac{7}{6}\cdot\frac{1}{b(b-1)}\\
&\leq \frac{7}{12}<\log 2.
\end{aligned}
$$

**Case 2.** $\mu(n)<0$

In this case, $n=p_1p_2\cdots p_k$, $k$ being odd. Hence for any prime $p\mid n$, we have $\mu(n/p)=1$. Let $q$ be the least prime divisor of $n$. Any divisor of $d$ of $n$ which is $\neq 1$ and not a prime is $\geq q^2$. Now,

$$
\begin{aligned}
\log S =&\mu(n)\log(1-b^{-1})+\sum_{p\mid n}\mu(n/p)\log(1-b^{-p})+\sum_{d\mid n;d\neq 1,p}\mu(n/d)\log(1-b^{-d})\\
=&-\log((b-1)/b)+\sum_{p\mid n}\log(1-b^{-p})+\sum_{d\mid n;d\neq 1,p}\mu(n/d)\log(1-b^{-d})\\
\leq&-\log((b-1)/b)+\log(1-b^{-q})+\sum_{d\geq q^2}-\log(1-b^{-d})\\
\leq&\log(b/b-1)+\log(1-b^{-q})+\sum_{d\geq q^2}\frac{b^{-d}}{1-b^{-d}},\qquad\text{(by (1))}\\
\leq&\log(b/b-1)+\log(1-b^{-q})+\sum_{d\geq q^2}\frac{1}{b^{d-1}}\\
=&\log(b/b-1)+\log(1-b^{-q})+\frac{1}{b^{q^2-2}(b-1)}\\
\leq&\log 2-\frac{1}{b^q}+\frac{1}{b^{q^2-2}}\\
\leq&\log 2\ \text{, since } q^2-2\geq q.
\end{aligned}
$$

Thus, the upper bound follows.

Now, for the lower bound, we see that case $\mu(n)\leq 0$ is analogous to the upper bound for the case $\mu(n)\geq 0$. Similarly, the case $\mu(n)>0$ is analogous to the upper bound for the case $\mu(n)<0$. Hence, we omit the proof for the lower bound here. This completes the proof. □

# 3 Proof of Theorem 1.

*Proof.* For a positive integer $n$, let $s(n)$ denote the square free part of $n$. Having proved Theorem 5, we observe that, for any integers $b>1$ and $n>2$; if the inequality

$$\frac{1}{2} \cdot b^{\phi(n)} > s(n) \tag{3}$$

holds, then $\Phi_n(b) > s(n)$. Using Lemma 3, we can conclude that there exists atleast one prime $p \mid \Phi_n(b)$ such that $p$ does not divide $n$, and hence this prime must be $\equiv 1 \pmod{n}$. Then, $p \mid \Phi_n(b)$ implies that $p \leq \Phi_n(b)$. Using Theorem 5 once again, we obtain,

$$p \leq 2 \cdot b^{\phi(n)} - 1.$$

This gives us an upper bound for $p$.

Theorem 1 gives the closest possible upper bound using this method. In order to prove it, we must put $b = 2$ in the above discussion and examine the corresponding inequality obtained by putting $b = 2$ in (1):

$$2^{\phi(n)-1} > s(n). \tag{4}$$

If this inequality holds for all integers $n \geq 2$, then we are done.

From Lemma 4, we know that $\phi(n) \geq \sqrt{n}$, for all integers $n > 2$ except $n = 6$. Hence,

$$2^{\phi(n)-1} \geq 2^{\sqrt{n}-1}$$

for all $n > 2, n \neq 6$. It is enough to prove that $2^{\sqrt{n}-1} > s(n)$, that is,

$$\sqrt{n} - 1 > \frac{\log s(n)}{\log 2}. \tag{5}$$

Since we know that $n \geq s(n)$, consider the following real valued function:

$$f(x) = \sqrt{x} - 1 - (\log x / \log 2).$$

It can be checked that this is an increasing function for $x > (2/\log 2)^2 \approx 8.325$. The first integer value of $x$ for which this function is positive is 40. This means that the function takes positive values for all integers $n \geq 40$. Thus,

$$2^{\phi(n)-1} \geq 2^{\sqrt{n}-1} > n \geq s(n), \text{ for all integers } n \geq 40.$$

This proves Theorem 1 for integers $n \geq 40$. When $n = p$, a prime, $\Phi_p(2) = 2^p - 1 > p$ for all primes $p \geq 2$.

