A Probable Prime Test with Very High Confidence for $n \equiv 1 \bmod 4$

Siguna Müller[*]

University of Klagenfurt, Department of Mathematics, 9020 Klagenfurt, Austria
siguna.mueller@uni-klu.ac.at

Abstract. Although the Miller-Rabin test is very fast in practice, there exist composite integers n for which this test fails for 1/4 of all bases coprime to n. In 1998 Grantham developed a probable prime test with failure probability of only 1/7710 and asymptotic running time 3 times that of the Miller-Rabin test. For the case that $n \equiv 1 \bmod 4$, by S. Müller a test with failure rate of 1/8190 and comparable running time as for the Grantham test was established. Very recently, with running time always at most 3 Miller-Rabin tests, this was improved to 1/131040, for the other case, $n \equiv 3 \bmod 4$. Unfortunately the underlying techniques cannot be generalized to $n \equiv 1 \bmod 4$. Also, the main ideas for proving this result do not extend to $n \equiv 1 \bmod 4$.
Here, we explicitly deal with $n \equiv 1 \bmod 4$ and propose a new probable prime test that is extremely efficient. For the first round, our test has average running time $(4 + o(1)) \log_2 n$ multiplications or squarings mod n, which is about 4 times as many as for the Miller-Rabin test. But the failure rate is much smaller than $1/4^4 = 1/256$. Indeed, for our test we prove a worst case failure probability less than 1/1048350. Moreover, each iteration of the test runs in time equivalent to only 3 Miller-Rabin tests. But for each iteration, the error is less than 1/131040.

Keywords: Probable Prime Testing, Error Probability, Worst Case Analysis, Quadratic-Field Based Methods, Combined Tests

1 Introduction

1.1 Motivation

Large prime numbers are essential for most cryptographic applications. Perhaps the most common probabilistic prime test is the *Strong Fermat Test* (Miller-Rabin Test), which consists of testing that $a^s \equiv 1$, resp. $a^{2^j s} \equiv -1 \bmod n$ for some $0 \leq j \leq r - 1$ where $n - 1 = 2^r s$ with s odd. Although exponentiation modulo n can be performed extremely fast, the catch with this, as with any probable prime test, is the existence of pseudoprimes. This means that certain composite integers are identified as primes by the test.

[*] Research supported by the Austrian Science Fund (FWF), FWF-Project no. P 14472-MAT

C. Boyd (Ed.): ASIACRYPT 2001, LNCS 2248, pp. 87–106, 2001.

In a typical cryptographic scenario, some of the involved parties may be malicious. If an adversary manages to sell composites as primes, this usually compromises the security of the corresponding protocol. As strong pseudoprimes can easily be *constructed* this often allows fooling a pseudoprimality testing device that utilizes Miller-Rabin only. As an example, strong pseudoprimes are known with respect to all forty-six prime bases a up to 200 [3]. While a composite number can be a strong pseudoprime for at most $1/4$ of all bases coprime to n, there exist composites that actually do pass for this largest possible bound of the $1/4$ bases. Moreover, such numbers can efficiently be characterized and constructed [9]. Although it is known that $a = 2$ is a *witness* (for the compositeness of n) for most odd composites, it was shown in [2] that there are infinitely many Carmichael numbers whose least witness is larger than $(\log n)^{1/3 \log\log\log n}$. Also, it is conjectured [2] that there are $x^{1/5}$ Carmichael numbers $n \leq x$ for which there is *no base* a in any given set of $\frac{1}{11} \log x$ distinct integers $\leq x$ that proves n composite by the Miller-Rabin test.

While Miller-Rabin works well for any average number n on input a random base a, due to the fact that pseudoprimes can be constructed, the cautious might want to minimize the chance of being sold a composite instead of a prime.

There exist a number of deterministic algorithms for primality testing (see e.g., [7,10,12,20,32]), which however require rather involved theory and implementation. The advantage with pseudoprimality testing still is, that these approaches are a lot faster and can much more easily be realized in practice.

The result of this paper is a new probable prime test which is considerably more reliable than the previous proposals, but which still is much easier to describe and implement than the deterministic tests.

1.2 The Proposed Test

The main ideas for the pseudoprimality tests [16,26,28] consist of a combined Miller-Rabin test by utilizing both, the original $\mathbb{F}_p$-based algorithm, as well as the quadratic field (QF)- based analogue. An additional testing criterion in [26, 28] is based on the underlying (Cipolla related) square root finding algorithm modulo primes p (Lemma 1 below). If the result is not a correct root modulo n, n is disclosed as composite. Otherwise, this gives an additional testing condition.

Here, we incorporate yet another root-finding algorithm when $n \equiv 1 \bmod 4$. This constitutes a counterpart to the very recent results in [28] for $n \equiv 3 \bmod 4$ (the easier case). Via some efficient algorithm we test for what should be a square root of some Q mod n, $\left(\frac{Q}{n}\right) = 1$. This automatically constitutes a strengthened version of a Miller-Rabin Test. Consecutively, we test for the square root of 1 in the quadratic extension. We show how the root finding part can be obtained with low cost, with simultaneously obtaining a speed-up for the evaluation of the QF-part, as well as a reduction of the failure rate.

In essence, the test for any $n \equiv 1 \bmod 4$ runs as follows. We incorporate the same trivial testing conditions in our precomputation as does Grantham, [16]. Also, as in [16], we assume that n is not a perfect square.

```
0. (Precomputation)
    – If $n$ is divisible by a prime up to min$\{B, \sqrt{n}\}$, where
      $B = 50000$, declare $n$ to be composite and stop.
    – If $\sqrt{n} \in \mathbb{Z}$ declare $n$ to be composite and stop.
1. (Parameter Selection)
   Select randomly $P \in \mathbb{Z}_n$, $Q$ in $\mathbb{Z}_n^*$ such that $\left(\frac{Q}{n}\right) = 1$, $\left(\frac{D}{n}\right) = -1$.
2. (Square Root Part)
    – Run one of the square root finding algorithms of sect. 2.3
      for the root of $Q$ modulo $n$.
      If the root finding algorithm declares $n$ composite, stop.
    – Let $a$ be the root of $Q$ obtained, and let $P' \leftarrow P/a \bmod n$.
3. ($QF$-Based Part)
    – Let $\alpha(P', 1)$, $\overline{\alpha}(P', 1)$ be the roots of $x^2 - P'x + 1$.
    – Test, if $\alpha(P', 1)^{(n+1)/2} \equiv \overline{\alpha}(P', 1)^{(n+1)/2} \bmod n$.
            // For efficient practical realization see sect. 3.1.
      If not, $n$ is composite and stop.
    – Compute $\gcd(\alpha(P', 1)^{(n+1)/2} \pm 1, n)$. If one of these reveals a
      proper factor of $n$, output the factor. Otherwise declare $n$
      to be a probable prime.
```

The above describes the first round of the test. When being iterated, some of the calculations can be done more efficiently (see sect. 3.3).

1.3 The Results of This Paper

The main result of this paper is the following theorem. As in [16], one selfridge is equivalent to the time required for one round of Miller-Rabin.

Theorem 1. *A composite integer $n \equiv 1 \bmod 4$ passes k iterations of the proposed test with worst case failure probability less than $1/1048350 \cdot 1/131040^{k-1}$, which is approximately $1/2^{17k+3}$.*

For k iterations, the above test has average running time $3k + 1$ selfridges.

In detail, the result can be stated as follows.

- For one round of the proposed test, the exact failure is less than $1/2^{20} + 1/(2 \cdot B^2) < 1/1048350$ and the average running time is 4 selfridges.
- For each additional iteration, the proposed test has worst case failure probability $1/2^{17} + 4/B^2 < 1/131040$ and average running time 3 selfridges.

The first round failure rate should be contrasted to the worst case error probability $1/256$ of four iterations of the Miller-Rabin test. For two iterations of the proposed test this is $1/(1.37 \cdot 10^{11})$, opposed to $1/16384$, for three iterations $1/(1.8 \cdot 10^{16})$ opposed to $1/1048576$, etc.

The estimate is based on worst case analysis and on the assumption of the existence of special (bad) composites. Otherwise, the result would even be better.

The number of pairs that pass the proposed test (so-called 'liars') can explicitly be determined. This number of liars is largest for integers n of the form like $p-1|n-1$ and $p+1|n+1$ for all primes $p|n$. Such special types of numbers must be very rare and it is not even known whether they exist at all. This shows the difficulty for composites to pass the test with respect to varied parameters. Thus, the average case error rate is expected to be much smaller (see [14,37]).

