Publ. Math. Debrecen
56 / 3-4 (2000), 523–534

On the running time of the Adleman–Pomerance–Rumely primality test

By J. PELIKÁN (Budapest), J. PINTZ (Budapest)
and ENDRE SZEMERÉDI (Budapest–New Brunswick)

Dedicated to Kálmán Győry on the occasion of his 60th birthday.

Abstract. In the present work we prove a relatively simple explicit upper bound for a number theoretic function which plays an important role in the running time analysis of the Adleman–Pomerance–Rumely primality test. The same function appears in the investigation of Carmichael's λ-function.

1. Introduction

In the running time analysis of the Adleman–Pomerance–Rumely (APR) Test [APR] the following function $f(n)$ plays a crucial role. Let $f(n)$ denote the least positive square-free integer such that the product of the primes q with $q-1 \mid f(n)$ exceeds $\sqrt{n}$. Similarly, the function $g(n)$ is defined as the least (not necessarily square-free) positive integer such that the product of the primes q with $q-1 \mid g(n)$ exceeds $\sqrt{n}$.

With these definitions, the running time $T(n)$ of the APR-test satisfies

$$\begin{aligned} f(n) &\le T(n), && \text{if } n \text{ is prime} \\ T(n) &\le f(n)^c, && \text{for all } n \end{aligned}$$

with an absolute, positive, explicitly calculable constant c. (This is Theorem 2 of [APR].)

Mathematics Subject Classification: 11A51.
Key words and phrases: primality tests, pseudoprimes, Carmichael's λ-function.

About the functions $g(n)$, $f(n)$, the following result, (Theorem 3) is proved in [APR]:

$$(\log n)^{c_1 \log_3 n} \leq g(n) \leq f(n) < (\log n)^{c_2 \log_3 n}$$

where c_1 and c_2 are explicitly calculable positive absolute constants. $\log_\nu$ denotes the ν-fold iterated logarithmic function. They also remark that a slightly more careful treatment leads

$$c_1 = \frac{1}{\log 2} + o(1). \tag{1.2}$$

Further they express in Remark 2 the

Conjecture. $c_2 = \frac{1}{\log 2} + o(1)$.

Concerning the actual value of c_2 provided by the work [APR], no calculations are given in [APR], but, the value would be very large due to the application of a deep result of Gallagher. The object of the present work is to show that c_2 can be chosen as small as $c_2 = 2.302$.

For the sake of completeness, we also include the standard proof of (1.2) (cf. Theorem 1 of [EPS]). The upper bound with $c_2 = 2.302$ also implies the simple upper bound

$$f(n) < 10^{\log_2 n \log_3 n} \quad \text{for } n > n_0 \text{ explicit constant.} \tag{1.3}$$

It would be very elaborate to give a good explicit value for n_0.

We will prove the following

Theorem. *There is a positive, absolute, calculable constant* c_0 ($c_0 = 2.3013598\dots$) *such that for any* $\varepsilon > 0$ *and* $n > n_0(\varepsilon)$ *we have*

$$(\log n)^{\left(\frac{1}{\log 2} - \varepsilon\right) \log_3 n} < g(n) \leq f(n) < (\log n)^{(c_0 + \varepsilon) \log_3 n}. \tag{1.4}$$

The exact definition of c_0 *is given in the Remark following the Main Lemma in Section 4. (cf.* (4.2)–(4.4)).

The authors are grateful to one of the referees who pointed out that the result of the present paper can be applied to Carmichael's λ-function. We formulate here the result which makes explicit the constant in the exponent in Theorem 1 of Erdős, Pomerance and Schmutz [EPS]. The only modification in their argument is that we need to replace the constant 2 in the definition of x_i (in the exponent) by $1 + o(1)$. Our Theorem or Main Lemma (cf. Section 4) implies then easily the following

Corollary. *Let $\lambda(n)$ denote Carmichael's λ-function. There exists a sequence $n_i \to \infty$ such that*

$$\lambda(n_i) < (\log n_i)^{(2c_0+o(1))\log_3 n_i} < (100)^{\log_2 n_i \log_3 n_i}$$

where $c_0 = 2.302$. (For the exact value of c_0 see the definition (4.2)–(4.4) *in Section 4.)*

