MATHEMATICS OF COMPUTATION
Volume 65, Number 213
January 1996, Pages 361–372

SOME RESULTS ON PSEUDOSQUARES

R. F. LUKES, C. D. PATTERSON, AND H. C. WILLIAMS

ABSTRACT. If p is an odd prime, the pseudosquare L_p is defined to be the least positive nonsquare integer such that $L_p \equiv 1 \pmod 8$ and the Legendre symbol $(L_p/q) = 1$ for all odd primes $q \leq p$. In this paper we first discuss the connection between pseudosquares and primality testing. We then describe a new numerical sieving device which was used to extend the table of known pseudosquares up to L_{271}. We also present several numerical results concerning the growth rate of the pseudosquares, results which so far confirm that $L_p > e\sqrt{p/2}$, an inequality that must hold under the extended Riemann Hypothesis.

1. INTRODUCTION

Let p be an odd prime. The *pseudosquare* L_p is defined in the following fashion:

(i) $L_p \equiv 1 \pmod 8$,
(ii) the Legendre symbol $(L_p/q) = 1$ for all odd primes $q \leq p$,
(iii) L_p is the least positive nonsquare integer satisfying (i) and (ii).

Thus, the pseudosquare L_p behaves locally like a perfect square modulo all primes $\leq p$, but is nevertheless not a perfect square. Hall [10] has shown that the values of L_p must be unbounded as p increases.

Kraitchik [11, pp. 41–46] seems to have been the first to consider these numbers, and in [11] provides a table of them up to L_{47}. Since then various authors, most notably D. H. Lehmer, who gave the pseudosquares their name (see Lehmer [16]), have extended Kraitchik's list up to L_{223} (Stephens and Williams [22]). Notice that the values of L_p seem to grow very rapidly with respect to p.

The growth rate of pseudosquares is of great importance in two problems in computational number theory: square recognition and primality testing. Cobham [8] has shown that if a number is not a perfect square, then under the Extended Riemann Hypothesis (ERH) it must fail to be a square modulo a small prime p. Thus, we expect that the pseudosquares should grow quickly. Incidentally, this problem of perfect power recognition, which can be of importance in primality testing and factoring, has been discussed more recently by Bach and Sorenson [5]. Also, as shown in Section 2, if pseudosquare growth is sufficiently rapid, then there exists a deterministic polynomial-time (in $\log N$) algorithm for determining the prime character of N. At the moment the best unconditional results on the primality testing problem are those of Adleman, Pomerance, and Rumely [1], who show that the problem can be solved for a given N by a deterministic algorithm of

Received by the editor August 23, 1993 and, in revised form, April 8, 1994.
1991 *Mathematics Subject Classification.* Primary 11A51, 11Y11, 11-04, 11Y55.
Research of the third author supported by NSERC of Canada grant #A7649.

time complexity $O((\log N)^{c \log\log\log N})$, and of Adleman and Huang [2], who show that there is a probabilistic polynomial-time algorithm for solving this problem. However, both of these algorithms are very complicated and difficult to implement, whereas the (conditional) algorithms provided in Section 2 are very simple. We should also mention here that Bach and Huelsbergen [4] have used the table of pseudosquares in [22] to support their heuristic argument that $G(n)$, the smallest value of x such that the primes $\leq x$ generate the multiplicative group modulo n, is asymptotically $\leq (\log 2)^{-1} \log n \log\log n$.

Because of the importance of the question of pseudosquare growth rate, it would be very helpful if the table in [22] could be extended. Unfortunately, this is very difficult to do simply because the pseudosquares do seem to grow very quickly. The purpose of this paper is first to discuss the connection between pseudosquares and primality testing and then to describe briefly a new sieving device, called MSSU, which has enabled us to extend the table in [22] from L_{223} up to L_{271}. Finally, we present several numerical results concerning the growth rate of the known pseudosquares. These results, thus far, confirm that $L_p > e^{\sqrt{p/2}}$, a result which must hold under the ERH. Indeed, they seem to support a belief that the pseudosquares grow much more rapidly than this.

2. Pseudosquares and primality testing

Throughout this section we will use the symbol N to denote an odd, positive integer. If p is an an odd prime, we say that $(-1)^{(p-1)/2}p$ is an apparent[1] (quadratic) residue of N when $(N/p) = 1$; we say that $(-1)^{(p-1)/2}p$ is an apparent nonresidue of N when $(N/p) = -1$. Furthermore, if the Jacobi symbol $(-1/N) = 1(-1)$, then -1 is said to be an apparent residue (nonresidue) of N; also, the apparent character of 2 and -2 can be defined in a similar fashion through the values of the Jacobi symbols $(2/N)$ and $(-2/N)$. Note that by the law of quadratic reciprocity, we see that if N is a prime, then any apparent residue of N is in fact a quadratic residue of N, and any apparent nonresidue of N is a nonresidue of N.

