Author preprint of:
Jim Barthel & Volker Müller (2022) A Conjecture on Primes in Arithmetic Progressions and Geometric Intervals, The American Mathematical Monthly, 129:10, 979-983, https://doi.org/10.1080/00029890.2022.2116250

A Conjecture on Primes in Arithmetic Progressions and Geometric Intervals

Jim Barthel and Volker Müller

Abstract. *Dirichlet's theorem on primes in arithmetic progressions* states that for any positive integer q and any coprime integer a, there are infinitely many primes in the arithmetic progression $a + nq$ ($n \in \mathbb{N}$). Unfortunately, the theorem does not predict the gap between those primes. Several renowned open questions such as the size of *Linnik's constant* try to say more about the distribution of such primes. This manuscript postulates a weak, but explicit, generalization of *Linnik*'s theorem, namely that each geometric interval $[q^t, q^{t+1}]$ contains a prime from each coprime congruence class modulo $q \in \mathbb{N}_{\geq 2}$. Subsequently, it proves the conjecture theoretically for all sufficiently large t, as well as computationally for all sufficiently small q. Finally, the impact of this conjecture on a result of *Pomerance* related to *Carmichael's conjecture* is outlined.

1. AN EXPLICIT GENERALIZATION OF LINNIK'S THEOREM.

Dirichlet's theorem on primes in arithmetic progressions [7] is the direct generalization of *Euclid*'s theorem on the infinity of primes to the setting of arithmetic progressions. Sadly, both of those theorems are purely existential and do not hint at the exact distribution of primes; a fact that has already puzzled mathematicians for several centuries. A first milestone was achieved in 1896 when the *Prime Number Theorem* describing the asymptotic distribution of primes was independently proven by *Hadamard* and *De la Vallée Poussin*. Shortly after, *De la Vallée Poussin* generalized his findings to primes in arithmetic progressions, indicating that the primes are evenly distributed among the coprime congruence classes. Over the last century, many mathematicians improved the asymptotic limits for the distribution of primes and outlined explicit computational bounds. Whereas the picture slowly clarifies for primes in general, there are not many explicit results for primes in arithmetic progressions. In fact, their study turns out to be extremely challenging if short intervals are involved. One example of this is the strenuous quest for predicting the size of the smallest prime in an arithmetic progression. An amazing result in this direction was achieved by *Linnik* in 1944 with the following theorem ([10], [11]).

Theorem 1 (Linnik). *There are absolute constants C and L such that for any $q \in \mathbb{N}_{\geq 2}$ and any $1 \leq a \leq q-1$ with $\gcd(a,q) = 1$, the smallest prime $p_0 \equiv a \pmod{q}$ does not exceed Cq^L.*

Although *Linnik* did not write out his predicted constants C and L, his development showed them to be effectively computable. Today, the infimum over all possible absolute constants L for which Theorem 1 holds is known as *Linnik's constant*. After several years of research, the best unconditional upper bound for *Linnik's constant* is $L \leq 5$ [**14**] and under GRH one may conclude that any constant $L > 2$ is admissible [**6**]. Nonetheless, aligned with *Schinzel's conjecture* H_2 [**13**], the detailed survey [**9**] conjectures the upper bound $L \leq 2$ and [**3**] shows that this actually holds for almost all moduli. After discussing the smallest prime in an arithmetic progression, one may go on and ask about the subsequent primes. Setting $C = 1$ and varying only the exponent in Theorem 1 leads to the following conjecture.

Conjecture 2. *For any positive integers $q \geq 2$, $1 \leq a \leq q-1$ with $\gcd(q, a) = 1$, and $t \geq 1$, there exists a prime p such that*

$$q^t \leq p < q^{t+1} \qquad \textit{and} \qquad p \equiv a \pmod q. \tag{1}$$

Of course, if primes smaller than q are allowed and $t = 1$, one recovers the conjecture on the size of *Linnik's constant*. Consequently, it is not surprising that Conjecture 2 is extremely difficult to prove for small exponents. However, the picture changes when t increases. Indeed, the expansion of these geometric intervals is faster than the decrease of the occurrence of primes. Thus, for sufficiently large t, the interval $[q^t, q^{t+1}]$ will contain many primes of the desired form. One could even shrink the considered intervals and still conclude that they contain one prime from each congruence class. Whereas this is the main focus of most recent asymptotic results, Conjecture 2 is meant to be fully explicit without any hidden constants. Although it does not reflect the optimal interval length for the existential conclusion, it gives a practical range for retrieving such primes. Furthermore, it is deeply connected with other classical results such as *Bertrand's postulate*, which can be obtained by considering $q = 2$.

