On a conjecture of Pomerance

by

L. HAJDU (Debrecen), N. SARADHA (Mumbai) and R. TIJDEMAN (Leiden)

Dedicated to Professor Schinzel on the occasion of his 75th birthday

1. Introduction. Let k > 1 be an integer. We denote Euler's totient function by $\varphi(k)$ and the number of distinct prime divisors of k by $\omega(k)$. We say that k is a *P*-integer if the first $\varphi(k)$ primes coprime to k form a reduced residue system modulo k. In 1980, Pomerance [8] proved the finiteness of the set of *P*-integers. The following conjecture was proposed by him in [8].

CONJECTURE OF POMERANCE. If k is a P-integer, then $k \leq 30$.

This conjecture is still open. Recently, Hajdu and Saradha [3] and Saradha [12] have given simple conditions under which an integer k is not a P-integer. From their results, it follows that

- no prime is a P-integer except 2;
- no square or a cube of a prime is a P-integer except 4;
- no integer k with its least odd prime divisor > $\log k$ is a P-integer except when $k \in \{2, 4, 6, 12, 18, 30\}$.

It is easy to check that the only *P*-integers ≤ 30 are 2, 4, 6, 12, 18, 30. It was checked in [3] by computation that if k is another *P*-integer, then $k \geq 5.5 \cdot 10^5$. In Theorem 4.1 we improve this bound to 10^{11} .

In this paper, we also give a quantitative version of the finiteness result of Pomerance and prove the conjecture of Pomerance under the Riemann Hypothesis. We have

THEOREM 1.1. If k is a P-integer, then $k < 10^{3500}$.

THEOREM 1.2. Suppose the Riemann Hypothesis holds. Then the only *P*-integers are 2, 4, 6, 12, 18, 30.

Key words and phrases: primes in residue classes, Riemann Hypothesis.

²⁰¹⁰ Mathematics Subject Classification: Primary 11N13.

L. Hajdu et al.

Pomerance's conjecture is closely related to the classical problem about the least primes in arithmetic progressions. Let l be a positive integer with gcd(k, l) = 1. Denote by p(k, l) the least prime $p \equiv l \pmod{k}$. Let P(k) be the maximum value of p(k, l) for all l. Linnik [7] has shown that

$$P(k) \ll k^L$$

for some constant L which is known as Linnik's constant. A huge literature is available on finding good values for L (see [4, 15]). In the other direction, Prachar [9] and Schinzel [13] have shown that there is an absolute constant c such that for each l there are infinitely many k with

$$p'(k,l) > \frac{ck \log k \cdot \log \log \log \log \log \log k}{(\log \log \log k)^2}$$

where p'(k, l) is the first prime q > k with $q \equiv l \pmod{k}$. In his proof of the finiteness of *P*-integers Pomerance [8] used the Jacobsthal function to show that

$$P(k) \ge (e^{\gamma} + o(1))\varphi(k)\log k$$

where γ is Euler's constant.

In our proofs we apply different tools. We use the fact that the primitive residues modulo k between 0 and k are symmetric around k/2. Our arguments are based on results about the zeros of the Riemann zeta function and estimates for the number of primes in intervals.

2. Lemmas. Throughout the paper, let $p_1 < p_2 < \cdots$ be the increasing sequence of prime numbers. For any x > 1, let $\pi(x)$ denote the number of prime numbers not exceeding x, and

$$\operatorname{Li}(x) = \lim_{\epsilon \to 0^+} \int_{t=0}^{1-\epsilon} \frac{dt}{\log t} + \int_{t=1+\epsilon}^{x} \frac{dt}{\log t}.$$

We put $\pi(x) = 0$ for $0 \le x \le 1$.

