Ramanujan J
DOI 10.1007/s11139-012-9420-8

# Odd prime values of the Ramanujan tau function

**Nik Lygeros · Olivier Rozier**

Received: 22 May 2012 / Accepted: 8 July 2012


**Abstract** We study the odd prime values of the Ramanujan tau function, which form a thin set of large primes. To this end, we define $LR(p,n) := \tau(p^{n-1})$ and we show that the odd prime values are of the form $LR(p,q)$ where $p,q$ are odd primes. Then we exhibit arithmetical properties and congruences of the $LR$ numbers using more general results on Lucas sequences. Finally, we propose estimations and discuss numerical results on pairs $(p,q)$ for which $LR(p,q)$ is prime.

**Keywords** Ramanujan function · Primality · Lucas sequences

**Mathematics Subject Classification (2010)** 11A41 · 11F30 · 11Y11

## 1 Introduction

The tau function is defined as the Fourier coefficients of the modular discriminant

$$\Delta(z) = q \prod_{n=1}^{+\infty} (1 - q^n)^{24} = \sum_{n=1}^{+\infty} \tau(n) q^n,$$

where $z$ lies in the complex upper half-plane and $q = e^{2\pi i z}$.

Nearly a century ago, the Indian mathematician Srinivasa Ramanujan showed great interest in the tau function and discovered some of its remarkable properties.

N. Lygeros
LGPC (UMR 5285), Université de Lyon, 69616, Villeurbanne, France
e-mail: nlygeros@gmail.com

O. Rozier (✉)
Service de calcul parallèle S-CAPAD, IPGP (UMR 7154), 75238, Paris, France
e-mail: olivier.rozier@gmail.com

Published online: 15 March 2013

Below are listed the known identities and congruences for the tau function:

$$\tau(nm) = \tau(n)\tau(m) \qquad \text{for } n, m \text{ coprime integers;} \tag{1}$$

$$\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}) \qquad \text{for } p \text{ prime and } r \text{ an integer } \geq 1; \tag{2}$$

$$\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}} \qquad \text{for } n \equiv 1 \pmod 8; \tag{3}$$

$$\tau(n) \equiv 1217\sigma_{11}(n) \pmod{2^{13}} \qquad \text{for } n \equiv 3 \pmod 8; \tag{4}$$

$$\tau(n) \equiv 1537\sigma_{11}(n) \pmod{2^{12}} \qquad \text{for } n \equiv 5 \pmod 8; \tag{5}$$

$$\tau(n) \equiv 705\sigma_{11}(n) \pmod{2^{14}} \qquad \text{for } n \equiv 7 \pmod 8; \tag{6}$$

$$\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^6} \qquad \text{for } n \equiv 1 \pmod 3; \tag{7}$$

$$\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^7} \qquad \text{for } n \equiv 2 \pmod 3; \tag{8}$$

$$\tau(n) \equiv n^{-30}\sigma_{71}(n) \pmod{5^3} \qquad \text{for } n \not\equiv 0 \pmod 5; \tag{9}$$

$$\tau(n) \equiv n\sigma_9(n) \pmod 7 \qquad \text{for } n \equiv 0, 1, 2, 4 \pmod 7; \tag{10}$$

$$\tau(n) \equiv n\sigma_9(n) \pmod{7^2} \qquad \text{for } n \equiv 3, 5, 6 \pmod 7; \tag{11}$$

$$\tau(p) \equiv 0 \pmod{23} \qquad \text{for } p \text{ prime, } \left(\frac{p}{23}\right) = -1; \tag{12}$$

$$\tau(p) \equiv \sigma_{11}(p) \pmod{23^2} \qquad \text{for } p \text{ prime of the form } u^2 + 23v^2; \tag{13}$$

$$\tau(p) \equiv -1 \pmod{23} \qquad \text{for other prime } p; \tag{14}$$

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}, \tag{15}$$

where $u$, $v$ are integers, $\sigma_k(n)$ denotes the sum of the $k$th powers of the divisors of $n$, and $(\frac{\cdot}{\cdot})$ denotes the Legendre symbol.

All congruences are given with their respective authors in [11], except (13) which is due to Serre. Swinnerton-Dyer showed that there are no congruences for $\tau(n)$ modulo primes other than 2, 3, 5, 7, 23 and 691.

Ramanujan [7] conjectured, and Deligne proved, the upper bound

$$\left|\tau(p)\right| \leq 2p^{\frac{11}{2}} \qquad \text{for } p \text{ prime.} \tag{16}$$

We recall that the values of the tau function are almost always divisible by any integer [10, p. 243].

