On infinitude of primes

S Srinivasan

▶ **To cite this version:**

S Srinivasan. On infinitude of primes. Hardy-Ramanujan Journal, 1984, Volume 7 - 1984, pp.21 - 26. 10.46298/hrj.1984.112 . hal-01104356

HAL Id: hal-01104356
https://hal.science/hal-01104356v1

Submitted on 16 Jan 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Hardy Ramanujan Journal
Vol. 7 (1984) 21—26

ON INFINITUDE OF PRIMES

By

S. SRINIVASAN

Let x_m $(m \geq 1)$ be an increasing sequence of positive integers satisfying

(1) $$x_m \mid x_{m+1}, \quad (x_m, x_{m+1} / x_m) = 1.$$

This immediately implies the infinitude of primes. For example, $a(n) = n^2 + n + 1$ satisfies $a(n^2) = a(n)\, a(-n)$ and $(a(n), a(-n)) = 1$ giving (1) with, in particular, $x_m = a(2^{2^m})$.

Further, for given prime p, taking $x_m = 2^{p^m} - 1$ we see that (1) is fulfilled, because then if a prime q divide x_m one has

(2) $$x_{m+1} / x_m = 1 + (x_m + 1) + \ldots + (x_m + 1)^{p-1}$$
$$\equiv p \pmod{q};$$

i.e., $(x_m, x_{m+1} / x_m)$ divides p; but $x_m \equiv 1 \pmod{p}$.

Now, from (1), it easily follows that $q \equiv 1 \pmod{p^{m+1}}$ for every prime q dividing x_{m+1} / x_m;

in particular we have infinitude of primes $\equiv 1 \pmod{p^r}$ for any given prime p and $r \geq 1$.

Actually, on the same principle, one can prove the infinitude of primes $\equiv 1 \pmod{k}$ for any given integer k (> 1). In fact, we can prove the following theorem.

Theorem.

Let K (>1), k (>1) be given integers. Then, for infinitely many primes q, we have

$$e_K(q) \equiv O \pmod{k^{[c_k \log\log q]}} \tag{3}$$

with a certain $c_k > 0$, where $e_K(q)$ denotes the exponent of K modulo q. In particular,

$$q \equiv 1 \pmod{k} \text{ for an infinity of primes } q. \tag{3'}$$

Proof.

Let $k = \prod_{i=1}^{s} p_i^{a_i}$ $(a_i \geqslant 1;$ primes $p_1 < \ldots < p_s)$ and set, for $r \geqslant 1$, $n = k^r$. Next, define $d_i = np_i^{-ra_i}$ and, for $m > 1$,

$$y_m = K_1^{n^m} - (-1)^k; \tag{4}$$

$$y'_m = l.c.m.(y_m, y_{m,1}, \ldots, y_{m,s}),$$

where $y_{m,i} = K_1^{d_i^{m+1} p_i^{ra_i}} - (-1)^k$, and

$$K_1 = K^{\phi(k)}.$$

Observe that

$$(y_j, K_1) = 1;\ y'_m \mid y_{m+1} \tag{5}$$

$$(\text{set } y'_m y''_m = y_{m+1}).$$

Now consider $m' = n^m + n^{m+1}(p_1^{-rma_1} + \ldots + p_s^{-rma_s})$

$\leqslant c\, n^{m+1}$ with $c = \frac{11}{12}$. (For $n = 2,3$, check $c > \frac{3}{4}$ suffices;

and for $n > 4$, $c > \frac{\pi^2}{6} - 1 + \frac{1}{4}$ suffices.) Hence we have

$$y''_m > \left(\frac{1}{2}K_1^{n^{m+1}}\right) / (2^{s+1}K_1^{m'}) > K_1^{-(s+2)+n^{m+1}/12}$$

Because $s < n-1$, we obtain

$$y''_m > K_1^{n} \quad (m > 5). \tag{5'}$$

As with (2), we get

$$(y'_m, y''_m) = 2^B \tag{6}$$

for some $B > 0$.