Remark 3. For the sake of clarity, the upcoming development relies on explicit results only.

2. A PARTIAL PROOF FOR CONJECTURE 2.

Recent explicit results on the distribution of primes in arithmetic progressions allow a partial proof of Conjecture 2. Indeed, the article [**2**], accompanied by an enormous computational data set, gives explicit bounds for the number of primes in bounded arithmetic progressions.

Theorem 4 (Bennett, Martin, O'Bryant, Rechnitzer). *Let $q \geq 3$ be an integer, let a be an integer that is coprime to q, and let ϕ denote the Euler totient function. Furthermore, let θ denote the first Chebyshev prime counting function for arithmetic progressions defined by*

$$\theta(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \log(p)$$

where the sum runs over all primes $p \leq x$ congruent to a modulo q. Then there exist explicit constants $c_\theta(q)$ and $x_\theta(q)$ such that

$$\left| \theta(x; q, a) - \frac{x}{\phi(q)} \right| < c_\theta(q) \frac{x}{\log(x)} \qquad \forall x \geq x_\theta(q).$$

Moreover, $c_\theta(q)$ and $x_\theta(q)$ satisfy $c_\theta(q) \leq c_0(q)$ and $x_\theta(q) \leq x_0(q)$, where

$$c_0(q) = \begin{cases} \frac{1}{840} & \textit{if} \quad 3 \leq q \leq 10^4 \\ \frac{1}{160} & \textit{if} \quad q > 10^4 \end{cases} \quad \textit{and} \quad x_0(q) = \begin{cases} 8 \cdot 10^9, & \textit{if} \quad 3 \leq q \leq 10^5 \\ \exp\left(\frac{3}{100}\sqrt{q}(\log(q))^3\right), & \textit{if} \quad q > 10^5 \end{cases}.$$

Theorem 4 gives rise to an explicit lower bound for the exponents for which Conjecture 2 will hold, that is

$$T_\theta(q) := \max\left\{ \frac{c_\theta(q)\phi(q)(q+2)}{(q-1)\log(q)} - 1;\ \log_q(x_\theta(q));\ 1 \right\}. \tag{2}$$

Lemma 5. *Let $q \geq 3$, $1 \leq a \leq q-1$ with $\gcd(a,q) = 1$ and $t \geq T_\theta(q)$. Then there exists a prime p such that $q^t \leq p < q^{t+1}$ and $p \equiv a \pmod q$.*

Proof. By assumption $t \geq T_\theta(q) \geq \log_q(x_\theta(q))$, and so $q^{t+1} > q^t \geq q^{\log_q(x_\theta(q))} = x_\theta(q)$. Thus, Theorem 4 yields a lower bound for $\theta(q^{t+1};q,a)$ and an upper bound for $\theta(q^t;q,a)$. Combining these bounds leads to the following inequalities:

$$\begin{aligned}\theta(q^{t+1};q,a) - \theta(q^t;q,a) &> \frac{q^{t+1}}{\phi(q)} - c_\theta(q)\frac{q^{t+1}}{(t+1)\log(q)} - \frac{q^t}{\phi(q)} - c_\theta(q)\frac{q^t}{t\log(q)}, \\ &\geq q^t\left[\frac{q-1}{\phi(q)} - \frac{c_\theta(q)}{\log(q)}\frac{qt+t+1}{t(t+1)}\right], \\ &\geq q^t\left[\frac{q-1}{\phi(q)} - \frac{c_\theta(q)}{\log(q)}\frac{q+2}{t+1}\right].\end{aligned}$$

As $t \geq T_\theta(q) \geq \frac{c_\theta(q)\phi(q)(q+2)}{(q-1)\log(q)} - 1$, the last quantity is non-negative, which guarantees the existence of a prime $p \in [q^t, q^{t+1}]$ such that $p \equiv a \pmod q$. ■

Although, $T_\theta(q)$ varies with q, Lemma 5 implies that for a fixed $q \geq 3$ Conjecture 2 holds except maybe for finitely many exponents, namely for $0 < t < T_\theta(q)$. Using the explicit lists of constants $c_\theta(q)$ and $x_\theta(q)$ from [2] published at

http://www.nt.math.ubc.ca/BeMaObRe/,

one can computationally verify the conjecture for those finitely many missing exponents. A verification for all $3 \leq q \leq 45000$ can be found at

https://files.uni.lu/jim.barthel/PrimesInAP/

and leads to the following conclusion.