In this paper, we will study the integers $n$ for which $\tau(n)$ is an odd prime, disregarding the sign of $\tau(n)$. It is easily seen that $\tau(n)$ is odd if and only if $n$ is an odd square. Then from (1) one should expect the smallest integer $n$ for which $\tau(n)$ is an odd prime to be of the form $p^r$ where $r$ is even and $p$ odd prime.

Indeed, D. H. Lehmer [2] found that $n = 63001 = 251^2$ is the smallest integer for which $\tau(n)$ is prime:

$$\tau(251^2) = -80561663527802406257321747.$$

Without the power of today's computers, proving such a result was not straightforward.

## 2 LR numbers

We propose to define the *LR* family of integers, in memory of D.H. Lehmer and S. Ramanujan, as follows:

**Definition 1** Let $p, q$ be odd primes. Then we define $LR(p,q) := \tau(p^{q-1})$. More generally, we shall use the notation $LR(p,n) := \tau(p^{n-1})$ for all positive integers $n$ and we set the value $LR(p,0) := 0$.

The main motivation for the introduction of the previous definition is related to Theorem 1, for which we will give a proof. It states a strong necessary condition on the integers $n$ such that $\tau(n)$ is an odd prime. Our notation will prove to be relevant as the "diagonal" terms $LR(p,p)$ have specific arithmetical properties (see Theorem 4).

In what follows, a prime $p$ such that $p \nmid \tau(p)$ is called ordinary. Otherwise $p$ is said to be non-ordinary.

**Theorem 1** *Let $n$ be a positive integer such that $\tau(n)$ is an odd prime. Then $n = p^{q-1}$ where $p$ and $q$ are odd primes and $p$ is ordinary.*

*Remark 1* Only finitely many non-ordinary primes are known to exist: 2, 3, 5, 7, 2411, 7758337633. We expect them to be the smallest elements of a very thin infinite set [4]. They are also referred to as supersingular primes.

Now we provide several formulations, notations, and intermediate results concerning the *LR* numbers that will be useful in our study.

Let $p$ be an odd prime. The recurrence relation (2) implies that $LR(p,n)$ is the $n$th term of the Lucas [3] sequence associated with the polynomial $X^2 - \tau(p)X + p^{11}$. Hence for $n > 0$, $LR(p,n)$ is a polynomial of degree $(n-1)$ in $\tau(p)$ and $p^{11}$:

$$LR(p,n) = \sum_{k=0}^{[\frac{n-1}{2}]} (-1)^k \binom{n-1-k}{k} p^{11k} \tau(p)^{n-1-2k}. \tag{17}$$

The divisibility property of the Lucas sequences applies:

$$\text{if} \quad m \mid n, \quad \text{then} \quad LR(p,m) \mid LR(p,n). \tag{18}$$

Our sequence has discriminant

$$D_p := \tau(p)^2 - 4p^{11} \tag{19}$$

which is negative by (16). We get the general expression

$$LR(p,n) = \frac{\alpha_p^n - \overline{\alpha}_p{}^n}{\alpha_p - \overline{\alpha}_p}, \quad \text{with } \alpha_p = \frac{\tau(p) + \sqrt{D_p}}{2}.$$

**Table 1** First values of $\tau(p)$, $\theta_p/\pi$, $\cos\theta_p$ and $\sin\theta_p$

| $p$ | $\tau(p)$ | $\theta_p/\pi$ | $\cos\theta_p$ | $\sin\theta_p$ |
|---|---|---|---|---|
| 2 | −24 | 0.585426 | −0.265165 | 0.964203 |
| 3 | 252 | 0.403225 | 0.299367 | 0.954138 |
| 5 | 4830 | 0.387673 | 0.345607 | 0.938379 |
| 7 | −16744 | 0.560289 | −0.188274 | 0.982117 |
| 11 | 534612 | 0.333173 | 0.500436 | 0.865773 |
| 13 | −577738 | 0.569230 | −0.215781 | 0.976442 |
| 17 | −6905934 | 0.700803 | −0.589825 | 0.807531 |
| 19 | 10661420 | 0.335570 | 0.493901 | 0.869518 |
| 23 | 18643272 | 0.402350 | 0.301988 | 0.953312 |
| 29 | 128406630 | 0.302561 | 0.581257 | 0.813720 |
| 31 | −52843168 | 0.553006 | −0.165756 | 0.986167 |
| 37 | −182213314 | 0.569299 | −0.215993 | 0.976395 |
| 41 | 308120442 | 0.433411 | 0.207673 | 0.978198 |
| 43 | −17125708 | 0.502827 | −0.008882 | 0.999961 |
| 47 | 2687348496 | 0.173811 | 0.854586 | 0.519310 |