Case i.

k *odd*. Note that $y_j \not\equiv 0 \pmod 4$, and so by (5') there is an odd prime q dividing y_m''. Now (since (K, q) = 1 by (5)) $e_K(q)$ divides $2\phi(K)\, n^{m+1}$ but does not divide $\phi(k)\, n^{m+1}$. Denoting by b_i the exact power of p_i in $e_K(q)$, suppose for *some* i, $b_i < a_i r$. This would mean that $e_K(q)$ divides $2\phi(k)\, d_i^{m+1} p_i^{ra_i}$ but does not divide $\phi(k)\, d_i^{m+1} p_i^{ra_i}$, Consequently $q \mid y_{m,i} \mid y'_m$ in contradiction to (6)

So, $b_i > ra_i$ $(1 \le i \le s)$, i. e.,

$$k^r \mid e_K(q) \mid 2\phi(k)\, n^{m+1}; \qquad m > 5. \tag{7'}$$

Taking here m = 5, say we get $q < K_1^{k^{1+6r}} < K^{k^{8r}}$ giving (3). This completes the proof in this case (on letting $r \to \infty$.)

Case (ii)

k *even*. Now we proceed to determine α_j, the exact power of 2 in y_j. If K is even, we have $\alpha_j = 0$. If $K = 2^{\alpha}K_0 + 1$, $K_0 = 2^{\beta} K' - 1$ with $\alpha > 1$, $\beta > 1$ and K′ odd, we see that $\alpha_j = A + \beta_1 + rj\beta_2$, where β_1, β_2 denote the exact power of 2 in ϕ (k), k (respectively) and $A = \alpha$ or $A = \beta + 1$ according as $\alpha \neq 1$, or $\alpha = 1$. Thus the exact power of 2 in y_{m+1} / y_m is $\alpha_{m+1} - \alpha_m = r\beta_2$. Since $r\beta_2 < n$ (trivially), we again conclude that y''_m has an odd prime divisor q. Proceeding, as in (i), with this q we can conclude that

$$(7'') \qquad k^r \mid e_K(q) \mid \phi(k)\, n^{m+1} \; ; m > 5.$$

The proof is completed again as before (in (i)).

Remarks.

(i) Taking r = 1 above, with K = 2 say, we obtain that for any given k (> 1) there is a prime $q \equiv 1 \pmod{k}$, with $q < 2^{k^7}$.

(ii) For given K (> 1), k (> 1) denoting by $Q_K(k)$ the set of primes q (constructed as in the above proof, with r > 1), we can conclude from (7′), (7″) that $Q_K(k_1)$ and $Q_K(k_2)$ are disjoint if k_j has a prime factor not dividing $k_i\, \phi(k_i)$.

In particular,

$$(8) \qquad Q_K(p) \cap Q_K(p') = \phi, \text{ primes } p \neq p'.$$

(iii) For given k (> 2), we can prove also the infinitude of primes $\neq 1 \pmod{k}$ via sequences x_m satisfying (1). To this

end, we see easily that it suffices if further $x_{m+1}/x_m \neq 1 \pmod{k}$ for sufficiently large m. These conditions are fulfilled by the choice $x_m = q^{q^m} - (-1)^q$, where (for example) $q = 2$, if k is not a power of 2 and $q = 3$, otherwise. (More can be similarly proved; like $q \equiv l \pmod{k}$ for some $l^2 \not\equiv 1 \pmod{k}$, if $k \times 24$. However, these will appear elsewhere.)

(iv) Also, we have from (7′), (7″) that

$$P(e_K(q)) = P(k) \tag{9}$$

holds for infinitely many primes $q \equiv 1 \pmod{k^{[c_k \log\log q]}}$ where P(m) denotes the greatest prime divisor of m.

(v) Perhaps the remarks in the current article are at least anticipated, as suggested by Professor H. Halberstam pointing out Ex. 5* on p. 59 of [1]. However, it may be noted that, writing $f_n(x)$ for the polynomial f(x) in the above exercise (which is close to the second paragraph of this article), the present article treats, in contrast, x as *fixed* and n as *varying*.

Acknowledgement.

I wish to express my thanks to Professor K. Ramachandra for checking through the manuscript. Also, I wish to thank Professor H. Halberstam for his comment (in Remark (v) above)

Reference

1. **W. J. Le Veque,** *Topics in Number Theory, Vol I,* Addison-Wesley (1956).

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005 (India)