The proof of our Theorem, similarly to that of [APR] follows the arguments of Prachar [P], who was the first to prove a result of such type. (For more details see the works [APR] and [P].) The improvement in [APR] compared to [P] was due to the idea of Odlyzko to use Gallagher's prime number theorem [G] instead of a theorem of Tatuzawa. Our relatively good explicit value of c_0 comes from the idea of using a statistical theorem about the distribution of primes in arithmetic progressions mod k (Theorem A) which requires more (although a bounded number of) exceptional moduli than Gallagher's prime number theorem [G], but allows much better dependence of the moduli k on x ($k < x^{5/12-\varepsilon}$) than Gallagher's theorem ($k < x^{\delta}$, δ small absolute constant, theoretically effective). Such kind of results may be derived in this strong form from the density theorem of Huxley [Hu] about the distribution of zeros of Dirichlet L-functions. Similar but weaker results were proved first by Rényi and later by Barban. A result anologous to Theorem A with the weaker exponent $1/3$ in place of $5/12$ was proved by P.D.T.A. Elliott [E]. For the present form of Theorem A we refer the reader for [AGP, Theorem 2.1].

Although the structure of the proof [APR] remains unchanged several significant modifications are introduced to get a possibly small value of c_0.

2. The lower estimate

As mentioned in Remark 6.3 of [APR], it is quite standard to show the lower estimate in (1.4). Using the well-known inequality [W]

$$d(k) \le 2^{(1+o(1))\log k/\log_2 k} \tag{2.1}$$

we have (cf. the proof of Theorem 1 in [EPS])

$$
\begin{aligned}
(2.2)\qquad \prod_{q-1|k} q &\le \prod_{d|k}(d+1) \le \prod_{d|k}(2d) = (2k^{1/2})^{d(k)}\\
&\le \exp\left\{\left(\log 2 + \frac{1}{2}\log k\right) 2^{(1+o(1))\frac{\log k}{\log_2 k}}\right\}\\
&= \exp\left\{2^{(1+o(1))\frac{\log k}{\log_2 k}}\right\} < \exp\left(\frac{\log n}{2}\right) = \sqrt{n}
\end{aligned}
$$

if

$$
(2.3)\qquad \frac{\log 2\cdot\log k}{\log_2 k}(1+o(1)) < \log_2 n - \log 2.
$$

Now, (2.3) and so (2.2) certainly holds if

$$
(2.4)\qquad \log k \le \frac{(1-\varepsilon)}{\log 2}\cdot\log_2 n\log_3 n \iff k \le (\log n)^{\frac{1-\varepsilon}{\log 2}\log_3 n}
$$

This calculation proves that

$$
(2.5)\qquad g(n) > (\log n)^{\frac{1-\varepsilon}{\log 2}\log_3 n}.
$$

3. Statistical theorems for primes in arithmetic progressions

Our basic tool is the following statistical theorem about the distribution of primes in arithmetic progressions, mentioned at the end of the Introduction.

Theorem A. *For every $\varepsilon > 0$ there are calculable positive numbers $x_0(\varepsilon)$ and $c(\varepsilon)$ such that if $x \ge x_0(\varepsilon)$ and k, a are co-prime integers with $k < x^{5/12-\varepsilon}$ then*

$$
(3.1)\qquad \left|\sum_{p\equiv a(k);\, p\le x}\log p - \frac{x}{\varphi(k)}\right| < \frac{\varepsilon x}{\varphi(k)}
$$

except possibly for those k which are divisible by at least one $k_\nu(x)$ where $k_\nu(x)$ are certain integers with $k_\nu(x) > \log x$, $\nu = 1, 2, \dots c(\varepsilon)$.