Below, we describe one method how the underlying algorithms can *easily and efficiently be evaluated*. This is based on a naive multiply/add arithmetic and can easily be implemented with low effort. Alternatively, this could be achieved via the computation of elements in a quadratic extension field [22], the evaluation of second-order recurrences and Lucas chains [9,16,23,34,40], or of powers of 2×2 matrices [35].

For modular exponentiation, many improvements to the conventional powering ladder have been designed. We hope that analogously to the many tools for speeding up exponentiation in the prime field, similar devices for the QF- part will further improve on the practicality of the proposed test.

1.4 Related Work

A number of probable prime tests have been proposed which are based on various testing functions [1,6,8,19,33]. It turns out that the methods based on different underlying techniques are the most reliable ones, whereas those based on one technique only, allow the generation of pseudoprimes, even with respect to varied testing parameters. From a practical viewpoint however, the suggestions based on third and higher-order recurrences seem to be too expensive.

Pomerance, Selfridge, Wagstaff [33] and *Baillie, Wagstaff* [8] proposed a test based on both the Fermat test and on second-order (Lucas) sequences, which is very powerful. Although the underlying criteria can be evaluated extremely fast, no composite number is known for which this probable prime test fails. Indeed, nobody has yet claimed the $620 that is offered for such an example. While it is not known whether this test does allow any pseudoprimes at all, some heuristics indicate that such composites actually might exist [31]. Although the specific choice of the parameters makes the routine easy to describe, it might increase the chance of generating any pseudoprimes with respect to these parameters. Some related tests based on different parameters have been implemented in several computer-algebra systems which however turned out to be quite weak [30]. It is not known how reliable other parameters to this test are. Also, there is no quantifying measure to determine how reliable it actually is.

Several **probabilistic tests** have been published, for which an *explicit estimate on the worst case failure probability* is known.

- The Miller-Rabin test is usually taken as a unit measure with running time 1 selfridge [16] and worst case failure 1/4.
- J. Grantham [16] proposed an extremely efficient test with worst case failure rate 1/7710 and asymptotic running time 3 selfridges. Unfortunately, the practical implementation is rather involved and it seems that on average

$4.5 \log_2(n)$ multiplications (instead of the asymptotic $(3 + o(1)) \log_2(n)$) are necessary.
- By S. Müller [26] a probable prime test for the case that $n \equiv 1 \bmod 4$ was developed. The test has running time similar to the Grantham test, but with worst case error probability 1/8290 per round. This bound, however, can only be achieved for at least two iterations of the test.
- Recently, a proposal has been made [28] for $n \equiv 3 \bmod 4$ with failure rate 1/131040 but only 3 selfridges running time.

Jaeschke's tables [17] of strong pseudoprimes show that these occur very frequently for $n \equiv 1 \bmod 4$. Unfortunately, the techniques for the most effective test above, [28], are exclusive for the case $n \equiv 3 \bmod 4$. As the condition $4|n + 1$ constitutes a critical requirement for both the methods employed, as well as for the failure estimate, this cannot be extended to $n \equiv 1 \bmod 4$. Our results will be improvements and extensions of the methods of [26]. Indeed, for integers $n \equiv 1 \bmod 4$ essentially new techniques will be developed in this paper.

Relevance to Cryptography: For cryptographic applications, it is often necessary to generate pseudoprimes which are primes except for arbitrary small error rate. E.g., if a probability $1/2^{100}$ is to be achieved, one needs

- 50 iterations of Miller-Rabin, which is 50 selfridges,
- 8 iterations of the Grantham test, which is (asymptotically) 24 selfridges,
- 6 iterations of the proposed test, which is only 19 selfridges.

Due to the simple evaluation method of the proposed test via a naive powering ladder (sect. 3.1), we hope that this theoretical improvement will have some practical significance as well.

2 The New Idea

2.1 Some Fundamental Properties

Unless stated otherwise, let p, p_i be an odd prime, respectively an odd prime divisor of an integer $n \equiv 1 \bmod 4$ that is to be tested for primality. For simplicity we use the abbreviations of [36], *psp*(a), *epsp*(a), *spsp*(a), to denote, respectively, a pseudoprime, an Euler pseudoprime, and a strong pseudoprime, to base a.

Let $\epsilon(p) = \left(\frac{D}{p}\right)$ and $\epsilon(n) = \left(\frac{D}{n}\right)$, for $D = P^2 - 4Q$ the discriminant of $x^2 - Px + Q$ with characteristic roots $\alpha = \alpha(P, Q)$, $\overline{\alpha} = \overline{\alpha}(P, Q)$. We will assume that $\gcd(2QD, n) = 1$.

A number of probable prime tests are based on suitable properties in $\mathbb{F}_{p^2}$. As with the Miller-Rabin test in $\mathbb{F}_n$, when $n = p$ is prime, for both roots $y \in \mathbb{F}_{n^2}$ of $x^2 - Px + Q$ with $\epsilon(n) = -1$, one has, $y^u \equiv 1 \bmod n$, or $y^{2^k u} \equiv -1 \bmod n$ for some $0 \le k \le t - 1$, where $n^2 - 1 = 2^t u$ with u odd. The exponent $2^k u = \frac{n^2-1}{2^j}$ is still too large for obtaining strong testing conditions. More restrictive ones are being obtained via $y^{n-\epsilon(n)} \equiv 1$, respectively $Q \bmod n$, according as $\epsilon(n) = 1$ or

-1. As the former case constitutes an ordinary Fermat condition, in combination with a Fermat test, it only makes sense to test for the latter one. Thus, unless stated otherwise, we will throughout assume $\epsilon(n) = -1$.

Composite integers n fulfilling $y^{n-\epsilon(n)} \equiv Q \bmod n$ for $\epsilon(n) = -1$ are known as quadratic field based pseudoprimes w.r.t. (P, Q), abbrev. $QFpsp(P, Q)$.

If $\left(\frac{Q}{n}\right) = 1$ and if $\alpha, \overline{\alpha}$ denote the two roots y, then, for n prime, the two roots need to evaluate to the same value, even with the smaller exponent $(n-\epsilon(n))/2$ in place of $n - \epsilon(n)$, i.e., we must have $\alpha^{(n-\epsilon(n))/2} \equiv \overline{\alpha}^{(n-\epsilon(n))/2} \bmod n$. Composite integers fulfilling this criterion are denoted $elpsp(P, Q)$. In our case, for $n \equiv 1 \bmod 4$ and $\epsilon(n) = -1$, the value $(n+1)/2$ is odd which already constitutes the strong Lucas test and the pseudoprimes are denoted $slpsp(P, Q)$.

Lemma 1. *Let $\epsilon(n) = -1$ and let $n \equiv 1 \bmod 4$ be a composite integer that fulfills $\alpha^{n-\epsilon(n)} \equiv \overline{\alpha}^{n-\epsilon(n)} \equiv Q \bmod n$ for $\left(\frac{Q}{n}\right) = 1$. Then n is both $psp(Q)$ and $QFpsp(Q)$. If $\alpha^{(n-\epsilon(n))/2} \equiv \overline{\alpha}^{(n-\epsilon(n))/2} \bmod n$ then n is $slpsp(P, Q)$ for $\left(\frac{D}{n}\right) = -1$ and, moreover, $\left(\frac{Q}{p}\right) = 1$ for all prime divisors p of n.*

Proof. This follows directly from the proof of Theorem 3, [26], because for $n \equiv 1 \bmod 4$, $(n - \epsilon(n))/2 = (n + 1)/2$ is odd. □

The above conditions are tested in [16], however, Grantham does not consider the nature of the value $\alpha^{(n-\epsilon(n))/2}$ modulo n. In [26], a formula was obtained when n is a prime, and this was used to establish a new pseudoprimality test.

Proposition 1. *If α is any root of $x^2 - Px + Q$, and if $a^2 \equiv Q \bmod n$ for n prime, then $\alpha^{\frac{n-\epsilon(n)}{2}} \equiv \overline{\alpha}^{\frac{n-\epsilon(n)}{2}} \bmod n$, and this is equivalent to $\left(\frac{P+2a}{n}\right) \bmod n$, if $\epsilon(n) = 1$, and equivalent to $\left(\frac{P+2a}{n}\right) a \bmod p$, if $\epsilon(n) = -1$.*

Often a composite n fulfills the condition $\alpha^{n-\epsilon(n)} \equiv \overline{\alpha}^{n-\epsilon(n)} \equiv Q \bmod n$, but not the stronger one of Proposition 1. In that case $\gcd(\alpha^{(n-\epsilon(n))/2} \pm a, n)$ is a proper factor of n. This is the final condition being tested in Step 3 of the test.