In response to a nonrigorous method of primality testing advocated by Kraitchik [12] (for a discussion of this test see Lehmer [15], Beeger [6], Kraitchik [13]), Hall [10] produced a mathematically correct version of Kraitchik's idea. This is provided in

Theorem 2.1. *If all the factors (not necessarily prime factors) of N are below L_p and if $\{-1, 2, -3, \ldots, (-1)^{(p-1)/2}p\}$ can be divided into two classes $A = \{a_1, a_2, \ldots, a_r\}$, the apparent residues of N, and $B = \{b_1, b_2, \ldots, b_n\}$, the apparent nonresidues of N, such that every a_i is also a quadratic residue of N and every $b_i b_j$ is a quadratic residue of N, then N is a prime or a power of a prime.* □

Notice that this is a primality test that involves the pseudosquares. Furthermore, Beeger [7] actually used this test to prove that a certain 13 digit factor of $12^{45} + 1$ is a prime. The main difficulty in utilizing Hall's test is the problem of determining whether a given integer m is a quadratic residue of N. This was usually done by rather tedious hit-or-miss methods which attempted to express certain multiples of N in the form $x^2 - mky^2$.

This latter problem was avoided in a test by Selfridge and Weinberger (the S-W test) presented in [23]. In order to discuss this test, we must first define the numbers

[1]This is Hall's [10] translation of Kraitchik's [12] "résidu éventuel".

that we will denote by M_p, where p is any prime. These must satisfy the following two properties:

(i) the Jacobi symbol $(q/M_p) = 1$ for all primes q such that $2 \le q \le p$,
(ii) M_p is the least positive nonsquare integer satisfying (i).

The S-W test can now be given as

Theorem 2.2. *If*

(1) *all prime factors of N must exceed B,*
(2) $N/B \le M_p$,
(3) $p_i^{(N-1)/2} \equiv \pm 1 \pmod N$ *for all primes p_i such that $2 \le p_i \le p$,*
(4) $p_j^{(N-1)/2} \equiv -1 \pmod N$ *for some prime p_j such that $2 \le p_j \le p$,*

then N is a prime or the power of a prime. □

A randomized version of this test was given by Lehmann [14]. Of course, this would be a most useful test of primality if it could be shown that M_p grows very quickly as a function of p. At the moment this seems very far from being achieved. We can, however, appeal to a result of Bach [3]:

Theorem 2.3. *Let G be a nontrivial subgroup of $\mathbf{Z}/(m)^*$ such that $n \in G$ for all $0 < n < x$. Then if the* ERH *holds, we must have*

$$x < 2(\log m)^2. \qquad \square$$

Consider the subgroup G of $\mathbf{Z}/(M_p)^*$ which is made up of all k such that $(k/M_p) = 1$. Since M_p is not a perfect square, there must be some odd prime q such that $q^a \| M_p$ and a is odd. Let t be a quadratic nonresidue of q and put $r \equiv t \pmod{q^a}$, $r \equiv 1 \pmod{M_p/q^a}$. Clearly, $r \in \mathbf{Z}/(M_p)^*$ and $(r/M_p) = -1$; thus, G is a nontrivial subgroup of $\mathbf{Z}/(M_p)$. Also, for all $0 < n < p$, we get $n \in G$; hence,

$$p < 2(\log M_p)^2,$$

or

$$M_p > e^{\sqrt{p/2}}. \tag{2.1}$$

Notice that if $N < M_p$, there must, by definition of M_p, exist some prime q such that $2 \le q \le p$ and $(q/N) \ne 1$. If N is a prime, then either $(q/N) = -1$ and $q^{(N-1)/2} \equiv -1 \pmod N$ or $q = N$. If $q = N$, there must be some prime $r < q$ such that $(r/q) = -1$; hence $r^{(N-1)/2} \equiv -1 \pmod N$. It follows that if $B = 1$, and N is a prime $< M_p$, then the conditions (3) and (4) of the S-W test must be satisfied. Thus, by (2.1), the S-W test is a deterministic polynomial-time prime test for N when $B = 1$.

As a proof of this result is provided in [23], we will only sketch the main ideas in it as a sequence of lemmas. We will then use these lemmas to provide a proof of Theorem 2.7, the proof of Theorem 2.2, the S-W test, being similar.