LEMMA 2.1. For any $x \in \mathbb{R}$ and $n \in \mathbb{N}$ we have

(i)
$$\pi(x) > \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{1.8x}{\log^3 x}$$
 for $x > 32299$;
(ii) $\pi(x) < \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{2.51x}{\log^3 x}$ for $x > 355991$;
(iii) $|\pi(x) - \text{Li}(x)| < .4394 \frac{x}{(\log x)^{3/4}} \exp\left(-\sqrt{\frac{\log x}{9.646}}\right)$ for $x \ge 58$;
(iv) if the Riemann Hypothesis holds, then

$$|\pi(x) - \operatorname{Li}(x)| < \frac{1}{8\pi}\sqrt{x}\log x \quad \text{for } x > 2656;$$

(v) Li(x) >
$$\pi(x)$$
 for $x \le 10^{14}$;
(vi) $p_n < n(\log n + \log \log n)$ for $n \ge 6$;
(vii) $p_n > n \log n$ for $n \ge 1$;
(viii) $\frac{n}{\varphi(n)} < 1.7811 \log \log n + \frac{2.51}{\log \log n}$ for $n \ge 3$.

Proof. We mention the references where the estimates from Prime Number Theory given in the lemma can be found: (i), (ii) Dusart [2, p. 36]; (iii) Dusart [2, p. 41]; (iv) Schoenfeld [14, p. 339]; (v) Kotnik [6, p. 59]; (vi), (vii) Rosser and Schoenfeld [10, p. 69]; (viii) Rosser and Schoenfeld [10, p. 72].

LEMMA 2.2. Let x be a real number with x > 712000. Then

$$2\pi\left(\frac{x}{2}\right) - \pi(x) > \frac{.693x}{\log^2 x}.$$

Proof. We have, by Lemma 2.1(i)–(ii), for x > 712000,

$$2\pi(x/2) - \pi(x) > \frac{x}{\log(x/2)} + \frac{x}{\log^2(x/2)} + \frac{1.8x}{\log^3(x/2)} - \frac{x}{\log x} - \frac{x}{\log^2 x} - \frac{2.51x}{\log^3 x} > \frac{x}{\log x \left(1 - \frac{\log 2}{\log x}\right)} - \frac{x}{\log x} + \frac{x}{\log^2 x \left(1 - \frac{\log 2}{\log x}\right)^2} - \frac{x}{\log^2 x} - \frac{.71x}{\log^3 x} > \frac{x}{\log x} \cdot \frac{\log 2}{\log x} + \frac{x}{\log^2 x} \cdot \frac{2\log 2}{\log x} - \frac{.71x}{\log^3 x} > \frac{.693x}{\log^2 x}.$$

LEMMA 2.3. Let x and y be positive real numbers with x > y, $x \ge 59$. Then

$$2\pi(x+y) - \pi(x) - \pi(x+2y) > \frac{y^2}{(x+2y)\log^2(x+2y)} - \frac{1.7576(x+2y)}{(\log x)^{3/4}}e^{-\sqrt{(\log x)/9.646}}$$

Proof. By Lemma 2.1(iii),

$$2\pi(x+y) - \pi(x) - \pi(x+2y)$$

> 2Li(x+y) - Li(x) - Li(x+2y) - 1.7576 $\frac{x+2y}{(\log x)^{3/4}} \exp\left(-\sqrt{\frac{\log x}{9.646}}\right)$.

Observe that

$$2\operatorname{Li}(x+y) - \operatorname{Li}(x) - \operatorname{Li}(x+2y) = \int_{x}^{x+y} \frac{dt}{\log t} - \int_{x+y}^{x+2y} \frac{dt}{\log t} = \int_{x}^{x+y} \left(\frac{1}{\log t} - \frac{1}{\log(t+y)}\right) dt = \frac{y^2}{\xi \log^2 \xi}$$

for some ξ with $x < \xi < x + 2y$, by the mean value theorem applied twice. Thus

$$2\pi(x+y) - \pi(x) - \pi(x+2y) > \frac{y^2}{(x+2y)\log^2(x+2y)} - 1.7576\frac{x+2y}{(\log x)^{3/4}}\exp\left(-\sqrt{\frac{\log x}{9.646}}\right).$$