Let

$$\begin{aligned}\Theta(x,k,a) &= \sum_{p\equiv a(k);\, p\le x} \log p,\\ \Theta_0(x,k,a) &= \sum_{p\equiv a(k);\, p\le x} \mu^2(p-1)\log p\end{aligned} \tag{3.2}$$

where μ denotes the Möbius function. This means that in Θ_0 we count only those primes p where $p-1$ is square-free. Let

$$\alpha = \prod_p \left(1-\frac{1}{p^2-p}\right) = 0.3740\dots .$$

Let $\psi(k)$ denote the multiplicative function whose value at the prime power p^d is $1-1/(p^2-p)$. We have clearly $\alpha \le \psi(k) < 1$ for all k.

Theorem A implies the following

Theorem B. *For every $\varepsilon > 0$ there are calculable positive numbers $x_1(\varepsilon)$ and $c(\varepsilon)$ such that if $x \ge x_1(\varepsilon)$, and $k < x^{5/12-\varepsilon}$ is square-free, then*

$$\left|\Theta_0(x,k,1) - \frac{\alpha x}{\psi(k)k}\right| < \varepsilon\frac{x}{k}\prod_{p\mid k}\left(1+\frac{2}{p-1}\right) \tag{3.3}$$

except possibly for those k for which k^2 is a multiple of at least one $k'_\nu(x)$ where $k'_\nu(x)$ are certain integers with $k'_\nu(x) > (\log x)^{3/4}$, $\nu = 1,2,\dots c(\varepsilon)$.

Proof. Let us write every square-free natural number m in the form $m = ab$, where $a \mid k$, $(b,k)=1$. By the inclusion-exclusion principle we have ($\sum'$ denotes summation over square-free numbers)

$$\begin{aligned}\Theta_0(x,k,1) &= {\sum_m}' (-1)^{\omega(m)}\Theta(x,[k,m^2],1)\\ &= {\sum_{a\mid k}}'(-1)^{\omega(a)} {\sum_{(b,k)=1}}' (-1)^{\omega(b)}\Theta(x,kab^2,1),\end{aligned} \tag{3.4}$$

where $\omega(n)$ denotes the number of distinct prime factors of n. Let $T = \left[\frac{1}{\varepsilon}\right]$ and let $M(T)$ denote the right side of (3.4) where we consider only square-free numbers b having all prime factors below T. Denoting $Q = \prod_{p\nmid k;\, p<T} p$,

we have

$$M(T) = \sum_{a|k}{}' (-1)^{\omega(a)} \sum_{b|Q} (-1)^{\omega(b)} \Theta(x, kab^2, 1). \tag{3.5}$$

Further, we have

$$\begin{aligned} |\Theta_0(x,k,1) - M(T)| &\le \sum_{a|k}{}' \sum_{b\ge T} \Theta(x, kab^2, 1) \\ \le \sum_{a|k}{}' \Big\{ \sum_{T<b\le x^{1/20}} \frac{c_3 x}{\varphi(k) a \varphi(b^2)} &+ \sum_{x^{1/2}>b>x^{1/20}} \log x \left(1 + \frac{x}{akb^2}\right) \Big\} \\ &\le \frac{c_4 x}{\varphi(k) T} \sum_{a|k} \frac{1}{a} = \frac{c_4 x}{kT} \prod_{p|k} \left(1 + \frac{2}{p-1}\right) \end{aligned} \tag{3.6}$$

by $\sum_{n>u} 1/\varphi(n^2) < c_5/u$ and the Brun–Titchmarsh inequality

$$\Theta(x, d, a) \le \frac{c_6 x}{\varphi(d)} \frac{\log x}{\log(x/d)}. \tag{3.7}$$

Choosing $k'_\nu = \frac{k_\nu}{(k_\nu, Q^2)}$ where k_ν are the exceptional moduli of Theorem A we can assure $k_\nu \nmid kab^2$ for $b \mid Q$, since our condition $k'_\nu \nmid k^2$ implies $k_\nu \nmid k^2Q^2$. Therefore we can apply our Theorem A for the quantities $\Theta(x, kab^2, 1)$ in (3.5). So we obtain

$$\begin{aligned} &\left| M(T) - \sum_{a|k}{}' (-1)^{\omega(a)} \sum_{b|Q}{}' (-1)^{\omega(b)} \frac{x}{\varphi(k) a \varphi(b^2)} \right| \\ &\le \varepsilon \frac{x}{\varphi(k)} \sum_{a|k}{}' \frac{1}{a} \sum_{b|Q}{}' \frac{1}{\varphi(b^2)} \le \frac{c_7 \varepsilon x}{k} \prod_{p|k} \left(1 + \frac{2}{p-1}\right). \end{aligned} \tag{3.8}$$