Now, we shall prove that Theorem 1 is true for all composite numbers $n \leq 39$. It is enough to show that

$$\Phi_n(2) > n \tag{6}$$

holds for integers $n$, with $2 \leq n \leq 39$. This can be checked by computing the values of $\Phi_n(2)$ for these integers. We list the results as follows:

| $n$ | $\Phi_n(2)$ | $n$ | $\Phi_n(2)$ | $n$ | $\Phi_n(2)$ | $n$ | $\Phi_n(2)$ |
|---|---|---|---|---|---|---|---|
| 4 | 5 | 15 | 151 | 24 | 241 | 33 | 599479 |
| 6 | 3 | 16 | 257 | 25 | 1082401 | 34 | 43691 |
| 8 | 17 | 18 | 57 | 26 | 2731 | 35 | 8727391 |
| 9 | 73 | 20 | 205 | 27 | 262657 | 36 | 4033 |
| 10 | 11 | 21 | 2359 | 28 | 3277 | 38 | 174763 |
| 12 | 13 | 22 | 683 | 30 | 331 | 39 | 9588151 |
| 14 | 43 | | | 32 | 65537 | | |

It can be seen that (6) holds for all $n$ such that $2 \leq n \leq 39$, except for $n = 6$. For $n = 6$, Theorem 1 easily follows with $p = 7$.

This proves Theorem 1. □

**Acknowledgement.** We are thankful to Prof. J. Oesterle for having a fruitful discussion on this problem.

# References

[1] T. M. Apostol, *Introduction to Analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

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

[3] T. Estermann, Note on a paper of A. Rotkiewicz, *Acta Arith.* **8** (1963) 465–467.

[4] H. Gauchman, A special case of Dirichlet's theorem on primes in an arithmetic progression, *Math. Mag.* **74** (2001) 397–399.

[5] H. Hasse, *Vorlesungen über zahlentheorie. 2*, Auflage, Springer-Verlag, Berlin, 1964.

[6] D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, *Proc. London Math. Soc.* **64** (1992) 265–338.

[7] D. G. Kendall and R. Osborn, Two Simple Lower Bounds for Euler's Function, *Texas J. Sci.* **17** (1965).

[8] Y. V. Linnik, On the least prime in an arithmetic progression - I. The basic theorem, *Rec. Math. (Mat. Sbornik)* N. S. **15** (1944) 139–178.

[9] ——, On the least prime in an arithmetic progression - II. The Deuring-Heilbronn phenomenon, *Rec. Math. (Mat. Sbornik)* N. S. **15** (1944) 347–368.

[10] I. Niven and B. Powell, Primes in certain arithmetic progressions, this MONTHLY **83** (1976) 467–469.

[11] S. S. Pillai, On the smallest primitive root of a prime, *J. Indian Math. Soc.* N. S. **8** (1944) 14–17.

[12] A. Rotkiewicz, Démonstration arithmétique de lexistence dune infinité de nombres premiers de la forme nk+1, *L Enseign. Math.* **7** (1961) 277–280.

[13] J. Sabia and S. Tesauri, The least prime in certain arithmetic progressions, this MONTHLY **116** (2009) 641–643.

[14] I. Schur, über die existenz unendlich vieler primzahlen in einigen speziellen arithmetischen progression, *Sitzber. der Berliner Math. Ges.* **11** (1912) 40–50, Reproduced in *Gesammelte Abhandlungen II*, eds., A. Brauer and H. Rohrbach, Springer-Verlag, Berlin, 1973, 1-11.

[15] N. Sedrakian and J. Steinig, A particular case of Dirichlets theorem on arithmetic progression, *LEnseign. Math.* **44** (1998) 3–7.

[16] A. Selberg, An elementary proof of Dirichlet's theorem about primes in an arithmetic progression, *Ann. of Math.* **50** (1949) 297–304.

[17] J. P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, vol.7, Springer-Verlag, New York, 1977.

[18] R. Thangadurai, On the coefficients of cyclotomic polynomials, in *Cyclotomic fields and related topics (Pune, 1999)*, Bhaskaracharya Pratishthana, Pune, 2000, 311–322.

[19] J. Wendt, Elementarer beweis des satzes, dass in jeder unbegrenzten arithmetischen progression my + 1 unendlich viele primzahlen vorkommenm, *J. Reine und Angew andte Math.* **115** (1895) 85–88.

[20] T. Xylouris, Über die Linniksche Konstante, Ph.D. thesis, Diplomarbeit, Universität Bonn, 2009, available at `http://arxiv.org/pdf/0906.2749`.

*R. Thangadurai, School of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019, INDIA*
*thanga@hri.res.in*

*A. Vatwani, IIIrd year Int.M.Sc, IISER, Central tower, Sai Trinity building, Pashan circle, Pune 411021, INDIA*
*a.vatwani@iiserpune.ac.in*