LEMMA 2.4. Suppose the Riemann Hypothesis holds true. Let x > y > 0, $x \ge 2657$. Then

$$2\pi(x+y) - \pi(x) - \pi(x+2y) > \frac{y^2}{(x+2y)\log^2(x+2y)} - \frac{\log(x+2y)}{\theta}\sqrt{x+2y}$$

where

$$\theta = \begin{cases} 2\pi & \text{if } x + 2y > 10^{14}, \\ 4\pi & \text{if } x + 2y \le 10^{14}. \end{cases}$$

Proof. By Lemma 2.1(iv)–(v),

$$2\pi(x+y) - \pi(x) - \pi(x+2y) > 2\text{Li}(x+y) - \text{Li}(x) - \text{Li}(x+2y) - \frac{\log(x+2y)}{\theta}\sqrt{x+2y}.$$

The lemma follows in the same way as in the proof of Lemma 2.3. \blacksquare

3. A criterion for an integer k not to be a P-integer. Suppose k is a P-integer > 30. Further, due to results from [3] and [12] mentioned in the introduction, we may also assume that neither k nor k/2 is prime. Let $\varphi(k) + \omega(k) = T$. Then there are exactly $\varphi(k)$ primes belonging to the set $\{p_1, \ldots, p_T\}$ which are coprime to k and form a reduced residue system mod k. The remaining $\omega(k)$ primes in this set divide k. Let

$$D'_{k} = \{i \leq T : p_{i} \pmod{k} < k/2\}, D''_{k} = \{i \leq T : p_{i} \pmod{k} \ge k/2\}, D'''_{k} = \{i \leq T : p_{i} \mid k\}.$$

Note that $|D_k'''| = \omega(k)$ where |A| denotes the number of elements of a set A. By the symmetry of the primitive residues about k/2, we get

$$|D'_k \setminus D'''_k| = |D''_k \setminus D'''_k|,$$

which implies

(1)
$$|D'_k| - |D''_k| \le |D'''_k| = \omega(k).$$

Let t be an integer such that $tk < p_T < (t+1)k$. We observe that if $p_T \in (tk, tk + k/2)$, then

$$|D'_k| = \sum_{n=0}^{t-1} (\pi(nk+k/2) - \pi(nk)) + T - \pi(tk),$$
$$|D''_k| = \sum_{n=0}^{t-1} (\pi(nk+k) - \pi(nk+k/2)),$$

and if $p_T \in (tk + k/2, tk + k)$, then

$$|D'_k| = \sum_{n=0}^{t} (\pi(nk+k/2) - \pi(nk)),$$

$$|D''_k| = \sum_{n=0}^{t-1} (\pi(nk+k) - \pi(nk+k/2)) + T - \pi(tk+k/2).$$

Thus we get

$$|D'_k| - |D''_k| = \sum_{n=0}^{t-1} (2\pi(nk + k/2) - \pi(nk) - \pi(nk + k)) + T - \pi(tk)$$

in the former case, and in the latter case

$$|D'_k| - |D''_k| = \sum_{n=0}^t (2\pi(nk+k/2) - \pi(nk) - \pi(nk+k)) + \pi(tk+k) - T.$$

Let L(k) = t - 1 in the former case and L(k) = t in the latter. Let L := L(k). We shall use this parameter L later on without any further mentioning. Noting that $T - \pi(tk)$ and $\pi(tk + k) - T$ are both non-negative and that $\omega(k) < \log k$, we find by (1) the following criterion.

LEMMA 3.1. The integer k is not a P-integer if

$$S_L := \sum_{n=0}^{L} (2\pi(nk+k/2) - \pi(nk) - \pi(nk+k)) - \log k > 0.$$

We note that

 $tk < p_T \le p_k \le k \log(k \log k)$

by Lemma 2.1(vi). Thus

(2)
$$L \le t < \log(k \log k).$$

On the other hand, using Lemma 2.1(vii)–(viii), putting

$$h(k) = 1.7811 \log \log k + \frac{2.51}{\log \log k},$$

we get

(3)
$$L+2 \ge t+1 > \frac{p_T}{k} \ge \frac{p_{\varphi(k)}}{k} > \frac{\log k - \log h(k)}{h(k)}.$$

4. A computational result

THEOREM 4.1. If $30 < k \le 10^{11}$, then k is not a P-integer. Further, if k is even with $30 < k \le 2 \cdot 10^{11}$ then k is not a P-integer.