Following Ramanujan [7], we define the angles $\theta_p \in (0,\pi)$ such that $\tau(p) = 2p^{\frac{11}{2}}\cos\theta_p$. Some values of $\tau(p)$ and $\theta_p/\pi$ are listed in Table 1. Then we derive an equivalent formulation related to the Chebyshev polynomials of the second kind:

$$LR(p,n) = p^{\frac{11(n-1)}{2}} \frac{\sin(n\theta_p)}{\sin\theta_p} = \prod_{k=1}^{n-1}\left(\tau(p) - 2p^{\frac{11}{2}}\cos\frac{k\pi}{n}\right). \tag{20}$$

Hence, a fair estimation of the size of $|LR(p,n)|$ is given by $p^{\frac{11}{2}(n-1)}$ in most cases. This is supported by the numerical results.

Theorem 2, due to Murty, Murty and Shorey [6], proves that the tau function takes any fixed odd integer value, and *a fortiori* any odd prime value, finitely many times.

**Theorem 2** *There exists an effectively computable absolute constant $c>0$, such that for all positive integers $n$ for which $\tau(n)$ is odd, we have*

$$\left|\tau(n)\right| \geq (\log n)^c.$$

The next result is somehow related to Theorem 2 (see Remark 2), and will be used in the proof of Theorem 1.

**Lemma 1** *The equation $\tau(n) = \pm 1$ has no solution for $n > 1$.*

*Proof* (sketch) By property (1), we can assume without loss of generality that $n = p^r$ for a prime $p$ and integer $r > 0$. Thus $\tau(n) = LR(p, r+1)$.

Now it suffices to apply known results on Lucas sequences (Theorems C, 1.3, and 1.4 in [1]) to show that $LR(p, r+1)$ has a primitive divisor. □

*Remark 2* It is not quite obvious for us if Lemma 1 is a corollary of Theorem 2, as the latter appears to be essentially of qualitative nature. Moreover, the effectiveness in the special case $\tau(n) = \pm 1$ is nowhere mentioned in [6].

## 3 Proof of Theorem 1

Let $n$ be a positive integer such that $\tau(n)$ is an odd prime.

It follows from the multiplicative property (1) and Lemma 1 that $n$ is a power of a prime $p$. Thus $n = p^r$ for some positive integer $r$ and $\tau(n) = LR(p, r+1)$.

From the divisibility property (18) and once again Lemma 1, it turns out that $r + 1 = q$ where $q$ is prime. Since $LR(p, 2)$ is even, we have $r > 1$ and $q \neq 2$.

Now suppose that $p$ is non-ordinary. We get $p|\tau(p)$ which in turn implies that $p^2|\tau(n)$ by (17). Therefore, we have reached a contradiction.

## 4 Arithmetical properties

The theory of Lucas sequences is well developed (see, e.g., [9]) and has many implications for the LR numbers. It leads to the arithmetical properties:

$$\gcd\big(LR(p,m), LR(p,n)\big) = LR\big(p, \gcd(m,n)\big); \tag{21}$$

$$LR(p,q) \equiv \left(\frac{D_p}{q}\right) \pmod{q}; \tag{22}$$

$$\text{if} \quad q \nmid p \cdot \tau(p), \quad \text{then} \quad q|LR\left(p, q - \left(\frac{D_p}{q}\right)\right); \tag{23}$$

$$LR(p, 2n+1) = LR(p, n+1)^2 - p^{11} LR(p,n)^2 \tag{24}$$

for $m, n$ two positive integers and $p, q$ two odd primes. The discriminant $D_p$ is defined by (19).

Theorems 3 and 4 will prove to be useful in our estimations and numerical calculations (see Sects. 6, 7 and Appendix). As they are also related to known properties of the Lucas sequences, we only give sketches of proof.