Further we have

$$\left| \sum_{b|Q}{}' \frac{(-1)^{\omega(b)}}{\varphi(b^2)} - \sum_{b=1;\,(b,k)=1}^{\infty}{}' \frac{(-1)^{\omega(b)}}{\varphi(b^2)} \right| \le \sum_{b\ge T}{}' \frac{1}{\varphi(b^2)} < \frac{c_5}{T}. \tag{3.9}$$

Collecting (3.5), 3.6), (3.8) and (3.9) we finally get

$$\begin{aligned}(3.10)\qquad \left|\Theta_0(x,k,1) - \frac{x}{\varphi(k)}\prod_{p|k}\left(1-\frac{1}{p}\right)\prod_{p\nmid k}\left(1-\frac{1}{p^2-p}\right)\right| \\ < \frac{c_8\varepsilon x}{k}\prod_{p|k}\left(1+\frac{2}{p-1}\right)\end{aligned}$$

which proves Theorem B. □

4. The Main Lemma

Using Theorem B we shall prove now a lemma (an improved version of Proposition 10 of [APR] from which the final result will easily follow.)

Main Lemma. *There is a positive, absolute, calculable constant* c_0 ($c_0 = 2.3013598\ldots$) *such that for all* $x > 10$ *there is a square-free number* $M < x$ *with*

$$(4.1)\qquad \sum_{p-1|M;\ p\,\mathrm{prime}} 1 > e^{(1+o(1))\log x/c_0 \log_2 x}.$$

Remark. Let a denote the unique number $a \in \left(0, \frac{5}{12}\right)$ which satisfies the equality

$$(4.2)\qquad z(a) = \frac{12}{5}\log\left(1-\frac{12a}{5}\right) - \frac{7}{5}\log\left(1-\frac{7}{5}a\right) - \log a = 1.$$

(Since $\lim_{a\to 0} z(a) = +\infty$, $\lim_{a\to\frac{5}{12}-0} z(a) = -\infty$, and

$$z'(a) = \frac{-\left(\frac{12}{5}\right)^2}{1-\frac{12a}{5}} + \frac{\left(\frac{7}{5}\right)^2}{1-\frac{7}{5}a} - \frac{1}{a} < \frac{-\left(\frac{12}{5}\right)^2}{1-\frac{7}{5}a} + \frac{\left(\frac{7}{5}\right)^2}{1-\frac{7}{5}a} < 0,$$

there is really exactly one solution of (4.2).) Defining

$$\begin{aligned}(4.3)\qquad y(a) = \left(1-\frac{7}{5}a\right)\log\left(1-\frac{7}{5}a\right) \\ - \left(1-\frac{12a}{5}\right)\log\left(1-\frac{12a}{5}\right) - a\log a\end{aligned}$$

we will see later that c_0 can be chosen as

$$c_0 = 1/y(a). \tag{4.4}$$

Proof of the Main Lemma. We will actually show the Main Lemma with the estimate $M < x^{1+\varepsilon+o(1)}$ which is clearly equivalent with the original formulation due to the appearance of the factor $1+o(1)$ in (4.1), since ε is an arbitrary positive number here. Let us define with the choice of a in (4.2) ($a = 0.237218\dots$), q running through the primes

$$\begin{gathered} u = \left(1 - \frac{7}{5}a\right)\log x, \quad R = \pi(u) - \pi\left(\frac{u}{\log u}\right), \\ v = \frac{R}{1-\frac{7}{5}a}, \qquad k = \prod_{\frac{u}{\log u} < q < u} q, \qquad E = x^{\frac{12}{5}a(1+\varepsilon)}, \end{gathered} \tag{4.5}$$

where $\varepsilon > 0$ is arbitrary. With these choices we have (using the prime number theorem) clearly

$$\begin{gathered} k = e^{u(1+o(1))} = x^{\left(1-\frac{7}{5}a\right)(1+o(1))}, \quad R = \frac{(1+o(1))u}{\log u}, \\ v = \frac{1+o(1))\log x}{\log_2 x}. \end{gathered} \tag{4.6}$$