Lemma 2.4. *Let $2^s \| N - 1$ $(s \ge 1)$ and suppose that there exists some $c \in \mathbf{Z}$ such that*

$$c^{(N-1)/2} \equiv -1 \pmod N.$$

If q is a prime divisor of N, then $2^s | q - 1$. □

Lemma 2.5. *Let $2^s \| N-1$ $(s \geq 1)$ and suppose that there exists some $c \in \mathbf{Z}$ such that*

$$c^{(N-1)/2} \equiv \pm 1 \pmod{N}.$$

If $(c/q) \neq 1$ for some prime factor q of N such that $q \equiv 1 \pmod{2^s}$, then $2^s \| q-1$. □

Lemma 2.6. *If $2^s \| N-1$ $(s \geq 1)$, $2^s \| q_1 - 1$, $2^s \| q_2 - 1$, where q_1, q_2 are primes and c is some integer such that $(c/q_1 q_2) \neq 1$, then*

$$c^{(N-1)/2} \not\equiv \pm 1 \pmod{q_1 q_2}. \qquad \square$$

We combine the ideas of the Hall test and the S-W test to obtain

Theorem 2.7. *If*

(1) *all prime divisors of N exceed B,*
(2) *$N/B < L_p$ for some prime p,*
(3) *$p_i^{(N-1)/2} \equiv \pm 1 \pmod{N}$ for all primes p_i such that $2 \leq p_i \leq p$,*
(4) *$2^{(N-1)/2} \equiv -1 \pmod{N}$ when $N \equiv 5 \pmod{8}$,*
$p_j^{(N-1)/2} \equiv -1 \pmod{N}$ for some odd $p_j \leq p$ when $N \equiv 1 \pmod{8}$,

then N is a prime or prime power.

Proof. Assume that N is not a prime or prime power. If $N \equiv -1 \pmod{4}$, then $(-1)^{(N-1)/2} \equiv -1 \pmod{4}$. If $N \not\equiv -1 \pmod{4}$, then by condition (4) there must be some $c \in \mathbf{Z}$ such that

$$c^{(N-1)/2} \equiv -1 \pmod{N}.$$

It follows that if $2^s \| N-1$, then $q \equiv 1 \pmod{2^s}$ for all primes $q \mid N$. If $q \mid N$, we must have $q < N/B$; thus, if $q \equiv 1 \pmod{8}$, there must exist some p_k such that $(p_k/q) = (q/p_k) \neq 1$. If $q \equiv 5 \pmod{8}$, then $(2/q) = -1$, and if $q \equiv -1 \pmod{4}$, then $(-1/q) = -1$; thus, by Lemma 2.5 and condition (3), we find that

$$N = 1 + 2^s t = \prod_{i=1}^{k} q_i,$$

where $q_i = 1 + 2^s t_i$, $2 \nmid t_i$ and q_i is a prime for $i = 1, 2, \ldots, k$. Since t is odd, we must have k odd; hence, $k \geq 3$. Since N is not a prime power, there must be at least two distinct primes q_1, q_2 such that $q_1 q_2 \mid N$ and $q_1 q_2 < N/B$. If $q_1 q_2 \equiv 1 \pmod{8}$, there must exist some prime p_k such that $(p_k/q_1 q_2) = (q_1 q_2/p_k) \neq 1$; if $q_1 q_2 \equiv 5 \pmod{8}$, then $(2/q_1 q_2) = -1$, and if $q_1 q_2 \equiv -1 \pmod{4}$, then $(-1/q_1 q_2) = -1$. By condition (3) and Lemma 2.6 we get a contradiction. □

Also note that condition (3) of Theorem 2.7 must hold if N is a prime. Also, if $N \equiv 5 \pmod{8}$, then $2^{(N-1)/2} \equiv -1 \pmod{N}$ when N is a prime, and if $N \equiv 1 \pmod{8}$, we see by the same reasoning as used earlier that $(p_k/N) = -1$ for some odd $p_k \leq p$ when N is a prime. Thus, if $B = 1$, and $N < L_p$, the conditions (3) and (4) must hold.

Define negative pseudosquares (see Lehmer, Lehmer and Shanks [18]) N_p for odd primes p by:

(i) $N_p \equiv -1 \pmod{8}$,
(ii) $(-N_p/p_i) = 1$ for all odd primes p_i such that $2 < p_i \leq p$,
(iii) N_p is the least positive integer satisfying (i) and (ii).

Recently, the table of N_p given in [22] has been extended by Bronson and Buell [9] from N_{211} to N_{227}.

By quadratic reciprocity it follows that

$$(p_i/L_p) = (p_i/N_p) = 1$$

for all primes p_i such that $2 \leq p_i \leq p$; thus it is easy to see that

$$M_p = \min\{L_p, N_p\}. \tag{2.2}$$

It is possible, then, for the test of Theorem 2.7 to be slightly better than the S-W test, in that L_p seems often to exceed N_p. Also, as long as we have a table of values of L_p, the test of Theorem 2.7 can certainly be used as a primality test which is very easy to implement on even a pocket calculator. As long as the numbers to be tested are not very large ($< 10^{26}$ or thereabouts), it should work reasonably well.

By our previous remarks we can see that if the growth rate of the pseudosquares is sufficiently rapid, then primality testing of N could be achieved in deterministic polynomial time. By (2.2) and (2.1), this is certainly the case under the ERH, but it might be possible to show that a result like

$$L_p > e^{\sqrt{p/2}} \tag{2.3}$$

holds without appealing to the ERH. Thus, it is of some interest to examine, at least empirically, the growth rate of L_p.