2.2 The Main Problem

While the values $\alpha(P, Q)^k$, $\overline{\alpha}(P, Q)^k$, and $Q^k \bmod n$ theoretically can be evaluated with less than $(3+o(1)) \log_2 n$ multiplications [16], the practical application of the techniques in [16] is rather involved. For general Q, the fastest algorithm is given in [16]. Unfortunately, this requires special representation of k in terms of shortest addition chains. Brauer's Theorem [18] guarantees that asymptotically the number of multiplications in such shortest addition chains is $o(log(n))$, that is, it is vanishingly small compared to the number of squarings needed. This gives the *asymptotically* small running time of the Grantham test, but in practice, the required number of multiplications seems to be more like $4.5 \log_2(n)$.

For $\alpha = \alpha(P, Q)$, $\overline{\alpha} = \overline{\alpha}(P, Q)$, define the Lucas functions by $U_m(P, Q) = \frac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}}$ and $V_m(P, Q) = \alpha^m + \overline{\alpha}^m$. It can be shown that these are always integers (see, e.g., [41]).

Thus, for the QF-based tests (with, as usual, $\epsilon(n) = -1$), the condition $\alpha^{(n+1)/2} \equiv \overline{\alpha}^{(n+1)/2} \bmod n$, is equivalent to the vanishing of $U_k(P,Q) \bmod n$ for $k = (n+1)/2$. This, in turn can easily be checked via the condition

$$DU_k(P,Q) = 2V_{k+1}(P,Q) - PV_k(P,Q) \tag{1}$$

by means of two V- values, which is much easier than evaluating the U- function.

Moreover, the computation of $V_k(P,Q)$ for $Q = 1$ is much easier and faster than for general Q. Thus, it is natural to ask, how easily the required $V_k(P,Q)$, $V_{k+1}(P,Q)$ can be computed via some shifted parameters (P', Q') with $Q' = 1$.

A transformation between $V_k(P,Q)$ and $V_{2k}(\hat{P}, 1)$ is given in [13]. Unfortunately this induces a shift of the degree from k to $2k$ and cannot be applied in our scenario, which requires $k = (n - \epsilon(n))/2 = (n+1)/2$ to remain odd.

As in our case Q is a square, we apply the following well-known identities,

$$V_k(ca, a^2) = a^k V_k(c,1), \quad aU_k(ca, a^2) = a^k U_k(c,1). \tag{2}$$

Hence, if $\alpha(P/a, 1)^{(n+1)/2} \equiv \overline{\alpha}(P/a,1)^{(n+1)/2} \equiv \pm 1 \bmod n$ and $a^2 \equiv Q \bmod n$, then also $\alpha(P,Q)^{(n+1)/2} \equiv \overline{\alpha}(P,Q)^{(n+1)/2} \equiv \pm a^{(n+1)/2} \bmod n$.

Our *main goal* is a method for the separate computation of a root a of Q modulo n and for the evaluation of $\alpha(P/a,1)^k$, which in total is faster than the evaluation of $\alpha(P,Q)^k$, and which also induces a smaller failure rate. In detail, for the former,

- Find a practical root-finding algorithm that returns the root a of Q, $\left(\frac{Q}{n}\right) = 1$ for n prime, but with high probability discloses n as composite, otherwise.
- If the value a returned is a correct root of Q modulo n, then this should impose restrictive pseudoprimality conditions on n.

Remark 1. 1. If a is indeed a correct root of $Q \bmod n$, then the QF- part of the proposed test implies $\alpha(P,Q)^{(n+1)/2} \equiv \overline{\alpha}(P,Q)^{(n+1)/2} \equiv \pm a^{(n+1)/2} \bmod n$. If the root-finding algorithm imposes the condition $a^{(n-1)/2} \equiv \pm 1 \bmod n$ on n, then the above quantity is congruent to $\pm a \bmod n$ (see Proposition 1) and in that case n is also *spsp*(Q).

2. This shows why the case $n \equiv 3 \bmod 4$ in [28] is easier to deal with. Not only can the root be efficiently computed via $Q^{(n+1)/4} \bmod n$, but also, even when n is composite, this implies that $a^{(n-1)/2} \equiv \pm 1 \bmod n$.
3. While the root-finding algorithms for $n \equiv 1 \bmod 4$ are more expensive, they will be used in a way so as to induce some additional testing conditions.

2.3 Square Roots Modulo n and Conditions on the Pseudoprimes

The case that $\boxed{n \equiv 1 \bmod 4}$.

Let $n = 2^r s + 1$, with s odd, and call r the order of n. Suppose $\left(\frac{u}{n}\right) = -1$ and $(u^s)^{2^{r-1}} \equiv -1 \bmod n$. Then the 2-Sylow subgroup S_r of $\mathbb{Z}_n^*$ is cyclic of order 2^r. Shanks' root-finding algorithm [38] is based on the relation $a^2 \equiv bQ \bmod n$

for some b in some S_k. When n is prime, there exist new k, b, a such that this condition still holds and the index k decreases. Subsequently b gets pushed down into smaller subgroups of S_k until finally $b \in S_0 = \{1\}$, and the solution is found.

Note that the algorithm hinges on the existence of some u as above. But that criterion is not limited to n being prime. Modulo n, that condition on the u will either fail, or often the result of the algorithm will not be a root of Q. Indeed, the algorithm of Shanks not only efficiently performs Step 2 of the proposed test, but also works as an efficient probable prime test (see also [29]).

```
  // Detailed Description of Step 2 of the Proposed Test.
  INPUT: $n = 2^r s + 1$, $2 \nmid s$, $\left(\frac{Q}{n}\right) = 1$.
  OUTPUT: $a$, a square root of $Q \bmod n$, or ‘$n$ is composite’.

1. (Precomputation)
   Choose randomly $u \in \mathbb{Z}_n^*$ with $\left(\frac{u}{n}\right) = -1$. Let $z \leftarrow u^s \bmod n$. If not
   $z^{2^{r-1}} \equiv -1 \bmod n$, declare $n$ to be composite.
2. (Initialization)
   Let $k \leftarrow r - 1$, $t \leftarrow Q^{(s-1)/2} \bmod n$, $a \leftarrow Qt \bmod n$, $b \leftarrow at \bmod n$.
3. (Body of the Algorithm)
   While $b \not\equiv 1 \bmod n$    (*)
         $m \leftarrow 1$, $B \leftarrow b$, $found \leftarrow$ false;
         While $m < k$ and $found =$ false   (**)
               if $B = 1$ then OUTPUT $g \leftarrow \gcd(B_0 - B, n)$;
                     // proper factor of $n$ found
               if $B = -1$ then $found \leftarrow$ true;
               else $m \leftarrow m + 1$, $B_0 \leftarrow B$, $B \leftarrow B^2 \bmod n$.
         If $found =$ false then OUTPUT ‘$n$ is composite’.
                     // otherwise we have $B \equiv b^{2^{m-1}} \equiv -1 \bmod n$
         Update $t \leftarrow z^{2^{k-m-1}}$, $z \leftarrow t^2$, $b \leftarrow bz$, $a \leftarrow at \bmod n$, $k \leftarrow m$.
4. OUTPUT $\pm a \bmod n$.
```

The algorithm always returns a root of Q when n is prime. This also holds for $n \equiv 3 \bmod 4$. Note the more restrictive condition (**), $b^{2^{m-1}} \equiv -1 \bmod n$ for $m \geq 1$, as opposed to the original one by Shanks, $b^{2^m} \equiv 1 \bmod n$. This introduces an additional pseudoprimality testing condition.

Lemma 2. *If a composite n passes the precomputation, then n is spsp(u). If the original b is congruent to 1 modulo n, or if n fulfills condition (**) at least for the first loop (*), then n is spsp(Q) and $a^{(n-1)/2} \equiv \pm 1 \bmod n$.*

Moreover, n passes at most $r-1$ iterations of the loop (*), where $r = \nu_2(n-1)$. Additionally, for $k \geq 2$ and random input Q, n passes k iterations of (*) with probability at most $1/3^k$.