**Theorem 3** *Let $p$ and $q$ be two odd primes, $p$ ordinary.*
*If $d$ is a prime divisor of $LR(p,q)$, then $d \equiv \pm 1 \pmod{2q}$ or $d = q$.*
*Moreover, $q|LR(p,q)$ if and only if $q|D_p$.*

*Proof* (sketch) We consider the number $LR(p, \gcd(q, d - (\frac{D_p}{d})))$ and we apply successively (21) and (23). Then we get

$$\gcd\left(q, d - \left(\frac{D_p}{d}\right)\right) \neq 1,$$

and the theorem follows by (22). □

**Theorem 4** *Let $p$ be an ordinary odd prime.*
*If $p \equiv 1 \pmod 4$, then $LR(p, p)$ is composite.*
*If $p \equiv 3 \pmod 4$ and $d$ is a prime divisor of $LR(p, p)$, then $d \equiv \pm 1 \pmod{4p}$.*

*Proof* (sketch) The first part of the theorem follows from formulation (20) leading to the generic factorization $LR(p, p) = N_0 N_1$ where

$$N_j = \prod_{k=1}^{\frac{p-1}{2}} \left( \tau(p) - (-1)^{j+k} \left( \frac{2k}{p} \right) 2p^{\frac{11}{2}} \cos \frac{k\pi}{p} \right), \quad \text{for } j = 0, 1.$$

One may verify that $N_0$ and $N_1$ are integers using the Gauss sum value

$$\sum_{k=1}^{p-1} \left( \frac{k}{p} \right) e^{\frac{2ki\pi}{p}} = \sqrt{p}, \quad \text{for } p \equiv 1 \pmod 4.$$

For the second part, we apply (24) and obtain that $p$ is a quadratic residue modulo $d$. The desired result easily follows by combining the law of quadratic reciprocity with the congruence $d \equiv \pm 1 \pmod{2p}$. □

## 5 Congruences modulo $p \pm 1$

No congruence modulo $p$ is known for $\tau(p)$ (see, e.g., [4]), hence *a fortiori* for the numbers $LR(p, n)$. Here we briefly study the sets $\mathcal{P}^+$ and $\mathcal{P}^-$ of primes $p$ for which the numbers $LR(p, n)$ have elementary congruences modulo $p + 1$ and $p - 1$, respectively, as specified in Lemma 2.

**Lemma 2** *Let $\mathcal{P}^+$ be the set of odd primes $p$ such that $\tau(p) \equiv 0 \pmod{p+1}$. Let $p \in \mathcal{P}^+$. Then $LR(p, n) \equiv 0 \pmod{p+1}$ if $n$ is even, and $LR(p, n) \equiv 1 \pmod{p+1}$ if $n$ is odd.*
*Let $\mathcal{P}^-$ be the set of odd primes $p$ such that $\tau(p) \equiv 2 \pmod{p-1}$. Let $p \in \mathcal{P}^-$. Then $LR(p, n) \equiv n \pmod{p-1}$ for all positive integer $n$.*

*Proof* (sketch) The recurrence relation (2) leads to an easy proof by induction for all positive integers $n$. □

Lemma 3 states that $\mathcal{P}^+$ and $\mathcal{P}^-$ both include most of the small primes. Nevertheless, there is numerical evidence that they have density zero among the primes.

**Lemma 3** *Let $A := 2^{14} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 23 \cdot 691$, and let $\mathcal{P}_0^+$ be the set of odd primes $p$ such that $p + 1 | A$. Then $\mathcal{P}_0^+ \subset \mathcal{P}^+$.*
*Let $B := 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 691$, and let $\mathcal{P}_0^-$ be the set of odd primes $p$ such that $p - 1 | B$. Then $\mathcal{P}_0^- \subset \mathcal{P}^-$.*

*Proof* (sketch) Let $p \in \mathcal{P}_0^+$. Then $p = 2^{r(2)} \cdot 3^{r(3)} \cdot 5^{r(5)} \cdot 7^{r(7)} \cdot 23^{r(23)} \cdot 691^{r(691)} - 1$, with $r(q) \le 14, 7, 3, 2, 1, 1$ for $q = 2, 3, 5, 7, 23, 691$, respectively.

From (3), (4), (5), (6), (8), (9), (11), (12), and (15), it follows that $\tau(p) \equiv 0 \pmod{q^{r(q)}}$ for $q = 2, 3, 5, 7, 23, 691$. Thus $\tau(p) \equiv 0 \pmod{p+1}$, that is $p \in \mathcal{P}^+$.

Similarly, we prove that $\mathcal{P}_0^- \subset \mathcal{P}^-$ using (3), (4), (5), (6), (7), (9), (10), and (15). □

*Remark 3* It is not possible to increase any of the exponents in the previous definitions of $A$ and $B$ without finding counter-examples of Lemma 3.

Obviously, $\mathcal{P}_0^+$ and $\mathcal{P}_0^-$ are finite sets. They comprise respectively 1140 and 325 primes and their smallest and largest elements are given below:

- $\mathcal{P}_0^+ = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 53, 59, 71, 79, 83, 89, 97, \ldots, \frac{1}{6}A - 1, \frac{1}{5}A - 1\}$ and $\max \mathcal{P}_0^+ \approx 6.97 \times 10^{14}$;
- $\mathcal{P}_0^- = \{3, 5, 7, 11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 71, 73, 97, \ldots, \frac{1}{32}B + 1, B + 1\}$ and $\max \mathcal{P}_0^- \approx 9.02 \times 10^{11}$.