Proof. In [3] it has been computationally verified that no integer k with $30 < k < 5.5 \cdot 10^5$ is a *P*-integer. Hence we may assume henceforth that

$$5.5 \cdot 10^5 \le k \le 2 \cdot 10^{11}.$$

To cover this interval, we apply a modified version of the algorithm used in [3].

To prove the statement for a given k we apply the following strategy. We find a prime p such that $k and p (mod k) is also a prime. Then k is not a P-integer. To make this strategy work on the whole range for k under consideration, we shall make use of the following two properties. Let k be an integer with <math>k \geq 5.5 \cdot 10^5$. Then

(4)
$$\pi(k+1) + 100 < \varphi(k)$$

and

(5)
$$p_{\pi(k+1)+100} < 1.5k.$$

These assertions can be easily checked e.g. by Magma [1], using parts (ii), (vi), (viii) of Lemma 2.1.

First we prove the statement for the even values of k. This is done by the algorithm below, which is based on the strategy indicated above.

INITIALIZATION. Let $k_0 = 5.5 \cdot 10^5$. Let H be the list of the first 100 primes larger than $k_0 + 1$, i.e. $H = [p_{\pi(k_0+1)+1}, \ldots, p_{\pi(k_0+1)+100}]$.

STEP 1. For the primes $p \in H$ check successively whether $p \pmod{k_0}$ is also a prime. When such a p is found then, by (4), k_0 is not a P-integer; proceed to the next step.

STEP 2. Check if $k_0 + 3$ is a prime. If not, then proceed to Step 3. If so, this is the first element of H. Remove this prime from H, and append to H the prime $p_{\pi(k_0+1)+101}$, which is the next prime to the last element of H.

STEP 3. If $k_0 < 2 \cdot 10^{11}$ then put $k_0 := k_0 + 2$, and go to Step 1.

Using this procedure we could check by a Magma program that there is no even *P*-integer in the interval $[5.5 \cdot 10^5, 2 \cdot 10^{11}]$.

Let now k be odd with $5.5 \cdot 10^5 < k < 10^{11}$. Then by our algorithm above, using (4) and (5), we know that there exists a prime p satisfying

180

 $2k such that <math>q := p \pmod{2k}$ is also a prime. Observe that q < k. Thus, as $\varphi(k) = \varphi(2k)$, p is a prime such that $k and <math>q = p \pmod{k}$ is also a prime. Hence k is not a P-integer and the theorem follows.

5. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. Let k be an integer with $k \ge 10^{3500}$. Then by (3), L > 500. We apply Lemma 2.1(i)–(ii) to get

$$2\pi(k/2) - \pi(k) > \frac{k}{\log(k/2)} + \frac{k}{\log^2(k/2)} + \frac{1.8k}{\log^3(k/2)} - \frac{k}{\log k} - \frac{k}{\log^2 k} - \frac{2.51k}{\log^3 k}$$

For $n \ge 1$ we apply Lemma 2.3 with x = nk, y = k/2 to find

$$2\pi(nk+k/2) - \pi(nk) - \pi(nk+k)$$

>
$$\frac{k}{4(n+1)\log^2(nk+k)} - 1.7576\frac{nk+k}{(\log nk)^{3/4}}\exp\left(-\sqrt{\frac{\log(nk)}{9.646}}\right).$$