Proof. The first assertions are obvious. Now suppose $n - 1$ is at least divisible by 2^3 and that n enters the loop (*) at least twice.

Note that after each iteration (*) the relation $a^2 \equiv Qb \bmod n$ holds. Once $b \equiv 1 \bmod n$, the desired solution is found.

From the previous iteration we have $b^{2^{m-1}} \equiv -1 \bmod n$. Let $h = z^{2^{k-m}}$. From the latter condition and the fact that $u^{(n-1)/2} \equiv -1 \bmod n$ it follows exactly as when n is a prime, that h has order 2^m modulo n.

If firstly $h^{2^{m-1}} \equiv -1 \bmod n$ (what would happen if n were prime), then $hb = t^2 b$ has order dividing 2^{m-1} and the new b enters the next loop. But this means that each new b has an order which is at least by one factor in 2 smaller than the previous b. This explains the condition that each new m has to be less than k (which was the previous m). Equivalently, the sequence of the k in the loop are strictly decreasing, so that altogether there are less than r iterations of (*) (unless n is already previously disclosed as composite).

On the other hand, if $h^{2^{m-1}} \not\equiv -1 \bmod n$, but $b^{2^{m-1}} \equiv -1 \bmod n$, then $(hb)^{2^{m-1}} \not\equiv 1 \bmod n$ and (hb) (which is the new b) has order 2^m, as does the previous b. In this case, the new b does not fulfill (**).

It follows from above that unless the algorithm already terminated, we have $b^{2^M} \equiv 1 \bmod n$ for some M. If $M = 0$, we are done. Otherwise, we are seeking the smallest m with $b^{2^{m-1}} \equiv -1 \bmod n$, when $b \neq 1$, i.e., when $m \geq 1$. In that case, in analogy to the Miller-Rabin test, the first such power of b before 1 has to be -1. When we first arrive at 1, without encountering -1, n is immediately disclosed as composite, and the gcd above obviously yields a proper factor of n. In exactly such a case the algorithm terminates at a point where it would not if n were prime. Thus, the above algorithm terminates much faster for composites. Precisely, it terminates for each case where $b^{2^m} \equiv 1 \bmod n$, but $b^{2^{m-1}} \equiv 1 \bmod p$ for one prime p dividing n, and $b^{2^{m-1}} \equiv -1 \bmod q$ for another prime $q|n$. It does not terminate when $b^{2^{m-1}} \equiv -1 \bmod p$ for all $p|n$. If n is the product of two primes, the latter only happens in one out of three cases, while if n has more factors, the probability not to terminate is even smaller. Thus, in at most 1 out of 3 cases each additional iteration of (*) does not terminate. The desired assertion follows from the hypothesis that the Q are randomly chosen (subject only to the condition $\left(\frac{Q}{n}\right) = -1$), which implies that all the b values are random. □

For the special case $\boxed{n \equiv 5 \bmod 8}$ the above can be achieved even simpler.

```
    // Alternative Case of Step 2 of the Proposed Test.

1. Select randomly $d \in \mathbb{Z}_n^*$.
   If $n$ is not $spsp(2d^2)$, declare $n$ to be composite.
2. Let $z \leftarrow (2d^2Q)^{(n-5)/8} \bmod n$ and $i \leftarrow z^2 \cdot 2d^2Q \bmod n$.
3. If not $i^2 \equiv -1 \bmod n$, declare $n$ to be composite, otherwise
   $a \equiv zdQ(i-1) \bmod n$ is a square root of $Q$ modulo $n$.
```

When n is known to be prime, this always gives is a square-root of Q via *one* exponentiation only (then clearly the first step can be omitted).

Lemma 3. *If a composite $n \equiv 5 \bmod 8$ passes the above algorithm, then a and i are correct roots of Q and $-1 \bmod n$, respectively. Moreover, n is $spsp(2d^2)$, as well as $spsp(2d^2Q)$. As a consequence, n is also $epsp(Q)$.*

Proof. This follows since any $epsp(a)$ for $\left(\frac{a}{n}\right) = -1$ is already $spsp(a)$. □

Remark 2. For $d = 1$ the above algorithm was proposed by Atkin [5], and actually constitutes a *deterministic* root-finding method for primes $n \equiv 5 \bmod 8$.

Step 1 is necessary to have n $epsp(Q)$, which will be required below. We incorporate the random value d to minimize the failure probability by means of Miller-Rabin with respect to the *random* base $2d^2$.

Corollary 1. *Suppose a composite integer n passes the proposed test. Then, in the case of the square root finding algorithm for $n \equiv 5 \bmod 8$, this implies $\alpha(P,Q)^{(n+1)/2} \equiv \overline{\alpha}(P,Q)^{(n+1)/2} \equiv \pm a^{(n+1)/2} \bmod n$, and in the case of the Shanks-based root finding algorithm, the latter value is congruent to $\pm a \bmod n$. In both cases, $\alpha(P,Q)^{n+1} \equiv \overline{\alpha}(P,Q)^{n+1} \equiv Q \bmod n$.*

Proof. The first part follows from above. Note that if n passes the root-finding algorithm then it is $epsp(Q)$. But if n is $epsp(Q)$ and $elpsp(P,Q)$, then by well-known results [24], this implies, $\alpha(P,Q)^{n+1} \equiv \overline{\alpha}(P,Q)^{n+1} \equiv Q \bmod n$. □

3 Performance

3.1 Evaluation of the QF-Based Part

By property (1), the QF-part can be evaluated via the V- functions only. Using the identities, $V_{2k}(P,1) = V_k(P,1)^2 - 2$ and $V_{2k+1}(P,1) = V_k(P,1)V_{k+1}(P,1) - P$, this can be done via a simple powering ladder analogously as for exponentiation.

The algorithm in [34] can easily be modified to obtain two consecutive V-values, as required. The operations are done modulo n.

```
   INPUT: $m = \sum_{j=0}^{l} b_j 2^j$, the binary representation of $m$, and $P$.
   OUTPUT: The pair $V_m(P,1)$ and $V_{m+1}(P,1)$.

1. (Initialization) Set $d_1 \leftarrow P,\ d_2 \leftarrow P^2 - 2$.
2. (Iterate on $j$) For $j$ from $l - 1$ down to 1 do
         If $b_j = 1$, set $d_1 \leftarrow d_1 d_2 - P$, $d_2 \leftarrow d_2^2 - 2$.
         If $b_j = 0$, set $d_2 \leftarrow d_1 d_2 - P$, $d_1 \leftarrow d_1^2 - 2$.
3. (Evaluate) Let $w_1 \leftarrow d_1 d_2 - P,\ w_2 \leftarrow d_1^2 - 2$.
   If $b_0 = 1$ return $(w_1, Pw_1 - w_2)$, else return $(w_2, w_1)$.
```

Thus, the pair $V_{(n+1)/2}(P,1)$, $V_{(n+1)/2+1}(P,1)$ may be computed modulo n using fewer than $2\log_2(n)$ multiplications mod n and $\log_2 n$ additions mod n. Half of the multiplications mod n are squarings mod n.

```
     // Detailed Description of Step 3 of the Proposed Test.

 – Let $k = (n+1)/2$ and evaluate $(V_k(P',1), V_{k+1}(P',1))$ modulo $n$.
 – Test, if $2V_{k+1}(P',1) \equiv P'V_k(P',1) \bmod n$. If not, declare $n$ to be
   composite.
 – Compute $\gcd(V_k(P',1) \pm 2, n)$. If this reveals a factor of $n$,
   output the factor. Otherwise declare $n$ to be a probable prime.
```

3.2 Runtime-Analysis

In [16], J. Grantham suggested a unit measure for a probable prime test based on the running time of the Miller-Rabin test. An algorithm with input n is said to have running time of k *selfridges* if it can be computed in $(k + o(1)) \log_2 n$ multiplications mod n. For simplicity, squarings are counted as multiplications.

As exponentiation to the tth power can be done in $(1 + o(1)) \log_2 t$ multiplications by using easily constructed addition chains [18], the Miller-Rabin test has running time of at most 1 selfridge.

Theorem 2. – *For random input Q and u, the proposed test, via the general root finding algorithm, has average running time* 4 *selfridges.*

– *For the $n \equiv 5 \bmod 8$ based root finding algorithm, the proposed test always has running time less than* 4 *selfridges.*

Proof. By the above, Step 3 of the proposed test requires at most two selfridges.