3. The MSSU

The real difficulty in the test given in Theorem 2.7 is the problem of computing the values of L_p. The best method currently known is still the sieving technique that Lehmer [17] so vigorously advocated.

Let $m_1, m_2, m_3, \ldots, m_k$ be k positive integers which are relatively prime in pairs. To each m_i there corresponds a set $R_i = \{r_{i1}, r_{i2}, \ldots, r_{in_i}\}$ of n_i *admissible* residues. Given $A, B \in \mathbf{Z}$ $(A < B)$, the general sieving problem is that of determining those values of x such that $A \leq x \leq B$ and $x \pmod{m_i} \in R_i$ $(i = 1, 2, \ldots, k)$. Such problems can be attacked by the use of special purpose devices called number sieves. It is not our purpose here to discuss such mechanisms in detail; for more information concerning the history and development of these machines, the reader is referred to [22] and Patterson [20]. Suffice it to say that a number sieve achieves its speed through parallelism, each candidate for $x \pmod{m_i}$ being tested for membership in R_i for all values of $i \leq k$ simultaneously. In speaking of such devices it is customary to use the term *ring corresponding to* m_i to refer to the reduced residues $\{0, 1, 2, \ldots, m_i - 1\}$ modulo m_i.

Let p_i be the ith prime. In the case where we are searching for pseudosquares, we could put $m_1 = 8$, $m_i = p_i$ $(i \geq 2)$, $n_1 = 1$, $n_i = (p_i - 1)/2$, $r_{1,2} = 1$, and use as the values of r_{ij} $(i > 1)$ the quadratic residues of m_i. Indeed, in order to increase the sieving speed, we can set up the problem in such a way that it will run faster than it would by using this naive approach. For example, since we know that $L_p \equiv 1 \pmod{24}$, we can consider $L_p = 1 + 24K_p$ and sieve, using different sets of admissible residues, to find K_p, thereby effecting a 24 fold speed-up.

We first used a larger version of OASiS [22] called OASiS II (OASiS with an additional sieve unit, see [22, p. 63]) to search for pseudosquares beyond the limit of Table 2 in [22]; however, after many months of continuous running of the device, we were able to find only two additional pseudosquares: L_{227} and L_{229}. As this rate

of sieving was just too slow, it was decided to construct a new sieve, the MSSU, which could search for values of L_p at a much greater rate than OASiS II. In what follows we give a brief description of this new sieve and its capabilities.

The *Manitoba Scalable Sieve Unit* (MSSU) employs Very Large Scale Integration (VLSI) circuits designed by Patterson [19, 20] at the University of Calgary. These sieve chips were manufactured using mature ($2\mu m$) CMOS gate array technology with a circuit complexity equivalent to 10,000 logic gates. Each device can accommodate the first 30 prime numbers (2 through 113) as moduli. The first four rings are special in that they correspond to moduli which are the prime powers 16, 9, 25 and 49. At present, the MSSU design utilizes a ring clock rate of 24 million shifts per second. Eight solution taps per ring bring the effective sieving rate to 192 million.

The small physical size and availability of a modest number of sieve chips made it possible for the MSSU design to incorporate 32 VLSI Sieve devices operating in parallel. The raw aggregate sieving rate of the MSSU is thus in excess of 6.4 billion integers per second. Effective partitioning of sieving problems across multiple sieve chips can result in a further speed-up. As an example, the pseudosquare problem can be partitioned to combine the moduli 8, 3, 5, 7 and 11, producing an implicit modulus of 9240 with 30 associated residue classes. The resulting effective sieving rate utilizing 30 Sieve chips (one per residue class) is thus:

$$9240 \times 192 \text{ million/sec} = 1.774 \text{ trillion/sec} = 6.387 \text{ quadrillion/hour}.$$

This optimization can be extended by combining the moduli 8, 3, 5, 7, 11 and 13, to form 180 residues, and then partitioning the problem into 6 subproblems of 30 chips each. This results in an increase of the maximum sieving rate by a factor of 13/6.

The MSSU hardware consists of two major subunits, the controller and the sieve chip array. The sieve controller consists of a high-speed microprocessor, memory and communication interfaces. The controller software accepts a small number of high-level commands from the host via a standard serial terminal port and translates them into the necessary low-level operations to be performed by the individual sieve chips. Typically, the host is a multi-user workstation; however, if need be, a dumb terminal can be used. The second major subunit is the sieve array circuit board. The sieve array contains 16 VLSI sieve devices and additional circuitry required to route ring data (admissible residues) and solution values to the desired chips. A maximal configuration of the MSSU supports the use of two sieve arrays for a total of 32 chips.

The nature of sieving problems often requires postprocessing of the solutions generated by the sieving hardware. Typically, we constrain solutions to have a specified property, such as being nonsquare or prime. This requires that hardware solutions be "filtered" to eliminate unwanted solutions. For many sieving problems, most notably the pseudosquares problem, solution filtering can be a bottleneck. The MSSU design utilizes several features which make solution filtering extremely efficient. Most importantly, filtering is performed locally by the control processor, not by relying on a host computer system like some previous systems.