Lemma 6. *Let $3 \leq q \leq 45000$, $1 \leq a \leq q-1$ with $\gcd(q,a) = 1$, and $1 \leq t \leq T_\theta(q)$. Then, there exists a prime p such that $q^t \leq p < q^{t+1}$ and $p \equiv a \pmod q$.*

Using SageMath and its built-in Pari-GP function *isprime()*, the verification program computed for each modulus $3 \leq q \leq 45000$ and each coprime remainder $1 \leq a \leq q-1$ an explicit list $L(q,a)$ of primes $p_1, ..., p_{\lceil T_\theta(q)\rceil - 1}$ verifying

$$q < p_1 < q^2 < p_2 < ... < q^{\lceil T_\theta(q)\rceil - 1} < p_{\lceil T_\theta(q)\rceil - 1} < q^{\lceil T_\theta(q)\rceil}$$

and $p_i \equiv a \pmod q$ for all $i \in \{1, ..., \lceil T_\theta(q)\rceil - 1\}$. These lists of primes are freely accessible and can also be used for other statistical analyses of primes in arithmetic progressions. Simultaneously, this verification guarantees correctness of the conjectured size of *Linnik's constant* for all $q \leq 45000$.

Remark 7. Let li denote the logarithmic integral defined by $li(x) = \int_0^x \frac{dt}{\log(t)}$. Let π denote the usual prime counting function for arithmetic progressions defined by

$$\pi(x;q,a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} 1$$

where the sum runs over all primes $p \le x$ congruent to a modulo q. Assuming the Extended Riemann Hypothesis, [1, Thm. 8.8.18] shows that

$$\left|\pi(x;q,a) - \frac{li(x)}{\phi(q)}\right| < \sqrt{x}(\log(x) + 2\log(q)) \qquad \forall x \ge 2.$$

Using those conditional bounds, one can show that Conjecture 2 holds for all $t \ge 3$ when $q \ge 2$, and even for $t = 2$ when q is sufficiently large (i.e. $q \ge 17386763$). Thus, under the Extended Riemann Hypothesis, only the conjectured bound $L \le 2$ for *Linnik's constant* remains to be proven.

3. A CONSEQUENCE FOR CARMICHAEL'S CONJECTURE.

Conjecture 2 is indirectly linked to *Carmichael's totient function conjecture* ([4],[5]). Before explaining this link, a short summary of this conjecture is required.

Conjecture 8 (Carmichael). *Let ϕ denote the Euler totient function. For a given number n, the equation $\phi(x) = n$ either has no solution at all or it has at least two solutions.*

Correctness of the conjecture has already been proven for all $x \le 10^{10^{10}}$ [8], but the existence of a counterexample has not yet been ruled out for larger values. The only known attempt for constructing a counterexample has been developed by *Pomerance* in [12]. His construction relies on the following observation.

Theorem 9 (Pomerance). *If x is a natural number such that for every prime p, $(p-1)|\phi(x)$ implies $p^2|x$, then $\phi(x) = \phi(y)$ has only the trivial solution $y = x$.*

However, *Pomerance* also points out that likely such a counterexample does not exist. In particular, he shows that if the following conjecture holds, then there cannot be a counterexample as it would necessarily be divisible by every single prime.

Conjecture 10 (Pomerance). *If $k \ge 2$, then $(p_k - 1)|\prod_{i=1}^{k-1} p_i(p_i - 1)$, where p_i denotes the i-th prime.*

Translating *Pomerance's conjecture* in terms of primes in arithmetic progressions with remainder 1 and comparing it with Conjecture 2 finally reveals the acclaimed link.

Proposition 11. *If Conjecture 2 holds, then Pomerance's conjecture holds, and hence there does not exist a counterexample to Carmichael's conjecture based on Theorem 9.*

Proof. Assume Conjecture 2 holds, and let $k \in \mathbb{N}_{\ge 2}$. In order to prove that $(p_k - 1)|\prod_{i=1}^{k-1} p_i(p_i - 1)$, it is sufficient to show that $v_q(p_k - 1) \le v_q(\prod_{i=1}^{k-1} p_i(p_i - 1))$ for all $q \in \{p_1, p_2, ..., p_{k-1}\}$ where $v_q : \mathbb{N} \to \mathbb{N}$ denotes the q-adic valuation map defined by $v_q(0) = \infty$ and $v_q(n) = \max\{v \in \mathbb{N} : q^v|n\}$. Indeed, any prime divisor of $(p_k - 1)$ is smaller than p_k and the valuation map outlines its highest power, granting an easy comparison of divisors. Accordingly, let $q \in \{p_1, p_2, ..., p_{k-1}\}$, then $q^t \le p_k - 1 < q^{t+1}$ for some $t \in \mathbb{N}$. Thus $v_q(p_k - 1) \le t$. If $t = 0$, then the claim is trivial. If $t > 0$, Conjecture 2 yields

$$v_q\left(\prod_{i=1}^{k-1} p_i(p_i - 1)\right) = 1 + v_q\left(\prod_{i=1}^{k-1}(p_i - 1)\right) \ge 1 + (t-1) = t$$

where the last inequality follows from Conjecture 2's claim that for all $t' \in \{1, ..., t-1\}$ there is a prime p such that $q^{t'} \leq p < q^{t'+1}$ and $p \equiv 1 \pmod q$. ■