The Atkin-based method always requires two exponentiations, so we only need to consider the general Shanks-based root finding algorithm. Precomputation and initialization require one exponentiation each. It follows from [21] that the number of multiplications averaged over primes $n \equiv 1 \bmod 4$ is $o(1) \log_2(n)$. The additional squarings that we require in Step 1 for the Miller-Rabin test base u can be comprised in the $o(1) \log_2(n)$ multiplications above.

We upper bound the number of multiplications in the worst case required by the loop (*). If n is $spsp(u)$ then $z = u^s$ generates S_r, the 2-Sylow subgroup of $\mathbb{Z}_n^*$. So S_r has order 2^r, S_{r-1} has order 2^{r-1}, is generated by z^2, and in general, S_{r-i} has order 2^{r-i} and is generated by z^{2^i} for $i = 0, 1, ..., r$.

The condition (**) indicates in which of the 2-subgroups b is in. Alternatively, we can consider the values that k takes in the algorithm, which also (except for the first k), specifies the subgroup where b is in. Namely, $b \in S_k \setminus S_{k-1}$.

Recall that the sequences of the k-values have to be strictly decreasing. E.g., for order $r = 4$, the possible k-sequences are, $(4, 1)$, $(4, 2)$, $(4, 2, 1)$, $(4, 3)$, $(4, 3, 1)$, $(4, 3, 2)$, $(4, 3, 2, 1)$. Generally there are 2^{r-1} such k-sequences.

For random Q's and u's the values b are random as well and it can be shown (see [21, p. 235]) that every k-sequence has the same probability. Lindhurst determined the total number of multiplications C_r over all the possible k-sequences and then divided by the number of sequences, 2^{r-1}, to get the average. Then, the average number of multiplications (after the initialization), is $C_r/2^{r-1} = (r^2 + 7r - 12)/4 + 1/2^{r-1}$ (see [21, p. 236]).

Although all sequences are equally like, they can be grouped into those with the same length. The 2^{r-1} sequences of order r are obtained by fixing the r as first value of the sequence, and by determining the $\binom{r-1}{1}, \binom{r-1}{2}, \ldots, \binom{r-1}{r-1}$ subsequences $(k_1, .., k_l)$ of respective lengths $1, 2, \ldots, r - 1$. This shows that an average sequence is expected to have length about $r/2$. Equivalently, on average, the loop (*) is iterated $r/2$ times. Additionally, for $r \geq 8$, more than 99 % of all sequences have length between $\lfloor \frac{r}{4} \rfloor$ and $\lceil \frac{3r}{4} \rceil$.

But then Lemma 2 and Lemma 6 below implies that on average at most $\frac{(r^2+7r-12)/4+1/2^{r-1}}{3^{\lfloor r/4 \rfloor}}$ multiplications are to be expected before the algorithm terminates, when n is composite. Comparing numerator and denominator, we see that this is much less than for primes, as repeated iterations of (*) are much less likely. □

3.3 The Iterated Test

After the first round it is more efficient to shorten each of the following iterations, instead of re-running the entire procedure. For entire iteration, we would achieve a failure probability of about $1/2^{20k}$ and $4k$ selfridges for k rounds.

Below, the failure rate of the QF-based part will be shown to be much smaller than the one based on the root finding algorithm. Yet, each of those parts requires about two selfridges. When being iterated, it is more efficient to repeat only a part of the root finding algorithm, whilst obtaining the full QF-part. In fact, for both of the above root finding algorithms, the first step is only required at the first round. This motivates the following shortened version of the proposed test for any iterations after the first.

```
      // Iterations After the First Round of the Test.

1. (Parameter Selection) As above.
2. (Square Root Part)
    - Let $u$ and $d$, accordingly, be the values of the first round
      of the proposed test in Step 1 of the root finding part.
    - Run one of the above root finding algorithms by skipping
      the corresponding Step 1.
      If the algorithms declares $n$ composite, stop.
    - Let $a$ and $P'$ be as above.
3. ($QF$-Based Part) As above.
```

4 The Probability Estimate

The proof of Theorem 1 will be given in a sequence of auxiliary results. The general idea is to determine an upper bound on the number of the liars (i.e., pairs that pass) and to upper bound the ratio of these to the number of all pairs possible as input to the test. It was shown in [16] that for n an odd composite, not a perfect square, the number of pairs (P, Q), such that $\left(\frac{P^2-4Q}{n}\right) = -1$ and $\left(\frac{Q}{n}\right) = 1$, $1 < \gcd(P^2 - 4Q, n) < n$, or $1 < \gcd(Q, n) < n$, is more than $n^2/4$.

4.1 The *QF*-Based Part

Underlying all the pseudoprimality tests based on quadratic fields is the investigation of the powers of the characteristic roots α, $\overline{\alpha}$. It is well known that if n is any integer with $\gcd(Q, n) = 1$ then there is a positive integer m such that $\alpha(P,Q)^m \equiv \overline{\alpha}(P,Q)^m \bmod n$. Let $\rho = \rho(n,P,Q)$ be the least such positive integer. This is usually called the *rank of appearance* (apparition) [36,41].

The rank of appearance has the following properties (see [11,36,39]).

$$\alpha(P,Q)^m \equiv \overline{\alpha}(P,Q)^m \bmod k \text{ if and only if } \rho(k,P,Q)|m, \tag{3}$$

$$\rho(p,P,Q) \mid p-\epsilon(p), \text{ and } \rho(p,P,Q) \mid (p-\epsilon(p))/2 \text{ iff } (Q/p)=1, \tag{4}$$

$$\rho(lcm(m_1,...,m_k)) = lcm(\rho(m_1),...,\rho(m_k)), \tag{5}$$

$$\text{If } p^c || \, \alpha(P,Q)^{\rho(p,P,Q)} - \overline{\alpha}(P,Q)^{\rho(p,P,Q)} \text{ then } \rho(p^e,P,Q) = p^{\max(e,c)-c}\rho(p,P,Q). \tag{6}$$

A necessary condition for the test to pass is $\alpha(P,Q)^{n+1} \equiv \overline{\alpha}(P,Q)^{n+1} \bmod n$. Since $p \not| \, n{+}1$ for $p|n$, we need not consider the pairs (P,Q) modulo p^α whose rank is a multiple of p (compare (6)). Thus, it suffices to investigate the parameters whose rank is an odd divisor of $p-\epsilon(p)$, since $(n+1)/2$ is odd for $n \equiv 1 \bmod 4$.

Given n, the task is to count the number of the liars (P,Q), which is determined by the rank of appearance of each of these pairs. But this requires knowledge of the individual quadratic residue symbols $\left(\frac{Q}{p_i}\right)$ and $\epsilon(p_i) = \left(\frac{P^2-4Q}{p_i}\right)$ for all primes $p_i|n$.

Generally, these values are not known for the number n to be tested for primality. However, certain conditions on these symbols are automatically satisfied when a composite n indeed passes the test. Specifically, by Lemma 1 it suffices to consider the case that $\left(\frac{Q}{p}\right) = 1$ for any prime p dividing n. We separately consider the values $\epsilon(p_i)$.

Definition 1. *Let $n = \prod_{i=1}^{\omega} p_i^{\alpha_i}$, where $\omega = \omega(n)$ is the number of different prime factors of n. For $1 \le i \le \omega$ let $\epsilon = \epsilon(p_i) \in \{1,-1\}$, and call $(\epsilon) = (\epsilon(p_1),...,\epsilon(p_\omega))$ the signature modulo n with respect to P and Q, when $\left(\frac{P^2-4Q}{p_i}\right) = \left(\frac{D}{p_i}\right) = \epsilon(p_i)$ for all i. Similarly, we call each $\epsilon(p_i)$ the signature modulo $p_i|n$, and $\epsilon(p)$ the signature modulo any prime p.*

Throughout, P is assumed to be different from 0, since otherwise the rank of appearance modulo n is always equal to 2. (This is no restriction as for $P=0$ always $(D/n)=1$ in our case.) Proposition 2 was proved in [28] and Proposition 3 was proved in [25].