We define $\mathcal{D}$ as follows,

$$\mathcal{D} = \{d;\ d \mid k,\ \omega(d) = [av]\},\ |\mathcal{D}| = D,\ B = \min_{d\in\mathcal{D}} d,\ F = \max_{d\in\mathcal{D}} d. \tag{4.7}$$

Let A denote the number of solutions of

$$m(p-1) \equiv 0 \pmod{k} \tag{4.8}$$

where $m \le \frac{k}{B}$, $p \le E$ is prime with $p-1$ square-free. For each $d \in \mathcal{D}$ let A_d denote the number of solutions of (4.8) with $d \mid p-1$, $(m,k) = k/d$.

First we note that for every $d \in \mathcal{D}$ we have

$$1 \le \prod_{p\mid d}\left(1 + \frac{2}{p-1}\right) \le \exp\left\{c_9 \sum_{u/\log u < p \le u} \frac{1}{p}\right\} = 1 + o(1) \tag{4.9}$$

and

$$\begin{aligned}(4.10)\qquad 1 \geq \psi(d) &= \prod_{p|d}\left(1-\frac{1}{p^2-p}\right)\\ &\geq \exp\left(-c_{10}\sum_{u/\log u<p\leq u}\frac{1}{p^2}\right) = 1+o(1).\end{aligned}$$

Therefore if d^2 is not divisible by any of $k_\nu = k'_\nu(E)$ then in view of

$$\begin{aligned}(4.11)\qquad F \leq u^{av} &= \exp\left(aR\log u\Big/\left(1-\frac{7}{5}a\right)\right)\\ &= \exp\left\{a(1+o(1))u\Big/\left(1-\frac{7}{5}a\right)\right\} = x^{a+o(1)}\end{aligned}$$

we have by Theorem B

$$\begin{aligned}(4.12)\qquad \Pi_0(E,d,1) &\overset{\text{def}}{=} \sum_{p<E;\, p\equiv 1(d)}\mu^2(p-1) \geq \frac{\Theta_0(E,d,1)}{\log E}\\ &\geq \left(\frac{\alpha}{\psi(d)}-2\varepsilon\right)\frac{E}{d\log E} > \frac{c_{11}E}{du}.\end{aligned}$$

Further, we have for any $Y \geq 1$

$$(4.13)\qquad Y \geq \sum_{n<Y;\,(n,k)=1} 1 \geq Y - \sum_{\frac{u}{\log u}<p\leq u}\frac{Y}{p} \geq Y(1+o(1)).$$

Therefore the number of $m \leq \frac{k}{B}$, $(m,k) = k/d$ is at least

$$(4.14)\qquad c_{12}\cdot\frac{k}{B}\cdot\frac{d}{k} = c_{12}\frac{d}{B}.$$

Thus, if $d \in \mathcal{D}$, $k'_\nu \nmid d^2$ $(\nu = 1, \dots c(\varepsilon))$ then

$$(4.15)\qquad A_d > c_{11}\frac{E}{du}\cdot c_{12}\frac{d}{B} = c_{13}\frac{E}{uB}.$$

Let us define now

$$\mathcal{D}^* = \{d; d \in \mathcal{D},\ k'_\nu(E) \nmid d^2 (\forall \nu = 1 \dots c(\varepsilon))\},\ |\mathcal{D}^*| = D^*. \tag{4.16}$$

Now, choosing for every k'_ν ($\nu = 1, 2, \dots c(\varepsilon)$) one prime-factor $q_\nu \mid k'_\nu$ with $q_\nu \in (u/\log u, u]$ (if there is any) we obtain

$$D^* \geq \binom{R - c(\varepsilon)}{[av]} = \binom{\left(1 - \frac{7}{5}a\right) v - c(\varepsilon)}{[av]} \tag{4.17}$$

and using Stirling's formula we get by (4.3)

$$\begin{aligned}(1 + o(1)) \log D^* \geq v \Bigg\{ \left(1 - \frac{7}{5}a\right) \log \left(1 - \frac{7}{5}a\right) \\ - \left(1 - \frac{12}{5}a\right) \log \left(1 - \frac{12}{5}a\right) - a \log a \Bigg\} = vy(a) = v/c_0.\end{aligned} \tag{4.18}$$