Now if we define the residual sets $\mathcal{P}_1^+ := \mathcal{P}^+ \setminus \mathcal{P}_0^+$ and $\mathcal{P}_1^- := \mathcal{P}^- \setminus \mathcal{P}_0^-$, it turns out that

- $\mathcal{P}_1^+ = \{593, 1367, 2029, 2753, 4079, 4283, 7499, 7883, 9749, 11549 \ldots\}$;
- $\mathcal{P}_1^- = \{103, 311, 691, 829, 1151, 1373, 2089, 2113, 2411, 2647, \ldots\}$.

Note that

- $\mathcal{P}^+$ contains the Mersenne primes $M_p := 2^p - 1$ for $p = 2, 3, 5, 7, 13, 17$, and 19, but $M_{31}$ is not in $\mathcal{P}^+$;
- $\mathcal{P}^-$ contains all known Fermat primes $F_n := 2^{2^n} + 1$ for $n = 0, 1, 2, 3, 4$;
- $\mathcal{P}_1^-$ contains the non-ordinary prime 2411 (see Remark 1), but the next one, 7758337633, is not in $\mathcal{P}^+ \cup \mathcal{P}^-$.

## 6 Estimations

Here we provide various estimates on the number and distribution of *LR* primes with only little justification. Then it will be compared with numerical results.

We refer to Wagstaff's heuristic reasoning [12] about the probability for a Mersenne number $M_p$ to be prime, mainly considering that all divisors are of the form $2kp + 1$. The proposed value is

$$\frac{e^{\gamma} \log 2p}{p \log 2},$$

where $\gamma = 0.577215\ldots$ is Euler's constant.

Let $p$ and $q$ be two odd primes such that $p \neq q$ and $\tau(p) \not\equiv 0 \pmod{p}$. We know from Theorem 3 that all prime divisors of $LR(p, q)$ are of the form $2kq \pm 1$, except possibly $q$ with probability $P(q)$. The expected value of $P(q)$ is roughly $1/q$, unless $q = 3$, 5, 7, or 23 for which we have the congruences (7) to (14). We easily get the exceptional values of $P(q)$ for $q = 3, 5$ or $7$ by considering all residues of $p$ modulo $q$ (see also [10, 11]), whereas $P(23)$ is the proportion of primes of the form $u^2 + 23v^2$:

$$P(3) = \frac{1}{2}; \qquad P(5) = \frac{1}{4}; \qquad P(7) = \frac{1}{2}; \qquad P(23) = \frac{1}{6}.$$

Now we estimate the probability that $LR(p,q)$ is prime by

$$\frac{e^\gamma \log 2q}{\log |LR(p,q)|}\big(1 - P(q)\big) \approx \frac{2e^\gamma \log 2q}{11(q-1)\log p}\big(1 - P(q)\big). \tag{25}$$

In the general case where $q \neq 3, 5, 7, 23$, we have $P(q) \approx 1/q$ and (25) simplifies to

$$\frac{2e^\gamma \log 2q}{11q \log p}.$$

If we assume further that $p = q$ and $p \equiv 3 \pmod 4$, then the same reasoning, using the results from Theorem 4, leads to the probability

$$\frac{e^\gamma \log 4p}{\log |LR(p,p)|} \approx \frac{2e^\gamma \log 4p}{11(p-1)\log p}. \tag{26}$$

Now we consider two large integers $p_{\max} \gg 1$ and $q_{\max} \gg 1$. The expected number of primes of the form $LR(p,q)$ for prime $p$ fixed and $q < q_{\max}$ is

$$\frac{2e^\gamma}{11 \log p} \sum_{\text{odd prime } q < q_{\max}} \frac{\log 2q}{q} \sim \frac{2e^\gamma \log q_{\max}}{11 \log p}. \tag{27}$$

Therefore, our estimate at first order for the number of primes of the form $LR(p,q)$ with $p < p_{\max}$ and $q < q_{\max}$ is

$$\frac{2e^\gamma \log q_{\max}}{11} \sum_{\text{ordinary prime } p < p_{\max}} \frac{1}{\log p} \sim \frac{2e^\gamma p_{\max} \log q_{\max}}{11(\log p_{\max})^2}. \tag{28}$$