Put

$$f_0(k) := \frac{k}{\log(k/2)} + \frac{k}{\log^2(k/2)} + \frac{1.8k}{\log^3(k/2)} - \frac{k}{\log k} - \frac{k}{\log^2 k} - \frac{2.51k}{\log^3 k} - \log k,$$

$$f_n(k) := \frac{k}{4(n+1)\log^2(nk+k)} - 1.7576 \frac{nk+k}{(\log nk)^{3/4}} \exp\left(-\sqrt{\frac{\log(nk)}{9.646}}\right)$$

for $n \geq 1$. A simple calculation shows that S_L , defined in Lemma 3.1, satisfies

$$S_L \ge f_0(k) + \sum_{n=1}^{L} f_n(k) > 0$$

for $L \leq 1500$. This implies that k is not a P-integer for such L. Hence we may assume that L > 1500.

We first check by Maple that $f_n(k)$ is a strictly decreasing function of n. By (2) it is therefore enough to show that

$$f_0(k) + \sum_{i=1}^{1500} f_i(k) + (L - 1500)f_n(k) > 0$$

for $k = 10^{3500}$ and $n = \lfloor \log(k \log k) \rfloor$. We check this again with Maple to get the final contradiction.

REMARK. The constant 9.646 which occurs in Lemma 2.1(iii) originates from a zero-free region of the Riemann zeta function derived by Rosser and Schoenfeld [11, Theorem 11], where the constant appears as R. The zero-free region has been widened by Kadiri in [5] where the corresponding constant R is 5.69693. If this constant is substituted into Lemma 2.1(iii) instead of the constant 9.646 and we follow our argument, we find that if k is a P-integer, then $k < 10^{1000}$. However, we do not know if this substitution is justified.

Proof of Theorem 1.2. Suppose the Riemann Hypothesis is true. Let k be an integer with $k \ge 3 \cdot 10^{13}$. By Lemma 2.2, we get

$$2\pi\left(\frac{k}{2}\right) - \pi(k) > \frac{.693k}{\log^2 k} > \log k > \omega(k).$$

For $n = 1, 2, ..., \lfloor \log(k \log k) \rfloor - 1$ we apply Lemma 2.4 with x = nk, y = k/2 to find

$$2\pi(nk+k/2) - \pi(nk) - \pi(nk+k) > \frac{k}{4(n+1)\log^2(nk+k)} - \frac{\log(nk+k)}{2\pi}\sqrt{nk+k}.$$

The term on the right hand side of the above inequality is positive if

$$\pi\sqrt{k} > 2(n+1)^{1.5}\log^3(nk+k).$$

This is satisfied, since $n < \log(k \log(k)) - 1$ and $k \ge 3 \cdot 10^{13}$. Hence by Lemma 3.1, we find that k is not a P-integer.

Next we take $k < 3 \cdot 10^{13}$. By Theorem 4.1, we may assume $k > 10^{11}$. Note that $L < \log(k \log k) \le 34$. Further,

$$L < \log k + \log \log k < 1.13 \log k$$

giving

$$k > e^{.88L} > 10^{.38L}$$
.

Define

$$k_L = [10^{\{.38L\}}]10^{[.38L]},$$

where [x] and $\{x\}$ denote the integral and fractional part of a real number x. Note that for any fixed L with $L \leq 34$ if $L(k) \geq L$, then $k \in [k_L, 3 \cdot 10^{13})$. Applying Lemma 2.4 with x = nk, y = k/2 we find

$$S_L > 2\pi(k/2) - \pi(k) - \log k + \sum_{n=1}^{L} \left(\frac{k}{4(n+1)\log^2(nk+k)} - \frac{\log(nk+k)}{4\pi} \sqrt{nk+k} \right).$$

For $n = 1, \ldots, L$, put

$$F_n(k) := \frac{1}{L} \left(\frac{k}{\log(k/2)} + \frac{k}{\log^2(k/2)} + \frac{1.8k}{\log^3(k/2)} \right) - \frac{1}{L} \left(\frac{k}{\log k} + \frac{k}{\log^2 k} + \frac{2.51k}{\log^3 k} + \log k \right) + \frac{k}{4(n+1)\log^2(nk+k)} - \frac{\log(nk+k)}{4\pi} \sqrt{nk+k}.$$