The pseudosquares problem specifies a set of linear congruences which generate a large number of perfect square solutions which must be discarded using a perfect square filter. At low count values, where the density of perfect squares is greatest, sieve hardware is often idle while filter resources are overwhelmed. When running

the pseudosquares problem on the MSSU, starting from an initial count of 1, we observed during the first hour that sieving proceeded at 35.6% of the theoretical maximum speed. As the density of perfect squares diminished, this value increased to 86.5% during the second hour, and 94.1% during the third. At higher count values, sieving rates exceed 99% of the maximum speed of the hardware, attesting to the efficiency of filtering on the MSSU.

The MSSU is connected to a Unix host which provides the file storage and editing capabilities required to specify problems and capture solutions. Problems are defined using a simple text format which is simple to code and easy to read. Consistency checks, referred to as checkpoints, are performed hourly, thus permitting efficient recovery from hardware errors by restarting the problem from the last successful checkpoint. Off-line solution processing is supported, using an arbitrary-precision math package.

4. Numerical results

The MSSU was used to search for all pseudosquares L_p and all negative pseudosquares N_p up to 10^{19}. (In the case of L_p we ran the MSSU a little further.) We also searched for the least prime solution for L_p and N_p. Extensions of Tables I and II of [18] are presented in Tables 4.1 and 4.2 (see pp. 368 and 369).

Denote by $h(D)$ the value of the class number for the quadratic field $\mathcal{K} = \mathcal{Q}(\sqrt{D})$. Also, denote by $L(1,\chi)$ the value of the Dirichlet L-function $L(s,\chi)$ at $s = 1$, where

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s},$$

$\chi(n)$ is the Kronecker symbol (d/n), and d is the discriminant of $\mathcal{K}$. After Shanks [21] we define the Upper Littlewood Index (ULI) of $\mathcal{K}$ to be the value of

$$L(1,\chi)/(2e^{\gamma} \log\log |d|).$$

If the Riemann Hypothesis on $L(s,\chi)$ above holds, we must have

$$L(1,\chi) < \{1 + o(1)\} 2e^{\gamma} \log\log |d|;$$

thus, we expect that the value of the ULI should not greatly exceed 1. In Tables 4.3–4.6 we present the values of $h, L(1,\chi)$ and the ULI for the various fields $\mathcal{K} = \mathcal{Q}(\sqrt{D})$ with $D = L_p$ or $-N_p$ from Tables 4.1 and 4.2. Tables 4.3–4.8 are located in the Supplement section of this issue. Notice that, although we have attempted to maximize the value of $L(1,\chi)$ by selecting these values of D, the results of our computations provide us with no reason to suspect that the Riemann Hypothesis is false for any of these D values.

In the course of determining the values of L_p and N_p we also accumulated all of the values of $L, N < 10^{19}$ such that

$$L \equiv 1 \pmod 8, (L/p) = 1 \quad (L \text{ not a perfect square})$$

and

$$N \equiv -1 \pmod 8, \quad (-N/p) = 1$$

for all odd primes $p \leq 199$. This provided us with two lists, each comprising about 4000 numbers. We evaluated $h, L(1,\chi)$ and the ULI for $\mathcal{K} = \mathcal{Q}(\sqrt{D})$ with $D = L$ and $D = -N$ for all L and N values in these lists.

TABLE 4.1. Positive pseudosquares

p	least solution		least prime solution
83	2805544681	$= 127 \times 859 \times 25717$	8114538721
89	2805544681		9176747449
97	2805544681		23616331489
101	10310263441	$= 4007 \times 2573063$	23616331489
103	23616331489		23616331489
107	85157610409	$= 397 \times 214502797$	196265095009
109	85157610409		196265095009
113	196265095009		196265095009
127	196265095009		196265095009
131	2871842842801		2871842842801
137	2871842842801		2871842842801
139	2871842842801		2871842842801
149	26250887023729	$= 389 \times 67483000061$	26437680473689
151	26250887023729		89436364375801
157	112434732901969		112434732901969
163	112434732901969		112434732901969
167	112434732901969		112434732901969
173	178936222537081		178936222537081
179	178936222537081		178936222537081
181	696161110209049	$= 3793 \times 59471 \times 3086183$	6072205049848081
191	696161110209049		6072205049848081
193	2854909648103881	$= 331 \times 16451 \times 524290601$	6072205049848081
197	6450045516630769	$= 9529397 \times 676857677$	11641399247947921
199	6450045516630769		11641399247947921
211	11641399247947921		11641399247947921
223	11641399247947921		11641399247947921
227	190621428905186449	$= 1033661 \times 184413873509$	196640248121928601
229	196640248121928601		196640248121928601
233	712624335095093521	$= 28099 \times 25361199156379$	781158046093912369
239	1773855791877850321	$= 356366341 \times 4977618781$	6938117179828687609
241	2327687064124474441	$= 479 \times 4859471950155479$	9064125655411231729
251	6384991873059836689	$= 112741 \times 56634160359229$	?
257	8019204661305419761	$= 6151 \times 15329 \times 85049496359$	?
263	10198100582046287689	$= 277 \times 1091 \times 1151 \times 29318344777$	?
269	10198100582046287689		?
271	10198100582046287689		?