Using (26), we also estimate the number of primes of the form $LR(p,p)$ with $p < p_{\max}$ by

$$\frac{2e^\gamma}{11} \sum_{\substack{\text{ordinary prime } p < p_{\max} \\ p \equiv 3 \pmod 4}} \frac{\log 4p}{(p-1)\log p} \sim \frac{e^\gamma}{11} \log\log p_{\max}. \tag{29}$$

## 7 Numerical results

We have checked the (probable) primality of $LR(p,q)$ for all pairs $(p,q)$ of odd primes in Table 2 (see Appendix for details). The estimates (*) follow from our first order approximations (28) and (29), whereas the other estimates (**) are simply a sum of the related expressions (25) or (26) over all considered $p, q$ values. The latter

**Table 2** Counting the primes and PRP's of the form $LR(p, q)$

| Conditions on $p, q$ | Max. number of digits | Number of (probable) primes | | |
|---|---|---|---|---|
| | | Actual | Expected* | Expected** |
| $(p < 10^6)$ and $(q < 100)$ | 3169 | 7312 | 7813 | 7203 |
| $(p < 20000)$ and $(q < 1000)$ | 23560 | 491 | 456 | 520 |
| $(p < 1000)$ and $(q < 5000)$ | 82432 | 76 | 57.8 | 74.7 |
| $(p < 300)$ and $(q < 20000)$ | 271302 | 32 | 29.6 | 38.9 |
| $(p < 100)$ and $(q < 30000)$ | 327687 | 17 | 15.7 | 18.3 |
| $p = q < 20000$ | 472856 | 1 | 0.37 | 0.32 |

estimates are in good agreement with the numerical results when the number of $LR$ primes is significant.

In Table 3, we give a list of 81 pairs $(p, q)$ of odd primes such that $p < 1000$ and $LR(p, q)$ is prime or probable prime (PRP). The number of decimal digits is ranging from 26 to 250924. The largest known prime value of the tau function is $LR(157, 2207)$, thanks to F. Morain (see Appendix). So far, $LR(41, 28289)$ is the largest known PRP value.

By estimation (27), we expect the existence of infinitely many primes of the form $LR(p, q)$ for each ordinary prime $p$. However, we found no PRP for $p = 13, 19, 23, 31, 37, 43, 53, 61, 67, 71, 73, 83, \ldots$.

*Remark 4* Considering the list $p = 11, 17, 29, 41, 47, 59, 79, 89, 97, \ldots$ for which we know LR (probable) primes, it is remarkable that the six first values correspond exactly to the odd values in the sequence of the Ramanujan primes: 2, 11, 17, 29, 41, 47, 59, 67, 71, 97, .... This sequence was introduced to provide a short proof of Bertrand's postulate [8]. However, we found no significant correlation past the value 59 and do not expect a close mathematical relationship between the tau function and the Ramanujan primes.

Note that the only prime of the form $LR(p, p)$ for $p < 20000$ is $LR(47, 47)$. Our estimation (29) suggests the existence of infinitely many such values.

We give in Table 4 the number of PRP's of the form $LR(p, q)$, for each given odd prime $q < 100$ and all $p < 10^6$, along with the estimates (**) obtained by summing over prime $p$ the expression (25). We partly explain the discrepancy between the actual data and our expectations by considering the compositeness of some $2kq \pm 1$ numbers for small positive integers $k$. For example, if $q = 59$, then those numbers are composite for $k = 1, 2, 4, 5, 8, \ldots$, which in turn implies that $LR(p, 59)$ has no divisor smaller than 353, except possibly $p$ and 59. In this case, we observe that the number of primes is effectively higher than expected.

**Acknowledgements** We are grateful to François Morain for his outstanding contribution to the numerical results. We also would like to thank Marc Hufschmitt and Paul Zimmermann for their helpful discussions, and the anonymous referee for his valuable suggestions.

**Table 3** Known pairs $(p, q)$, $p < 1000$, such that $LR(p, q)$ is prime (P) or probable prime (PRP). ECPP ($\diamond$) method has been used for the primality of two large values

