MATHEMATICS OF COMPUTATION
Volume 71, Number 240, Pages 1699–1734
S 0025-5718(02)01424-2
Article electronically published on May 16, 2002

A ONE-PARAMETER QUADRATIC-BASE VERSION OF THE BAILLIE-PSW PROBABLE PRIME TEST

ZHENXIANG ZHANG

ABSTRACT. The well-known Baillie-PSW probable prime test is a combination of a Rabin-Miller test and a "true" (i.e., with $(D/n) = -1$) Lucas test. Arnault mentioned in a recent paper that no precise result is known about its probability of error. Grantham recently provided a probable prime test (RQFT) with probability of error less than 1/7710, and pointed out that the lack of counter-examples to the Baillie-PSW test indicates that the true probability of error may be much lower.

In this paper we first define pseudoprimes and strong pseudoprimes to quadratic bases with one parameter: $T_u = T \mod (T^2 - uT + 1)$, and define the base-counting functions:

$$\mathrm{B}(n) = \#\{u : 0 \le u < n,\ n \text{ is a psp}(T_u)\}$$

and

$$\mathrm{SB}(n) = \#\{u : 0 \le u < n,\ n \text{ is an spsp}(T_u)\}.$$

Then we give explicit formulas to compute $\mathrm{B}(n)$ and $\mathrm{SB}(n)$, and prove that, for odd composites n,

$$\mathrm{B}(n) < n/2 \text{ and } \mathrm{SB}(n) < n/8,$$

and point out that these are best possible. Finally, based on one-parameter quadratic-base pseudoprimes, we provide a probable prime test, called the One-Parameter Quadratic-Base Test (OPQBT), which passed by all primes ≥ 5 and passed by an odd composite $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ ($p_1 < p_2 < \cdots < p_s$ odd primes) with probability of error $\tau(n)$. We give explicit formulas to compute $\tau(n)$, and prove that

$$\tau(n) < \begin{cases} 1/n^{4/3}, & \text{for } n \text{ nonsquare free with } s = 1; \\ 1/n^{2/3}, & \text{for } n \text{ square free with } s = 2; \\ 1/n^{2/7}, & \text{for } n \text{ square free with } s = 3; \\ \frac{1}{8^{s-4} \cdot 166(p_1+1)}, & \text{for } n \text{ square free with } s \text{ even} \ge 4; \\ \frac{1}{16^{s-5} \cdot 119726}, & \text{for } n \text{ square free with } s \text{ odd} \ge 5; \\ \frac{1}{4^s} \prod_{i=1}^{s} \frac{1}{p_i^{2(r_i-1)}}, & \text{otherwise, i.e., for } n \text{ nonsquare free with } s \ge 2. \end{cases}$$

The running time of the OPQBT is asymptotically 4 times that of a Rabin-Miller test for worst cases, but twice that of a Rabin-Miller test for most composites. We point out that the OPQBT has clear finite group (field) structure and nice symmetry, and is indeed a more general and strict version of the Baillie-PSW test. Comparisons with Gantham's RQFT are given.

Received by the editor August 14, 2000.

2000 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A51, 11R11.

Key words and phrases. Baillie-PSW probable prime test, Rabin-Miller test, Lucas test, probability of error, (strong) (Lucas) pseudoprimes, quadratic integers, base-counting functions, finite groups (fields), Chinese Remainder Theorem.

Supported by the China State Educational Commission Science Foundation, the NSF of China Grant 10071001, the SF of Anhui Province Grant 01046103, and the SF of the Education Department of Anhui Province Grant 2002KJ131.

1. Introduction

Pseudoprimes, Lucas pseudoprimes, and their strong versions have long been studied as special cases in simple primality tests for large numbers [2, 4, 5, 6, 9, 10, 15, 19, 23]. If n is prime, then for every rational integer b with $\gcd(n, b) = 1$,

$$b^{n-1} \equiv 1 \mod n, \tag{1.1}$$

and

$$\text{either } b^q \equiv 1 \mod n \text{ or } b^{2^i q} \equiv -1 \mod n \text{ for some } i = 0, 1, \cdots, k-1, \tag{1.2}$$

where we write $n - 1 = 2^k q$ with q odd. If n is composite such that (1.1) holds then we call n a pseudoprime to base b, or psp(b) for short. There are composite integers, called Carmichael numbers, such that (1.1) holds for every b with $\gcd(n, b) = 1$. Alford, Granville and Pomerance [1] proved that there are infinitely many Carmichael numbers. If (1.2) holds, then we say that n passes the Rabin-Miller (strong probable prime) test [15] to base b; if in addition, n is composite, then we say n is a strong pseudoprime to base b, or spsp(b) for short.