Excerpts of these results are presented in Tables 4.7 and 4.8, where we give the values of L or N for which the values of the corresponding $L(1, \chi)$ exceeds that for all previous values of L or N. Again, in spite of our attempt to try to maximize the ULI, there appears to be no violation of the Riemann Hypothesis.

Let p_i denote the ith prime ($p_1 = 2$). If we make the somewhat naive assumption (there will always be fluctuations) that the solutions of

$$x \equiv 1 \pmod 8, \quad (x/p_i) = 1 \qquad (i = 1, 2, \ldots, n) \tag{4.1}$$

are equidistributed in the region $0 < x < 8p_2p_3p_4 \cdots p_n$, then we would expect that if $p = p_n$, then[2]

$$L_p \approx 8p_2p_3 \cdots p_n/S,$$

[2]Of course we are assuming here that the least solution of (4.1) is not a perfect square.

TABLE 4.2. Negative pseudosquares († indicates that the negative pseudosquare is larger than the corresponding positive pseudosquare.)

p	least solution		least prime solution
137	844276851239	$= 794239 \times 1063001$	†4306732833311
139	1043702750999	$= 389 \times 5689 \times 471619$	†4306732833311
149	4306732833311		4306732833311
151	8402847753431		8402847753431
157	47375970146951	$= 151717 \times 312265403$	70864718555231
163	52717232543951	$= 223 \times 1747 \times 6863 \times 19717$	†317398900373231
167	100535431791791	$= 9873817 \times 10182023$	†501108392233679
173	†251109340045079	$= 2777 \times 90424681327$	†501108392233679
179	†493092541684679	$= 4723 \times 104402401373$	†501108392233679
181	493092541684679		501108392233679
191	493092541684679		5551185799073591
193	1088144332169831	$= 293 \times 464941 \times 7987687$	5551185799073591
197	1088144332169831		5551185799073591
199	1088144332169831		7832488789769159
211	1088144332169831		7832488789769159
223	†71608584429428591	$= 397 \times 2083 \times 86593503641$	†102097158739597271
227	88163809868323439	$= 96757 \times 911187923027$	102097158739597271
229	†218748706425968039	$= 12241 \times 17870166361079$	†315759454565514431
233	423414931359807911	$= 241 \times 1756908428878871$	†868116409360316399
239	695681268077667119	$= 3413 \times 203832777051763$	3412527725201978759
241	1116971853972029831	$= 1721 \times 869521 \times 746416591$	3546374752298322551
251	1116971853972029831		3546374752298322551
257	3546374752298322551		3546374752298322551
263	3546374752298322551		3546374752298322551
269	3546374752298322551		3546374752298322551

where S is the number of solutions of (4.1) in the given region. Since

$$S = \prod_{i=2}^{n} (p_i - 1)/2,$$

we get

$$L_p \approx 2^{n+1} \prod_{i=1}^{n} p_i/(p_i - 1).$$

By Mertens' Theorem we get

$$L_p \approx c_1 2^n \log p$$

for a constant $c_1 = 2e^{\gamma}$, suggesting that the nth pseudosquare should grow exponentially in n. In fact, since $p_n \sim n \log n$, we would expect that

$$\log(L_p/\log n) \approx n(\log 2 + o(1)) + c_2,$$

where $c_2 = \gamma + \log 2$.

In Figure 4.9, we present a plot of the values of $\log(L_p/\log n)$ for the L_p given in Table 4.1 against the values of n. The straight line represents the least squares line fitted to these data. For this line we have