| $p$ | $q$ | Digits | Primality | $p$ | $q$ | Digits | Primality |
|---|---|---|---|---|---|---|---|
| 11 | 317 | 1810 | P | 439 | 29 | 407 | P |
| 17 | 433 | 2924 | P | 449 | 547 | 7965 | PRP |
| 29 | 31 | 242 | P | 461 | 3019 | 44215 | PRP |
| 29 | 83 | 660 | P | 463 | 2753 | 40347 | PRP |
| 29 | 229 | 1834 | P | 487 | 479 | 7066 | PRP |
| 41 | 2297 | 20367 | PRP | 491 | 167 | 2457 | P |
| 41 | 28289 | 250924 | PRP | 503 | 73 | 1070 | P |
| 47 | 5 | 37 | P | 557 | 109 | 1631 | P |
| 47 | 47 | 424 | P | 571 | 1091 | 16526 | PRP |
| 47 | 4177 | 38404 | PRP | 587 | 1093 | 16629 | PRP |
| 59 | 1381 | 13441 | PRP | 607 | 13 | 184 | P |
| 59 | 8971 | 87365 | PRP | 613 | 47 | 706 | P |
| 79 | 1571 | 16386 | PRP | 613 | 1013 | 15515 | PRP |
| 79 | 6317 | 65920 | PRP | 619 | 1297 | 19900 | PRP |
| 89 | 73 | 772 | P | 643 | 953 | 14703 | P $\diamond$ |
| 97 | 331 | 3606 | P | 673 | 1019 | 15834 | PRP |
| 97 | 887 | 9682 | PRP | 677 | 3 | 32 | P |
| 103 | 14939 | 165374 | PRP | 691 | 1523 | 23770 | PRP |
| 109 | 373 | 4169 | PRP | 739 | 2503 | 39475 | PRP |
| 113 | 197 | 2214 | P | 761 | 13 | 190 | P |
| 157 | 2207 | 26643 | P $\diamond$ | 773 | 67 | 1049 | P |
| 173 | 103 | 1256 | P | 787 | 73 | 1147 | P |
| 197 | 5 | 50 | P | 809 | 149 | 2367 | P |
| 199 | 4519 | 57125 | PRP | 811 | 43 | 671 | P |
| 223 | 101 | 1292 | P | 821 | 1163 | 18626 | PRP |
| 223 | 281 | 3617 | P | 829 | 11 | 161 | P |
| 223 | 9431 | 121795 | PRP | 839 | 4177 | 67153 | PRP |
| 227 | 11 | 130 | P | 857 | 683 | 11002 | PRP |
| 239 | 107 | 1387 | P | 857 | 3847 | 62042 | PRP |
| 251 | 3 | 26 | P | 877 | 3617 | 58531 | PRP |
| 251 | 1193 | 15733 | PRP | 881 | 241 | 3888 | PRP |
| 257 | 1699 | 22506 | PRP | 881 | 251 | 4050 | PRP |
| 281 | 19 | 243 | P | 937 | 59 | 949 | P |
| 331 | 2129 | 29492 | PRP | 941 | 349 | 5692 | PRP |
| 349 | 409 | 5706 | PRP | 947 | 41 | 654 | P |
| 353 | 239 | 3335 | P | 953 | 557 | 9111 | PRP |
| 379 | 11 | 142 | P | 971 | 3 | 33 | P |
| 401 | 59 | 831 | P | 971 | 433 | 7098 | PRP |
| 409 | 4423 | 63520 | PRP | 977 | 59 | 954 | P |
| 421 | 89 | 1271 | P | 983 | 3 | 33 | P |
| 421 | 317 | 4561 | PRP | | | | |

**Table 4** For odd primes $q < 100$, actual and expected** number of primes $p < 10^6$ such that $LR(p, q)$ is PRP, and first values of $p$

| $q$ | Actual | Expected** | $p$ |
|---|---|---|---|
| 3 | 838 | 904 | 251, 677, 971, 983, 1229, ... |
| 5 | 910 | 871 | 47, 197, 1123, 2953, 3373, ... |
| 7 | 438 | 444 | 1151, 2141, 5087, 6907, 7129, ... |
| 11 | 663 | 567 | 227, 379, 829, 1217, 1367, ... |
| 13 | 593 | 506 | 607, 761, 1033, 1867, 1999, ... |
| 17 | 438 | 419 | 1301, 1319, 1373, 8363, 9209, ... |
| 19 | 321 | 386 | 281, 4751, 5717, 7103, 10181, ... |
| 23 | 273 | 293 | 1013, 2113, 6577, 6581, 8609, ... |
| 29 | 263 | 283 | 439, 1783, 3109, 3209, 3301, ... |
| 31 | 256 | 269 | 29, 6737, 7757, 8243, 8707, ... |
| 37 | 208 | 235 | 1061, 1217, 1621, 2699, 3167, ... |
| 41 | 214 | 217 | 947, 2671, 4817, 5231, 6079, ... |
| 43 | 242 | 209 | 811, 7549, 8089, 9337, 9923, ... |
| 47 | 232 | 195 | 47, 613, 1361, 2963, 4219, ... |
| 53 | 143 | 178 | 4153, 4457, 6311, 23209, 30211, ... |
| 59 | 232 | 163 | 401, 937, 977, 1609, 3121, ... |
| 61 | 181 | 159 | 1583, 1747, 5209, 7057, 10079, ... |
| 67 | 159 | 148 | 773, 1597, 2969, 3823, 4603, ... |
| 71 | 142 | 141 | 1601, 6469, 10037, 15391, 23371, ... |
| 73 | 144 | 138 | 89, 503, 787, 7687, 12689, ... |
| 79 | 104 | 129 | 21193, 23339, 31847, 38239, 38327, ... |
| 83 | 112 | 124 | 29, 2927, 3391, 7873, 8597, ... |
| 89 | 104 | 117 | 421, 2843, 4637, 4937, 5659, ... |
| 97 | 102 | 110 | 5261, 7537, 11933, 22613, 23627, ... |