Proposition 2. *Let k, $p \not| k$, be a positive integer and $\epsilon \in \{-1,1\}$ a constant. For a fixed value of P_0, $P_0 \neq 0$, the number of $Q \bmod p^\alpha$ such that $\left(\frac{Q}{p}\right) = 1$, (P_0,Q) has signature $\epsilon \bmod p$, and $\alpha(P_0,Q)^k \equiv \overline{\alpha}(P_0,Q)^k \bmod p^\alpha$, equals $\frac{1}{2}\left(\gcd(k,\frac{p-\epsilon}{2})-2\right)$ if $2|k$ and $2|\frac{p-\epsilon}{2}$, and $\frac{1}{2}\left(\gcd(k,\frac{p-\epsilon}{2})-1\right)$, otherwise.*

Proposition 3. *Let k be a positive integer with $p \not| k$ and $\epsilon \in \{-1,1\}$ a constant. For a fixed value of Q_0, $\left(\frac{Q_0}{p}\right) = 1$, the number of $P \bmod p^\alpha$ such that (P,Q_0) has signature ϵ and $\alpha(P,Q_0)^k \equiv \overline{\alpha}(P,Q_0)^k \bmod p^\alpha$ is, $\frac{1}{2}\gcd(k,p-\epsilon)-1$, when $\nu_2(k) \ge \nu_2(p-\epsilon)$, and $\gcd(k,\frac{p-\epsilon}{2})-1$, otherwise.*

Corollary 2. *Let a signature* (ϵ) *be fixed. Then the number of pairs* (P,Q) *that fulfill* $\alpha(P,Q)^{(n+1)/2} \equiv \overline{\alpha}(P,Q)^{(n+1)/2} \bmod n$ *with respect to this signature is at most* $\frac{1}{2^\omega}\prod_{i=1}^{\omega}\left(\gcd(\frac{n+1}{2},\frac{p_i-\epsilon(p_i)}{2})-1\right)^2 \cdot \prod_{i=1}^{\omega} p_i^{\alpha_i-1}$.

Lemma 4. *Let* $n \equiv 1 \bmod 4$ *be an odd integer, not a perfect square. If* p_j *is a prime such that* p_j^2 *divides* n*, then* n *is slpsp*(P,Q) *for* $\left(\frac{D}{n}\right)=-1$ *with probability less than* $1/(8p_j)$.

Proof. Let (ϵ) be a fixed signature. By Corollary 2, the number of liars (P,Q) with respect to this signature is at most $(1/2^{3\omega})\prod_{i=1}^{\omega}(p_i-1)^2\cdot\prod_{i=1}^{\omega}p_i^{\alpha_i-1}$.

If $\omega=2$, then there are two possible signatures with $\left(\frac{D}{n}\right)=-1$ and so the number of the liars is at most $(1/2^5)\cdot\prod_{i=1}^{\omega}(p_i-1)^2\cdot\prod_{i=1}^{\omega}p_i^{\alpha_i-1}$. This gives a failure probability of less than $(1/2^3)\cdot\prod_{i=1}^{\omega}p_i^{\alpha_i+1}/\prod_{i=1}^{\omega}p_i^{2\alpha_i}=1/(2^3\cdot\prod_{i=1}^{\omega}p_i^{\alpha_i-1})\leq 1/(8p_j)$. For $\omega\geq 3$ there are always less than 2^ω different signatures with $\left(\frac{D}{n}\right)=-1$ and the number of liars is less then $(1/2^{2\omega})\cdot\prod_{i=1}^{\omega}p_i^{\alpha_i+1}$ which gives a probability of at most $1/(2^{2\omega-2}p_j)\leq 1/(2^4p_j)$. Finally, if $\omega=1$, so that $n=p_j^{\alpha_j}$, then necessarily $\alpha_j>2$ by hypothesis and the probability in this case is at most $1/(2p_j^2)$. □

Typical for pseudoprimality testing based on the Fermat/QF-based combinations is the fact that $\left(\frac{D}{p}\right)=1$ becomes rather unlikely for $p|n$ when $\left(\frac{D}{n}\right)=-1$.

Proposition 4. *The number of pairs* $(P,Q) \bmod n$ *for which a squarefree integer* n *with* ω *prime factors fulfills* $\alpha(P,Q)^{(n+1)/2}\equiv\overline{\alpha}(P,Q)^{(n+1)/2} \bmod n$ *such that* $\left(\frac{P^2-4Q}{p_i}\right)=1$ *for some* $p_i|n$*, is given as follows. It is less than* $\frac{5n\phi(n)}{2^6B}$ *if* $\omega=2$*, less than* $n\phi(n)\left(\frac{\omega}{2^{3\omega-2}B}+\frac{1}{2^{2\omega-4}B^2}\right)$ *if* $\omega\geq 4$ *is even, and less than* $\frac{n\phi(n)}{B^2}$ *if* ω *is odd.*

Proof. See the proof to Proposition 5 in [28], where exactly the number of such pairs is being established. □

Remark 3. For $\omega=2$ the proof in [28] shows that the above quantities are only obtained for strongest divisor properties, like odd$(p_i+1)|n+1$ for one $p_i|n$, and odd$(p_j+1)|t(n+1)$ for $t=3$ and the other $p_j|n$. Otherwise, the results would be much smaller.

When the test passes for some fixed $Q=Q_0$, then we have for each parameter P, $\alpha^{(n+1)/2}\equiv\overline{\alpha}^{(n+1)/2} \bmod n$, and this is either equivalent to $a^{(n+1)/2} \bmod n$, or to $-a^{(n+1)/2} \bmod n$, where a is independent of P, and by the root finding algorithms is uniquely determined by the Q_0. For all P that pass, this determines a specific general 'multiplier' $S\equiv a^{(n+1)/2}$, resp. $S\equiv -a^{(n+1)/2}$ modulo n. The proof to the next result is analogous to Lemma 5, [26] (see Proposition 4, [28]).

Lemma 5. *Let $n \equiv 1 \bmod 4$ be any composite integer, and $Q = Q_0$, as well as some 'multiplier' S be fixed. If p is any prime dividing n, then there are at most $\frac{1}{2}\left(\gcd(\frac{n+1}{2}, p-\epsilon(p)) - 1\right)$ elements P with $\left(\frac{P^2-4Q_0}{p}\right) = \epsilon(p)$ for which $\alpha(P,Q)^{\frac{n+1}{2}} \equiv \overline{\alpha}(P,Q)^{\frac{n+1}{2}} \equiv S \bmod p$.*

Corollary 3. *For a squarefree $n \equiv 1 \bmod 4$ let (ϵ) be a fixed signature. Then the number of pairs (P,Q) with $\alpha(P,Q)^{(n+1)/2} \equiv \overline{\alpha}(P,Q)^{(n+1)/2} \equiv \pm a^{(n+1)/2} \bmod n$ w.r.t. this signature is at most $\frac{1}{2^{2\omega-1}}\prod_{i=1}^{\omega}(\gcd(\frac{n+1}{2}, \frac{p_i-\epsilon(p_i)}{2}) - 1)^2$.*

Remark 4. It is essential that $n \equiv 1 \bmod 4$ to have $(n+1)/2$ odd. For $n \equiv 3 \bmod 4$ analogous, but more involved results can be obtained, [28].

This gives the error rate for each iteration of the test (after the first round).

Theorem 3. *Let P and Q be randomly chosen in Step 1 of the proposed test. Let $n \equiv 1 \bmod 4$ be a composite integer which is not a perfect square and not divisible by primes up to B. Then the probability that n fulfills $\alpha(P,Q)^{(n+1)/2} \equiv \overline{\alpha}(P,Q)^{(n+1)/2} \equiv \pm a^{(n+1)/2} \bmod n$ for $a^2 \equiv Q \bmod n$, is given as follows.*

- *If n is not a product of exactly three prime factors, it is less than $1/2^{17} + 4/B^2 < 1/131040$.*
- *If n is the product of three different primes, and if n is further epsp(Q), then it is less then $4/B^2 + 3(B^2+1)/2(B^4 - 3B^2)$.*

Proof. When n is not squarefree, Lemma 4 gives the result. If a squarefree n has an even number of prime factors we apply Proposition 4, where the probability becomes largest for $\omega = 2$ in which case it is less than $5/(2^4 B) < 1/160000$.

Further, if $n = p_1 p_2 p_3$ is squarefree and has exactly 3 prime factors, we can use Lemma 2.11 of [16]. In this Lemma, Grantham separately considers the cases, $\left(\frac{P^2-4Q}{p_i}\right) = 1$ for some i, and $\left(\frac{P^2-4Q}{p_i}\right) = -1$ for all i. By Proposition 4 (which corresponds to Lemma 2.9 of [16] when ω is odd), the former case yields a probability of $4/B^2$. In the latter case, necessarily $\alpha^{n+1} \equiv Q \bmod p_i$ and $\alpha^{p_i+1} \equiv Q \bmod p_i$ so that $\alpha^{n-p_i} \equiv 1 \bmod p_i$, since n is *epsp*(Q) by hypothesis (see Corollary 1). This congruence holds for exactly $\gcd(n-p_i, p_i^2-1)$ elements. Since n has only three factors, these $\gcd's$ cannot all be equal to its maximal value, $p_i^2 - 1$. Indeed, Grantham gives an upper limit for these quantities. From this, he obtains the probability for such pairs which pass the test. By adding both cases, the probability can be bounded by $4/B^2 + 3(B^2+1)/2(B^4 - 3B^2)$.