As Conjecture 2 holds for all $q \leq 45000$, Pomerance's conjecture holds for a non-negligible proportion of all primes.

Corollary 12. *Pomerance's conjecture holds for any prime p_k such that the largest square factor of $p_k - 1$ is* 45000*-smooth.*

Proof. Pomerance's conjecture trivially holds whenever $p_k - 1$ is squarefree. Thus assume that $p_k - 1 = B^2\chi$ where B is 45000-smooth and χ is squarefree. Regrouping the prime factors gives $p_k - 1 = B'\chi'$ where B' is 45000-smooth and χ' is either equal to 1 or squarefree with smallest prime factor larger than 45000. In both cases, $\prod_{i=1}^{k-1} p_i(p_i - 1)$ is trivially divisible by χ'. Furthermore, the same valuation argument as used in the proof of Proposition 11 shows that also $B' | \prod_{i=1}^{k-1} p_i(p_i - 1)$, which concludes the proof. ■

Remark 13. Proposition 11 does not contradict the general existence of a counterexample of *Carmichael's conjecture*, but it only rules out counterexamples stemming from Theorem 9. Corollary 12 thus strengthens the correctness of *Carmichael's conjecture* but is not sufficient to prove it.

ACKNOWLEDGMENT. The authors wish to thank the editors and the anonymous referees for their helpful suggestions. The first author was supported in part by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

REFERENCES

1. Bach, E., Shallit, J. (1996). *Algorithmic number theory*, Vol. 1: Efficient Algorithms. Cambridge, MA: MIT Press.
2. Bennett, A. M., Martin, G., O'Bryant, K., Rechnitzer, A. (2018). Explicit bounds for primes in arithmetic progressions. *Illinois J. Math.* **62**(1-4): 427-532. doi.org/10.1215/ijm/1552442669
3. Bombieri, E., Friedlander, J. B., Iwaniec, H. (1989). Primes in arithmetic progressions to large moduli. III. *J. Amer. Math. Soc.* **2**(2): 215-224. doi.org/10.1090/S0894-0347-1989-0976723-6
4. Carmichael, R. D. (1907). On Euler's ϕ-function. *Bull. Amer. Math. Soc.* **13**(5): 241-243. doi.org/10.1090/S0002-9904-1907-01453-2
5. Carmichael, R. D. (1922). Note on Euler's φ-function. *Bull. Amer. Math. Soc.* **28**(3): 109-110. doi.org/10.1090/S0002-9904-1922-03504-5
6. Chowla, S. (1934). On the least prime in an arithmetical progression. *Acta Arith.* **1**(2): 1-3.
7. Dirichlet, P. G. L. (1837). Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abh. K. Preuss. Akad. Wiss.* 45-81.
8. Ford, K. (1998). The distribution of totients. *Ramanujan J.* **2**(1-2): 67-151. doi.org/10.1023/A:1009761909132
9. Heath-Brown, D. R. (1992). Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc.* **64**(2): 265-338. doi.org/10.1112/plms/s3-64.2.265
10. Linnik, U. V. (1944). On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.* **15**(57): 139-178. mi.mathnet.ru/eng/msb6196
11. Linnik, U. V. (1944). On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. *Rec. Math. [Mat. Sbornik] N.S.* **15**(57): 347-368. mi.mathnet.ru/eng/msb6202

12. Pomerance, C. (1974). On Carmichael's conjecture. *Proc. Amer. Math. Soc.* **43**(2): 297-298. doi.org/10.1090/S0002-9939-1974-0340161-0
13. Schinzel, A., Sierpiński, W. (1958). Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.* **4**(3): 185-208. eudml.org/doc/206115
14. Xylouris, T. (2018). Linniks Konstante ist kleiner als 5.*Chebyshevskii Sb.* **19**(3): 80-94. doi.org/10.22405/2226-8383-2018-19-3-80-94

Faculty of Science, Technology and Medicine, University of Luxembourg, Belval 4365, Luxembourg, jim.barthel@uni.lu and volker.muller@uni.lu