## Appendix: Computations

Here we provide a PARI/GP implementation of the *LR* numbers, using a known formula (see, e.g., [4]) along with the recurrence relation (2).

```
LR(p,n)={
  local(j,p11,s10,t,tp,t0,t1,t2,tmax);
  tmax=floor(2*sqrt(p));
  s10=sum(t=1, tmax, (t^10)*qfbhclassno(4*p-t*t));
  tp=(p+1)*(42*p^5-42*p^4-48*p^3-27*p^2-8*p-1)-s10;
  t0=1; t1=tp; p11=p^11;
  for (j=1, n-2, t2=tp*t1-p11*t0; t0=t1; t1=t2);
  if (n==1, t1=1);
  return(t1)
}
```

We took about seven months of numerical investigations for primes of the form $LR(p, q)$, $p$ and $q$ odd primes, using the multiprecision software PARI/GP (version 2.3.5) and PFGW (version 3.4.5) through four stages:

1. Finding small divisors of the form $2kq \pm 1$ with PARI/GP;
2. 3-PRP tests with PFGW;
3. APRCL primality tests for all PRP's up to 3700 decimal digits with PARI/GP;
4. Baillie-PSW PRP tests for all PRP's above 3700 decimal digits with PARI/GP.

Stage 4 leads to a greater probability of primality than stage 2 (there is no known composite number which is passing this test), but takes more time.

We point out that François Morain provides primality certificates for two large *LR* numbers (see diamonds $\diamond$ in Table 3) on his web page. He used his own software fastECPP, implementing a fast algorithm of elliptic curve primality proving [5], on a computer cluster. His calculations required respectively 355 and 2355 days of total CPU time, between January and April 2011. Since $LR(157, 2207)$ has 26643 decimal digits, it appears to be the largest prime certification using a general-purpose algorithm, at the date of submission.

## References


1. Bilu, Y., Hanrot, G., Voutier, P.M.: Existence of primitive divisors of Lucas and Lehmer numbers. J. Reine Angew. Math. **539**, 75–122 (2001)
2. Lehmer, D.H.: The primality of Ramanujan's Tau-function. Am. Math. Mon. **72**, 15–18 (1965)
3. Lucas, E.: Théorie des fonctions numériques simplement périodiques. Am. J. Math. **1**, 184–240 and 289–321 (1878)
4. Lygeros, N., Rozier, O.: A new solution for the equation $\tau(p) \equiv 0 \pmod{p}$. J. Integer Seq. **13**(10.7.4), 1–11 (2010)
5. Morain, F.: Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. Math. Comput. **76**, 493–505 (2007)
6. Murty, M.R., Murty, V.K., Shorey, T.N.: Odd values of the Ramanujan $\tau$-function. Bull. Soc. Math. Fr. **115**, 391–395 (1987)
7. Ramanujan, S.: On certain arithmetical functions. Trans. Camb. Philos. Soc. **22**, 159–184 (1916)
8. Ramanujan, S.: A proof of Bertrand's postulate. J. Indian Math. Soc. **11**, 181–182 (1919)
9. Ribenboim, P.: The New Book of Prime Number Records. Springer, Berlin (1996)
10. Serre, J.-P.: Divisibilité de certaines fonctions arithmétiques. Enseign. Math. **22**, 227–260 (1976)
11. Swinnerton-Dyer, H.P.F.: On $\ell$-adic representations and congruences for coefficients of modular forms. Lect. Notes Math. **350**, 1–55 (1973)
12. Wagstaff, S.S.: Divisors of Mersenne numbers. Math. Comput. **40**, 385–397 (1983)