$$y = .67987\mathrm{n} + 4.4835.$$

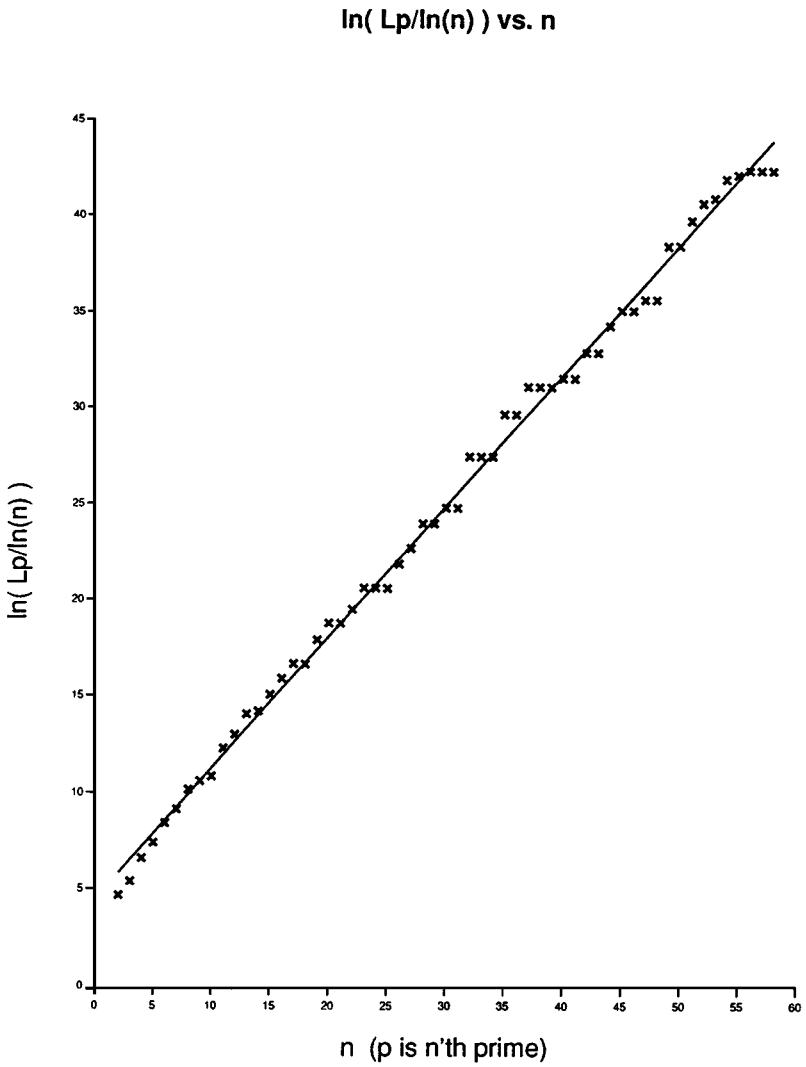

FIGURE 4.9

Thus, these numerical data lend some support to the heuristic belief that L_p should grow exponentially in n. In Figure 4.10 we have plotted the values of $\log L_p$ against p. We have also plotted the values of $\sqrt{p/2}$. Note that the growth rate of $\log L_p$ is much greater than that of $\sqrt{p/2}$, supporting (2.3). Thus, from the numerical data that we have so far been able to determine, it appears that L_p has a growth rate well in excess of $e^{\sqrt{p/2}}$. Indeed, our heuristic analysis above suggests that since $n \sim p_n/\log p_n$, we should have a growth rate for L_p of the form $2^{(p/\log p)(1+o(1))}$, a suggestion confirmed numerically in Figure 4.10. We should also point out that this growth rate for L_p could also be predicted from the plausible assumption made in [4] that pseudosquares will provide extreme values of $G(p)$. Under this assumption