It remains to consider the case where n is squarefree and divisible by an odd number ω of at least 5 prime factors. The number of pairs with $\left(\frac{D}{p}\right) = 1$ for at least one $p|n$ is again by Proposition 4 less than n^2/B^2. So it suffices to consider the pairs with $\left(\frac{D}{p}\right) = -1$ for all primes $p|n$. In this case the number of pairs is by Corollary 3 at most $(1/2^{4\omega-1})\prod(p_i-1)^2$. When adding these two cases, the probability is upper bounded by $1/2^{17} + 4/B^2$ which is less than $1/131040$. □

4.2 The Square Root Finding Based Part

It is well-known that when a is taken randomly from $\mathbb{Z}_n^*$, the probability for a to be a Miller-Rabin liar is at most 1/4. If $\left(\frac{a}{n}\right)$ is fixed to some special value (e.g., -1), then in that case there are only $\phi(n)/2$ such a as possible input values to the Miller-Rabin test. Yet, even for fixed jacobi symbol, we show below that in our case the failure rate is smaller than the expected 2/4.

The following result can immediately be verified.

Proposition 5. *Let n be spsp(u), where $\left(\frac{u}{n}\right) = -1$, and let p be any prime divisor of n. Then, if $\left(\frac{u}{p}\right) = -1$, we have $\nu_2(p-1) = \nu_2(n-1)$, and if $\left(\frac{u}{p}\right) = 1$, we have $\nu_2(p-1) > \nu_2(n-1)$.*

Notation: Let $\nu(n)$ denote the largest integer such that $2^{\nu(n)}$ divides $p-1$ for each prime p dividing n. As above, write $n-1 = 2^r s$ with s odd.

Proposition 6. *Suppose n is spsp(a) for $\left(\frac{a}{n}\right) = -1$. Then $a \in \mathcal{S}_{-1}(n)$ where $\mathcal{S}_{-1}(n) = \{a \bmod n :\ a^{2^{\nu(n)-1}s} \equiv -1 \bmod n\}$. Moreover, we have $\#\mathcal{S}_{-1}(n) = 2^{(\nu(n)-1)\omega(n)} \prod_{p|n} \gcd(s, p-1)$.*

Proof. If $\left(\frac{a}{n}\right) = -1$ then there exists $p|n$ with $\left(\frac{a}{p}\right) = -1$ and by Proposition 5, $\nu_2(p-1) = r = \nu(n)$. Moreover, in that case, $\nu_2(p-1) = \nu_2(\mathrm{ord}_p(a))$. By a standard result for n being *spsp*(a) (see e.g., [2]), we also have $\nu_2(\mathrm{ord}_p(a)) = \nu_2(\mathrm{ord}_q(a))$, so that $\nu_2(\mathrm{ord}_q(a)) = \nu(n)$ for any $q|n$. In particular, if $a^{2^i s} \equiv -1 \bmod n$ for some $0 \le i \le r-1$ (the first case for n being *spsp*(a)), then $a^{2^{\nu(n)-1}s} \equiv -1 \bmod q$ for any $q|n$. Note also that the case $a^s \equiv 1 \bmod n$ (the second case for n being *spsp*(a)), is impossible, since $a^{(n-1)/2} \equiv -1 \bmod n$ by hypothesis.

The cardinality $\#\mathcal{S}_{-1}(n)$ follows from [13, p. 128]. □

Lemma 6. *Suppose an odd composite integer n, not a perfect square, is not the product of exactly three prime factors. Let $a \in \mathbb{Z}_n^*$ be chosen randomly from the set of all b with $\left(\frac{b}{n}\right) = -1$. Then the probability that n is spsp(a) is given as follows. If $n = p_1 p_2$ where $p_1 = 2^k t + 1$ and $p_2 = 2^{k+1} t + 1$, $2 \not| t$, it is at most 1/4. Otherwise, it is at most 1/8.*

Proof. We follow the proof of Lemma 3.4.8. in [13]. Then the desired probability can be determined via

$$\frac{\phi(n)}{2\#\mathcal{S}_{-1}(n)} = \frac{1}{2} \prod_{p^\alpha || n} p^{\alpha-1} \frac{p-1}{2^{\nu(n)-1} \gcd(s, p-1)}.$$

Note that each factor $(p-1)/(2^{\nu(n)-1} \gcd(s, p-1))$ is an even integer. Then, if $\omega(n) \ge 4$, we have $\phi(n)/(2\#\mathcal{S}_{-1}(n)) \ge 1/2 \cdot (2^4) = 8$.

If $\omega(n) = 2$, we distinguish the following cases. Suppose $2^{\nu(n)+2} | p - 1$ for one $p|n$. Then $2^{\nu(n)-1} \gcd(s, p-1) \leq (p-1)/8$ and therefore $\phi(n)/(2\#\mathcal{S}_{-1}(n)) \geq 1/2 \cdot (2 \cdot 8) = 8$.

Now, let $2^{\nu(n)+\delta} | p-1$ for one $p|n$, where δ equals 0 or 1. Write the two primes in the form $p_1 = 2^{\nu(n)+\delta} t_1 + 1$ and $p_2 = 2^{\nu(n)} t_2 + 1$.

For the case that $t_1 \neq t_2$, Arnault [4, p. 877] showed that $t_1 | s$ and $t_2 | s$ is simultaneously impossible. This means that for at least one p_i, $\gcd(s, p_i - 1) \leq t_i/3$. If $\delta = 0$, then $\phi(n)/(2\#\mathcal{S}_{-1}(n)) \geq 1/2 \cdot (2 \cdot 6) = 6$, while if $\delta = 1$, this introduces an additional factor of 2, and $\phi(n)/(2\#\mathcal{S}_{-1}(n)) \geq 12$.

The result of the Lemma follows, since for $\left(\frac{Q}{n}\right) = -1$ and $\omega(n) = 2$ there is one prime factor p_i with $\left(\frac{Q}{p_i}\right) = 1$, so that by Proposition 5, $\nu_2(p_i - 1) > \nu_2(n-1) = \nu_2(p_j - 1) = \nu(n)$. This means we do have $\delta = 1$, as required.

Finally, the special case $p_1 = 2^k t + 1$ and $p_2 = 2^{k+1} t + 1$ implies $t|s$, in which case $\phi(n)/(2\#\mathcal{S}_j(n)) \geq 1/2 \cdot (2 \cdot 4)$, since $2^{\nu(n)+1} | p_2 - 1$. □

4.3 Proof of the Main Result

Proof of Theorem 1. Suppose firstly that n is a product of three different prime factors. Then Theorem 3 and Lemma 2, respectively Lemma 3, give the result.

For the Atkin-based root finding method Lemma 3 asserts that n is *spsp*$(2d^2)$. Since $\left(\frac{2d^2}{n}\right) = -1$ as $\left(\frac{2}{n}\right) = -1$ for $n \equiv 5 \bmod 8$, we can apply Lemma 6. By assumption, d is chosen randomly in the square root finding algorithm. For random selection of this basis, the condition on n to be *spsp*$(2d^2)$ is independent of the QF-based test.

If n is not such a special two-factor integer as described in Lemma 6, this introduces a factor of 1/8 (for each random d) in addition to the failure probability obtained above in Theorem 3 for the test that checks the QF-condition.

If n passes the Shanks-based method, it firstly is *spsp*(u) for u with $\left(\frac{u}{n}\right) = -1$. For randomly chosen u this again introduces a factor of 1/8 in the failure probability.

Finally, for both types of the root finding algorithms, if n does have the special two-factor form, then it follows easily that Proposition 4 introduces a much smaller failure rate than above (the corresponding number of the QF-liars, which is based on the quantities $\gcd(n+1, p \pm 1)$, becomes much smaller when the odd part of $p-1$ divides $n-1$). In total, for $\omega = 2$ the largest failure rate applies to the general type of two factor numbers.