Now (4.15) and (4.18) together give

$$A \geq \sum_{d \in \mathcal{D}^*} A_d \geq c_{13} \frac{E}{uB} e^{(1+o(1))v/c_0}. \tag{4.19}$$

Clearly the number of integers $n \leq kE/B$ divisible by k is at most E/B, and all solutions of (4.8) are of this form. Thus there exists some $n_0 \leq kE/B$, $k \mid n_0$ which has at least

$$\frac{A}{E/B} \geq c_{13} u^{-1} e^{(1+o(1))v/c_0} = e^{(1+o(1)) \frac{\log x}{c_0 \log_2 x}} \tag{4.20}$$

representations as $m(p-1)$. If M denotes the largest square-free divisor of n_0, then M clearly satisfies (4.1), further similarly to (4.11)

$$B \geq u^{(1+o(1))av} \geq x^{a+o(1)} \tag{4.21}$$

and so, by (4.5), (4.6)

$$M \leq n_0 \frac{kE}{B} = x^{1+\varepsilon+o(1)} \tag{4.22}$$

which proves the Main Lemma. □

5. Proof of the theorem

It is now very easy to finish the proof of the Theorem. Let us choose with the $\varepsilon > 0$ stated in the Theorem

$$x = (\log n)^{(1+\varepsilon)c_0 \log_3 n} = \exp\{(1+\varepsilon)c_0 \log_2 n \log_3 n\}. \tag{5.1}$$

Then the main lemma implies the existence of a square-free $M \le x$ with

$$\begin{aligned} h(M) = \sum_{p-1|M;\ p\,\mathrm{prime}} 1 &> \exp\left(\frac{(1+o(1))\log x}{c_0 \log_2 x}\right) \\ &= \exp\left(\frac{(1+o(1))(1+\varepsilon)c_0 \log_2 n \log_3 n}{c_0(1+o(1))\log_3 n}\right) > \log n \end{aligned} \tag{5.2}$$

and therefore

$$\prod_{p-1|M} p \ge 2^{h(M)} > 2^{\log n} > \sqrt{n}. \tag{5.3}$$

This immediately gives

$$f(n) \le M \le x = (\log n)^{(1+\varepsilon)c_0 \log_3 n} \tag{5.4}$$

and thus proves our Theorem.

References

[APR] L. M. Adleman, C. Pomerance and R. S. Rumely, On distinguishing prime numbers from composite numbers, *Ann. Math.* **117** (1983), 173–206.

[AGP] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.* (2) **139** no. 3 (1994), 703–722.

[E] P. D. T. A. Elliott, On the size of $L(1,\chi)$, *J. Reine Angew. Math.* **236** (1969), 26–36.

[EPS] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arith.* **58** (1991), 363–385.

[G] P. X. Gallagher, A large sieve density estimate near $\sigma = 1$, *Invent. Math.* **11** (1970), 329–339.

[HU] M. N. Huxley, Large values of Dirichlet polynomials, *Acta Arith.* **26** (1975), 435–444.

[P] K. Prachar, Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben, *Monatsh. Math.* **59** (1955), 91–97.

[W] S. Wigert, Sur l'orde de grandeur du nombre des diviseurs d'un entier, *Arkiw fur Math. Astr. Fys.* **3** no. 18 (1907), 1–9.

J. PELIKÁN
EÖTVÖS UNIVERSITY
BUDAPEST
HUNGARY

J. PINTZ
MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST
HUNGARY

ENDRE SZEMERÉDI
COMPUTER SCIENCE DEPARTMENT
RUTGERS UNIVERSITY
NEW BRUNSWICK, NJ 08903
USA
MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST
HUNGARY

(Received September 24, 1999; revised May 3, 2000)