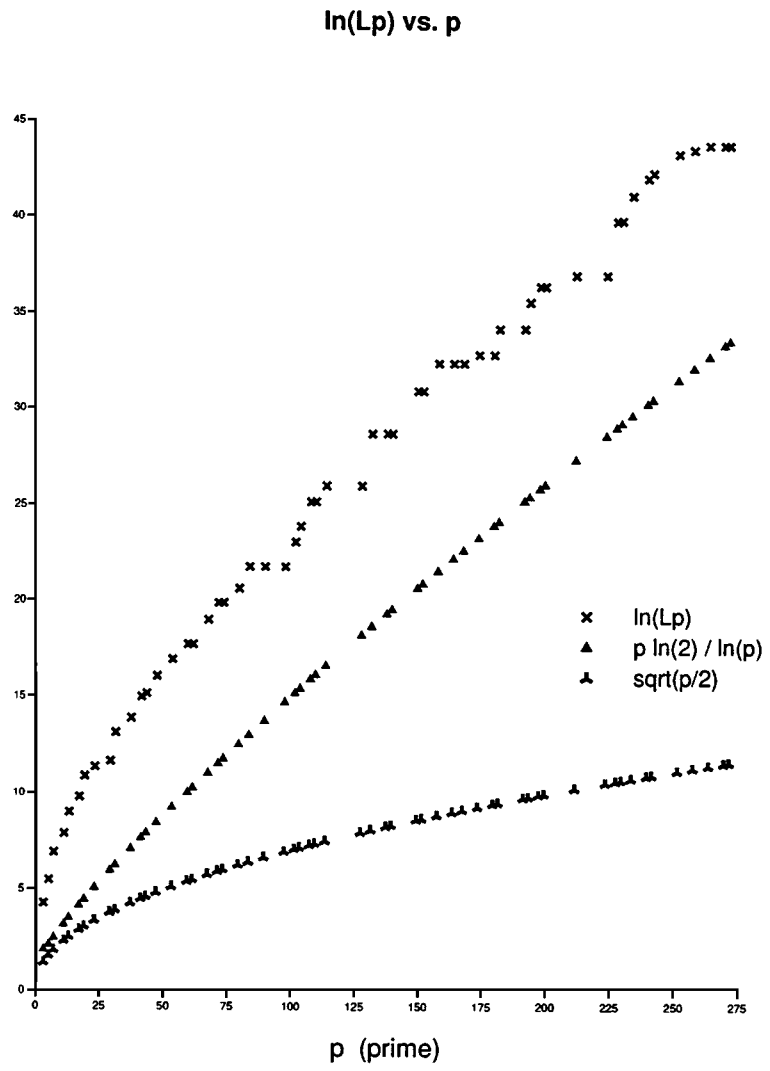

FIGURE 4.10

we would have

$$p \approx \frac{\log L_p \log\log L_p}{\log 2};$$

thus $\operatorname{Log} L_p \approx p \log 2 / \log p$.

ACKNOWLEDGEMENTS

The authors would like to extend their appreciation to the Alberta Microelectronic Centre, which produced the sieve chips used in the construction of the MSSU at only a nominal cost. They would also like to thank Mike Jacobson for evaluating all the class numbers and L-functions needed in Section 4. Thanks are also due

to an anonymous referee, who made many helpful suggestions for improving this paper.

References

1. L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983),173–206. MR **84e:**10008
2. L. M. Adleman and M.-D. Huang, *Primality testing and Abelian varieties over finite fields*, Lecture Notes in Math., vol. 1512, Springer-Verlag, Berlin, 1992. MR **93g:**11128
3. Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355–380. MR **91m:**11096
4. Eric Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, Math. Comp. **61** (1993), 69–82. MR **93k:**11089
5. Eric Bach and J. Sorenson, *Sieve algorithms for perfect power testing*, Algorithmica **9** (1993), 313–328. MR **94d:**11103
6. N. G. W. H. Beeger, *Sur la décomposition de grands nombres*, Nieuw Arch. Wisk. (2) **16** (1929/30), 37–42.
7. ———, *Note sur la factorisation de quelques grands nombres*, Arch. Inst. Grand-Ducal Luxembourg Sect. Sci. Nat. Phys. Math. **16** (1946), 93–95. MR **8:**134
8. A. Cobham, *The recognition problem for perfect squares*, Proc. 1966 IEEE Symposium on Switching and Automata Theory, IEEE Press, 1966, pp. 78–87.
9. N. D. Bronson and D. A. Buell, *Congruential sieves on FPGA computers*, Proc. Sympos. Appl. Math., vol. 48, 1994, pp. 547–551.
10. M. Hall, *Quadratic residues in factorization*, Bull. Amer. Math. Soc. **39** (1933), 758–763.
11. M. Kraitchik, *Recherches sur la théorie des nombres*, Gauthier-Villars, Paris, 1924.
12. ———, *Récherches sur la théorie des nombres.* I. II, Gauthier-Villars, Paris, 1929.
13. ———, *Factorisation es grands nombres*, Sphinx **1** (1931), 35–37.
14. D. J. Lehmann, *On primality tests*, SIAM J. Comput. **11** (1982), 374–375. MR **83i:**10006
15. D. H. Lehmer, *A fallacious principle in the theory of numbers*, Bull. Amer. Math. Soc. **36** (1930), 847–850.
16. ———, *A sieve problem on pseudo-squares*, MTAC **8** (1954), 241–242. MR **16:**113
17. ———, *A history of the sieve process*, A History of Computing in the Twentieth Century, Academic Press, New York, 1980, pp. 445–456. MR **81i:**68002
18. D. H. Lehmer, E. Lehmer, and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. **24** (1970), 433–451. MR **42:**5889
19. C. Patterson, *A* 538 *billion integer per second sieve*, Proc. 1991 Canad. Conf. on Electrical and Computer Engineering, 1991, pp. 13.1.1–13.1.4.
20. ———, *The derivation of a high speed sieve device*, Ph.D. Thesis, Dept. of Computer Science, University of Calgary, Calgary, Canada, 1991.
21. D. Shanks, *Systematic examination of Littlewood's bounds on* $L(1,\chi)$, Proc. Sympos. Pure Math., vol. 24, Amer. Math. Soc., Providence, RI, 1973, pp. 267–283. MR **49:**2596
22. A. J. Stephens and H. C. Williams, *An open architecture number sieve*, Number Theory and Cryptography (Sydney, 1989), London Math. Soc. Lecture Note Ser., vol. 154, Cambridge Univ. Press, Cambridge, 1990, pp. 38–75. CMP 90:13
23. H. C. Williams, *Primality testing on a computer*, Ars Combin. **5** (1978), 127–185. MR **80d:**10002

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

E-mail address: rflukes@cs.umanitoba.ca

Xilinx Development Corporation, 52 Mortonhall Gate, Edinburgh EH16 6TJ, Scotland

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

E-mail address: hugh_williams@csmail.cs.umanitoba.ca