Monier [16] gave a formula for counting the number of bases b such that n is an spsp(b). Both Rabin [20] and Monier [16] proved that if n is an odd composite positive integer, then n passes the Rabin-Miller test for at most $(n-1)/4$ bases b with $1 \le b \le n-1$.

We shall use both $|\ |$ and $\#$ to denote cardinality of a set, reserving the latter symbol for sets written with braces. Jacobi's symbol is denoted by $\left(\frac{*}{n}\right)$ or $(*/n)$ with n odd.

Lucas pseudoprimes and strong Lucas pseudoprimes are traditionally defined via Lucas sequences with two parameters. Let P and Q be integers and $D = P^2 - 4Q \neq 0$. The Lucas sequences U_i and V_i are defined by

$$\begin{gathered} U_0 = 0,\ U_1 = 1,\ V_0 = 2,\ V_1 = P, \\ U_i = PU_{i-1} - QU_{i-2},\ V_i = PV_{i-1} - QV_{i-2} \text{ for } i \ge 2. \end{gathered} \tag{1.3}$$

If n is prime and relatively prime to $2QD$, then

$$U_{n-(D/n)} \equiv 0 \mod n, \tag{1.4}$$

and

$$\text{either } n \mid U_q \text{ or } n \mid V_{2^i q} \text{ for some } i \text{ with } 0 \le i < k, \tag{1.5}$$

where we write $n - (D/n) = 2^k q$ with q odd. If n is composite and relatively prime to $2QD$ such that condition (1.4) or (1.5) holds, then we call n a Lucas pseudoprime [4, 19] or a strong Lucas pseudoprime [3, 4] to parameters P and Q, or lpsp(P, Q) or slpsp(P, Q) for short.

Let D be an integer, and n a composite number relatively prime to $2D$ and distinct from 9. Arnault [3] gave a formula to compute the base-counting function

$$\mathrm{SL}(D, n) = \#\{(P, Q) : 0 \le P, Q < n, P^2 - 4Q \equiv D \mod n,\ n \text{ is an slpsp}(P, Q)\}, \tag{1.6}$$

and proved that, for all integers D,

$$\mathrm{SL}(D, n) \le 4n/15, \tag{1.7}$$

except if n is the product $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$ of twin primes with q_1 odd and such that the Legendre symbols satisfy $(D/2^{k_1}q_1 - 1) = -1, (D/2^{k_1}q_1 + 1) = 1$. Also the following inequality is always true:

$$\mathrm{SL}(D, n) \leq n/2. \tag{1.8}$$

A prp (sprp, lprp, slprp) is either a prime or a psp (spsp, lpsp, slpsp).

Baillie, Pomerance, Selfridge and Wagstaff [4, 19] suggested a probable prime test which is a combination of a Rabin-Miller test and a "true" (i.e., with $(D/n) = -1$) Lucas test, and which seems much more secure than one might expect considering each test separately. Although Pomerance [18] gave a heuristic argument to show that the number of counter-examples up to x to the Baillie-PSW test is $\gg x^{1-\delta}$ for any $\delta > 0$, not a single counter-example has yet been found. As mentioned by Arnault at the end of his paper [3], no precise result is known about its probability of error.

Grantham [9] provided a probable prime test (RQFT) using quadratic polynomials with two parameters, the running time of which is asymptotically 3 times that of the Rabin-Miller test for all composites. The RQFT, along with a fixed number of trial divisions, is passed by composites with probability of error less than 1/7710. Grantham [9] pointed out that the lack of counter-examples to the Baillie-PSW test indicates that the true probability of error may be much lower.

In this paper we provide a version of the Baillie-PSW test (OPQBT) based on strong pseudoprimes to quadratic bases with one parameter in the ring

$$\mathbb{Z}[T]/(T^2 - uT + 1).$$

We state our definitions and main results (Theorems $1-5$) in Section 2. In Sections $3-7$ we prove the five theorems. Comparisons with Grantham's RQFT are given in Section 8. Brief conclusions are given in Section 9.