Thus, we have the failure rate, for the first round, $F_1 = 1/2^{20} + 1/(2B^2)$, and for $k-1$ additional iterations, $F_1 \cdot (1/2^{17} + 4/B^2)^{k-1}$. For larger k the B proportion is negligible, so that for a total of k rounds we have failure approximately $1/(2^{20} \cdot 2^{17(k-1)}) = 1/2^{17k+3}$. □

5 Open Problems and Further Remarks

While with the much smaller failure rate of 1/1048350, our test has running time 4 times that of the Miller-Rabin test. We do not know how effectively the failure rate still can be reduced, when allowing more time for evaluation (for each round). On the other hand, the question is, how to optimally tackle the tradeoff between the reliability and the running time, and what the limits for a test with much larger running time are, so that it practically still makes sense.

Strong pseudoprimes with respect to at least 4 random bases exist very often. Below $n = 1000$ there are 54 such composites with at least four non-trivial bases as liars. Our test, without trial division and, for simplicity $d = 1$ (see Lemma 3) for $n \equiv 5 \bmod 8$, would for any possible pairs of parameters detect these.

Similarly, it is extremely easy to construct strong pseudoprimes with respect to at least 4^2, 4^3, ..., random bases. We do not know, computationally, how much more effort is required for the generation of pseudoprimes for the iterated proposed test (say, for the $n \equiv 5 \bmod 8$ algorithm with $d = 1$). Here, the typical Fermat/Lucas restrictions come into play and considerably limits the effectiveness of the Fermat- based generation methods for pseudoprimes.

On the other hand, sometimes it seems that many repeated iterations would not be necessary, if the input parameters have certain advantageous values. For the Miller-Rabin test, it is known that the bases $2, 3, 5, 7$ seem to work better, as they are primitive roots for most primes.

Even more effectively, the special choice of the parameters in the Baillie-PSW test essentially improves on its reliability.

If the proposed tests were run for one pair of parameters only, it is not known to what extent, and for which parameters it is most reliable.

Note added in proof: I. Damgård and G. Frandsen recently established a QF-based test with average case error estimates [15].

Acknowledgements. I am grateful to the following individuals, who were most helpful to me in writing this paper. In alphabetical order, they are: W. Bosma, H. Dobbertin, J. Grantham, A. Lenstra, W.B. Müller, and H.C. Williams. I would also like to thank the anonymous referees for their insightful remarks.

References

1. Adams, W., Shanks, D., Strong primality tests that are not sufficient. *Math. Comp.* **39**, 255-300 (1982).
2. Alford, W.R., Granville, A., Pomerance, C., On the difficulty of finding reliable witnesses. *Algorithmic Number Theory*, LNCS **877**, 1-16 (1994).
3. Arnault, F., Rabin-Miller primality test: Composite numbers which pass it. *Math. Comp.* **64**, no. 209, 355 - 361 (1995).
4. Arnault, F., The Rabin-Monier theorem for Lucas pseudoprimes. *Math. Comp.* **66**, 869 - 881 (1997).
5. Atkin, A.O.L., Probabilistic Primality Testing. *INRIA Res. Rep. 1779*, 159-163 (1992).

6. Atkin, A.O.L., Intelligent primality test offer. *Computational Perspectives on Number Theory* (D. A. Buell, J.T. Teitelbaum, eds.), Proceedings of a Conference in Honor of A.O.L. Atkin, International Press, 1-11 (1998).
7. Atkin, A.O.L., Morain, F., Elliptic curves and primality proving. *Math. Comp.* **61**, 29-68 (1993).
8. Baillie, R., Wagstaff, S.S., Lucas pseudoprimes. *Math. Comp.* **35**, 1391-1417 (1980).
9. Bleichenbacher, D., *Efficiency and Security of Cryptosystems based on Number Theory.* Dissertation ETH Zürich (1996).
10. Bosma, W., Van der Hulst, M.-P., Faster primality testing. *EUROCRYPT' 89*, LNCS **434**, 652-656 (1990).
11. Carmichael R.D., On sequences of integers defined by recurrence relations. *Quart. J. Pure Appl. Math.* **48**, 343-372 (1920).
12. Cohen, H., Lenstra H. W., Primality testing and Jacobi sums. *Math. Comp.* **42**, 297-330 (1984).
13. Crandall, R., Pomerance, C., Prime Numbers. A Computational Perspective. Springer-Verlag (2001).
14. Damgård, I., Landrock, P., Pomerance, C., Average case error estimates for the strong probable prime test. *Math. Comp.* **61**, no. 203, 177-194 (1993).
15. Damgård, I., Frandsen, G. S., An extended quadratic Frobenius primality test with average case error estimates. Draft, University of Aarhus, Denmark, August 31 (2001).
16. Grantham, J., A probable prime test with high confidence. *J. Number Theory* **72**, 32-47 (1998).
17. Jaeschke, G., On strong pseudoprimes to several bases. *Math. Comp.* **61**, 915-926, (1993).
18. Knuth, D., The Art of Computer Programming. Vol. 2/Seminumerical Algorithms. Addison-Wesley, 1997.
19. Kurtz G., Shanks, D., Williams, H.C., Fast primality tests for numbers less than $50 \cdot 10^9$. *Math. Comp.* **46**, 691-701 (1986).
20. A. K. Lenstra, H. W. Lenstra Jr., The Development of the Number Field Sieve. Springer-Verlag, Berlin, 1993.
21. Lindhurst, S., An analysis of Shank's Algorithm for computing square roots in finite fields. *CRM* Proceedings and Lecture Notes, Vol. 19, 231-242 (1999).
22. Menezes, A., van Oorschot, P.C., Vanstone, S., Handbook of Applied Cryptography. CRC (1997).
23. Montgomery, P., Evaluating recurrences of form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains. Preprint.
24. More, W., The LD probable prime test. *Contemporary Mathematics*, **225**, 185-191 (1999).
25. Müller, S., On the combined Fermat/Lucas probable prime test. In: Walker, M. (ed.) *Cryptography and Coding*, LNCS **1746**, Springer - Verlag, 222-235 (1999).
26. Müller, S., On probable prime testing and the computation of square roots mod n. *Algorithmic Number Thory*, ANTS IV, Proceedings, Wieb Bosma (ed.), LNCS **1838**, 423-437 (2000).
27. Müller, S., On the rank of appearance and the number of zeros of the Lucas sequences over F_q. *Finite Fields and Applications*, H. Niederreiter, A. Enge (eds.), 390-408, Springer (2001).
28. Müller, S., A probable prime test with very high confidence for $n \equiv 3 \bmod 4$. Submitted.

29. Müller, S., On probable prime testing and Shanks' root finding algorithm. Preprint, University of Klagenfurt 2001.
30. Pinch, R. G. E., Some primality testing algorithms. Preprint (1993).
31. Pomerance, C., Are there counter-examples to the Baillie-PSW primality test? In: Lenstra, A.K. (ed.) Dopo Le Parole aangeboden aan Dr. A. K. Lenstra. Privately published Amsterdam (1984).
32. C. Pomerance, The number field sieve. *Proceedings of Symposia in Applied Mathematics,* Vol. **48**, pp. 465–480 (1994).
33. Pomerance, C., Selfridge, J. L., Wagstaff, S.S., Jr., The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.* **35**, no. 151, 1003–1026 (1980).
34. Postl, H., Fast evaluation of Dickson Polynomials. *Contrib. to General Algebra* **6**, 223-225 (1988).
35. Riesel, H., Prime Numbers and Computer Methods for Factorization. Birkhäuser (1994).
36. Ribenboim, P., *The New Book of Prime Number Records.* Berlin, Springer (1996).
37. Shoup, V., Primality testing with fewer random bits. *Computational Complexity* **3**, 355–367 (1993).
38. Shanks, D., Five number-theoretic algorithms. *Proc. of the second Manitoba Conf. on numerical mathematics*, Thomas, R.S.D., Williams, H.C. (eds.), 51-70 (1972).
39. Somer, L., On Lucas d-Pseudoprimes. In: *Applications of Fibonacci Numbers, Volume 7*, Bergum G.E., Philippou, A.N., Horadam, A.F. (eds.), Kluwer, 369-375, (1998).
40. Williams, H.C., A $p + 1$ method of factoring. *Math. Comp.* **39**, no. 159, 225–234 (1982).
41. Williams, H.C., *Éduard Lucas and Primality Testing.* John Wiley & Sons (1998).