We have, by Lemma 2.1(i)–(ii),

$$S_L > \sum_{n=1}^L F_n(k).$$

So it is sufficient to show that the right hand side is positive. For this, we proceed as follows. First, let $29 \leq L \leq 34$. We calculate the value k_L from its definition above. Thus (L, k_L) is one of the pairs from

 $\{(29, 10^{11}), (30, 2 \cdot 10^{11}), (31, 6 \cdot 10^{11}), (32, 10^{12}), (33, 3 \cdot 10^{12}), (34, 8 \cdot 10^{12})\}.$

We check by Maple that all functions $F_n(k)$ are strictly increasing on $[k_L, 3 \cdot 10^{13}]$, and further

$$\sum_{n=1}^{L} F_n(k_L) > 0.$$

Hence by Lemma 3.1, there is no *P*-integer k with $L(k) \in [29, 34]$. Now we consider $k \in [10^{11}, 3 \cdot 10^{13}]$. Then obviously L(k) > 0. We may assume $1 \leq L \leq 28$. We check that all functions $F_n(k)$ are strictly increasing and the preceding inequality also holds. Hence we conclude that no integer $k \in [10^{11}, 3 \cdot 10^{13}]$ is a *P*-integer.

Acknowledgements. The authors are grateful to the referee for her/his helpful and useful remarks.

Research of L. Hajdu was supported in part by the OTKA grants K67580 and K75566, and by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund.

References

- W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), 235–265.
- P. Dusart, Autour de la fonction qui compte le nombre de nombres premiers, thèse, Université de Limoges, 1998, 172 pp.
- [3] L. Hajdu and N. Saradha, On a problem of Recaman and its generalization, J. Number Theory 131 (2011), 18–24.
- [4] 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.
- [5] H. Kadiri, Une région explicite sans zéros pour la fonction ζ de Riemann, Acta Arith. 117 (2005), 303–339.
- [6] T. Kotnik, The prime-counting function and its analytic approximations. $\pi(x)$ and its approximations, Adv. Comput. Math. 29 (2008), 55–70.
- Yu. V. Linnik, On the least prime in an arithmetic progression, Rec. Math. (Mat. Sb.) N.S. 15 (57) (1944), 139–178, 347–368.

L. Hajdu et al.

- C. Pomerance, A note on the least prime in an arithmetic progression, J. Number Theory 12 (1980), 218–223.
- K. Prachar, Über die kleinste Primzahl einer arithmetischen Reihe, J. Reine Angew. Math. 206 (1961), 3–4.
- [10] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962), 64–94.
- [11] J. B. Rosser and L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, Math. Comp. 29 (1975), 243–269.
- N. Saradha, Conjecture of Pomerance for some even integers and odd primorials, Publ. Math. Debrecen 79 (2011), 699–706.
- [13] A. Schinzel, Remark on the paper of K. Prachar "Über die kleinste Primzahl einer arithmetischen Reihe", J. Reine Angew. Math. 210 (1962), 121–122.
- [14] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II, Math. Comp. 30 (1976), 337–360, 900.
- [15] T. Xylouris, On Linnik's constant, thesis, arXiv:0906.2749 [math.NT], 2009.

L. Hajdu Institute of Mathematics University of Debrecen and the Number Theory Research Group of the Hungarian Academy of Sciences P.O. Box 12 H-4010 Debrecen, Hungary E-mail: hajdul@science.unideb.hu N. Saradha School of Mathematics Tata Institute of Fundamental Research Dr. Homibhabha Road Colaba, Mumbai, India E-mail: saradha@math.tifr.res.in

R. Tijdeman Mathematical Institute Leiden University P.O. Box 9512 2300 RA Leiden, The Netherlands E-mail: tijdeman@math.leidenuniv.nl

Received on 18.7.2011 and in revised form on 22.9.2011

(6767)