Remark 1.1. The ring $\mathbb{Z}[T]/(T^2 - uT + 1)$ was first used by the author for factoring large integers near group orders [24]. The idea of using this ring in primality testing is motivated from the Lucas-Lehmer Test described in [7, 8], where the ring $\mathbb{Z}[T]/(T^2 - uT - 1)$ was used. Lenstra's Galois Theory Test [14] is a method of proving primality using finite fields.

2. Definitions and main results

Let $u\ (\neq \pm 2) \in \mathbb{Z}$. Put $T_u = T \mod (T^2 - uT + 1)$ and

$$R_u = \mathbb{Z}[T]/(T^2 - uT + 1) = \{a + bT_u : a, b \in \mathbb{Z}\}, \tag{2.1}$$

a ring of quadratic algebraic integers associated with the parameter u.

Given an odd integer $n > 1$, let u be an integer with

$$0 \leq u < n \quad \text{and} \quad \varepsilon = \left(\frac{u^2 - 4}{n}\right) \in \{1, -1\}.$$

It is clear that if n is prime, then we have, in the ring R_u,

$$T_u^{n-\varepsilon} \equiv 1 \mod n, \tag{2.2}$$

and

$$\text{either } T_u^q \equiv 1 \mod n \text{ or } T_u^{2^i q} \equiv -1 \mod n \text{ for some } i = 0, 1, \cdots, k-1, \tag{2.3}$$

where we write $n-\varepsilon = 2^k q$ with q odd. There are composites which satisfy (2.2) or both conditions (note that (2.3) implies (2.2)). These facts lead us to make the following definition.

Definition 2.1. If n is composite such that (2.2) holds, then we call n a pseudoprime to the base T_u, or psp(T_u) for short. If n is composite such that (2.3) holds, then we call n a strong pseudoprime to the base T_u, or spsp(T_u) for short. A prp(T_u) is a prime or a psp(T_u); an sprp(T_u) is a prime or an spsp(T_u). For odd $n > 3$ and $\varepsilon \in \{1, -1\}$, define the base-counting functions:

$$\text{B}(n,\varepsilon) = \#\left\{u : 0 \le u < n, \left(\frac{u^2-4}{n}\right) = \varepsilon, \text{ and (2.2) holds}\right\}, \tag{2.4}$$

$$\text{SB}(n,\varepsilon) = \#\left\{u : 0 \le u < n, \left(\frac{u^2-4}{n}\right) = \varepsilon, \text{ and (2.3) holds}\right\}, \tag{2.5}$$

$$\text{B}(n) = \text{B}(n,1) + \text{B}(n,-1) = \#\{u : 0 \le u < n,\ n \text{ is a psp}(T_u)\}, \tag{2.6}$$

$$\text{SB}(n) = \text{SB}(n,1) + \text{SB}(n,-1) = \#\{u : 0 \le u < n,\ n \text{ is an spsp}(T_u)\}, \tag{2.7}$$

$$\begin{cases} \tau_0(n,\varepsilon) = \frac{\text{B}(n,\varepsilon)}{(n-\varepsilon-2)/2},\ \tau(n,\varepsilon) = \frac{\text{SB}(n,\varepsilon)}{(n-\varepsilon-2)/2}, \\ \tau_0(n) = \tau_0(n,1)\tau_0(n,-1), \text{ and } \tau(n) = \tau(n,1)\tau(n,-1). \end{cases} \tag{2.8}$$

Note that an spsp(T_u) must be a psp(T_u). Thus we have

$$\text{SB}(n,\varepsilon) \le \text{B}(n,\varepsilon),\ \text{SB}(n) \le \text{B}(n),\ \tau(n,\varepsilon) \le \tau_0(n,\varepsilon), \text{ and } \tau(n) \le \tau_0(n). \tag{2.9}$$

Let $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ be the prime decomposition of odd $n > 1$. For $\varepsilon \in \{1, -1\}$ and $1 \le i \le s$, write

$$p_i - \varepsilon = 2^{k_{i,\varepsilon}} q_{i,\varepsilon} \text{ with } q_{i,\varepsilon} \text{ odd, and } n - \varepsilon = 2^{k_\varepsilon} q_\varepsilon \text{ with } q_\varepsilon \text{ odd.} \tag{2.10}$$

For $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s \in \{1, -1\}$, put

$$m(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s) = \min\{k_{i,\varepsilon_i} : 1 \le i \le s\}. \tag{2.11}$$

It is clear that there exists one and only one s-tuple $(e_1, e_2, \cdots, e_s)$ with $m(e_1, e_2, \cdots, e_s) \ge 2$, and that $m(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s) = 1$ for all other $2^s - 1$ s-tuples $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s)$.

Definition 2.2. Given an odd $n \ge 5$. The One-Parameter Quadratic-Base Test (*OPQBT*) consists of the following:

Step 1 (*Nonperfect square pretest*). Check if n is a perfect square using Newton's method. If it is, declare n to be composite and stop.

Step 2 (*First sprp subtest*). Select a random integer u with $0 \le u < n, u \ne \pm 2 \bmod n$ and $\gcd(u^2-4, n) = 1$. Put $\varepsilon = \left(\frac{u^2-4}{n}\right)$; then $\varepsilon \in \{1, -1\}$. If n is not an sprp(T_u), i.e., condition (2.3) does not hold, declare n to be composite and stop.

Step 3 (*Second sprp subtest*). Select several random integers v with $0 \le v < n, v \ne \pm 2 \bmod n$, until one finds a v with $\left(\frac{v^2-4}{n}\right) = -\varepsilon$. (By Lemma 6.1 in Section 6, it is easy to find such a v, since n is not a perfect square.) If n is not an sprp(T_v), declare n to be composite and stop.

If n is not declared composite in Steps 1–3, declare n to be a strong probable prime, and say that n passes (one iteration of) the OPQBT.

With the above notations and definitions we state our main results as the following five theorems.

Theorem 1. *We have, for odd $n > 1$ and $\varepsilon \in \{1, -1\}$,*

$$\mathrm{B}(n,\varepsilon) = \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}} \prod_{i=1}^{s}\left(\frac{\gcd(n-\varepsilon, p_i-\varepsilon_i)}{2} - 1\right), \tag{2.12}$$

and

$$\mathrm{SB}(n,\varepsilon) = \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}} \left(2\prod_{i=1}^{s}\frac{\gcd(q_\varepsilon, q_{i,\varepsilon_i})-1}{2} + \frac{2^{s(m-1)}-1}{2^s-1}\prod_{i=1}^{s}\gcd(q_\varepsilon, q_{i,\varepsilon_i})\right), \tag{2.13}$$

where $m = m(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s)$, as defined in (2.11).

Theorem 2. *We have, for odd positive composite n (i.e., $s \geq 2$ or $r_1 \geq 2$),*

$$\mathrm{B}(n) < n/2 \quad \textit{and} \quad \mathrm{SB}(n) < n/8. \tag{2.14}$$

Theorem 3. *We have, for odd positive composite n (i.e., $s \geq 2$ or $r_1 \geq 2$),*

$$\tau_0(n) < \begin{cases} 1/n^{4/3}, & \textit{for } n \textit{ nonsquare free with } s = 1;\\ 1/n^{2/3}, & \textit{for } n \textit{ square free with } s = 2;\\ 1/n^{2/7}, & \textit{for } n \textit{ square free with } s = 3;\\ \frac{2}{p_1+1}, & \textit{for } n \textit{ square free with } s \textit{ even} \geq 4;\\ \frac{1}{4^{s-1}}\prod_{i=1}^{s}\frac{1}{p_i^{2(r_i-1)}}, & \textit{otherwise;} \end{cases} \tag{2.15}$$

and

$$\tau(n) \leq \begin{cases} \tau_0(n), & \textit{for } n \textit{ nonsquare free with } s = 1\\ & \textit{or } n \textit{ square free with } s = 2, 3;\\ \frac{1}{8^{s-4}\cdot 166(p_1+1)}, & \textit{for } n \textit{ square free with } s \textit{ even} \geq 4;\\ \frac{1}{16^{s-5}\cdot 119726}, & \textit{for } n \textit{ square free with } s \textit{ odd} \geq 5;\\ \frac{1}{4^s}\prod_{i=1}^{s}\frac{1}{p_i^{2(r_i-1)}}, & \textit{otherwise, i.e., for } n \textit{ nonsquare free with } s \geq 2. \end{cases} \tag{2.16}$$

Theorem 4. *The OPQBT is always passed by primes ≥ 5, and passed by odd composites with probability of error $\tau(n)$.*

Theorem 5. *It takes $(2 + o(1))\log_2 n$ multiplications* mod n *to do an sprp test in Step 2 or 3, assuming that addition takes $o(1)$ multiplications* mod n. *Thus (an iteration of) the One-Parameter Quadratic-Base Test can be completed in the time it takes to perform at most $(4 + o(1))\log_2 n$ multiplications* mod n.

Remark 2.1. If n is a psp(b) (resp. an spsp(b)), then n is a psp(T_u) (resp. an spsp(T_u)) with $u = b + b^{-1} \mod n$. If n is a psp(T_u) (resp. an spsp(T_u)), n is not necessary a psp (resp. an spsp) to a rational base even if $\left(\frac{u^2-4}{n}\right) = 1$, unless $\left(\frac{u^2-4}{p}\right) = 1$ for every prime factor p of n. In particular, n is a psp(2) $\Longleftrightarrow$ n is a psp($T_{(n+5)/2}$).

Remark 2.2. If n is a psp(T_u), then n is an lpsp$(u,1)$ and an lpsp$(1,Q)$ with $Q = u^{-2} \mod n$ if $\gcd(u,n) = 1$. But the converse is not true. For examples, both 21 and 329 are lpsp$(3,1)$, but neither is a psp(T_3). There are 155 psp(T_3)'s among 279 lpsp$(3,1)$'s $< 10^6$. Arnault [3] and Grantham [9, 10] cited a preprint of Mo and Jones, who introduced a test via slpsp$(u,1)$, which has probability of error $< 1/8$. So far I have not been able to access the preprint. I sent e-mails to Jones for a copy, he replied that they were still working on it.

Remark 2.3. There are 4152 psp(T_3)'s $< 10^9$, among which 1165 numbers are spsp(T_3)'s.

Remark 2.4. Can $B(n)/n$ be arbitrarily close to $1/2$? The answer would be affirmative, if there are Carmichael numbers n with a fixed number of prime factors with the smallest factor arbitrarily large, and with the stronger requirement that $p \mid n$ implies $(p^2-1) \mid (n-1)$. Alford, Granville and Pomerance [1] have proved that there are infinitely many Carmichael numbers with the stronger requirement that $p \mid n$ implies $(p^2-1) \mid (n-1)$ (also cf. [11, A13]), but no one has yet been able to show that there are infinitely many Carmichael numbers n with a fixed number of prime factors.

Remark 2.5. If there are infinitely many pairs of twin primes p_1 and $p_2 = p_1 + 2$ with $p_1 \equiv 1 \mod 4$, then $\frac{SB(p_1p_2)}{p_1p_2}$ will be arbitrarily close to $1/8$, cf. Example 3.1 in Section 3 and the proof of Lemma 4.5 in Section 4.

3. Proof of Theorem 1

Let p be an odd prime, $k\ (\geq 1) \in \mathbb{Z}$, and $G(u,p^k)$ the multiplicative group of invertible elements of the ring

$$R_u/(p^k) = \{a + bT_{u,p^k} : a,b \in \mathbb{Z}/(p^k)\} \tag{3.1}$$

with $0 \leq u < p^k$, $\left(\frac{u^2-4}{p}\right) \in \{1,-1\}$ and $T_{u,p^k} = T_u \mod p^k$.

For $\varepsilon \in \{1,-1\}$ and a positive odd integer q, define

$$J(q,\varepsilon) = \#\left\{u : 0 \leq u < q, \left(\frac{u^2-4}{q}\right) = \varepsilon\right\}. \tag{3.2}$$

To prove Theorem 1 we need six lemmas.

Lemma 3.1. *Let p be an odd prime. Then*

$$J(p,0) = 2,\ J(p,\varepsilon) = (p-\varepsilon-2)/2 = \begin{cases} (p-1)/2, & \text{for } \varepsilon = -1, \\ (p-3)/2, & \text{for } \varepsilon = 1. \end{cases}$$

Proof. It is well known [12] that

$$\sum_{u=0}^{p-1}\left(\frac{u^2-4}{p}\right) = -1.$$

Since $J(p,0) = 2$, we have $J(p,-1) = (p-1)/2$ and $J(p,1) = (p-3)/2$. □

Lemma 3.2. *Let p be an odd prime and $\varepsilon \in \{1,-1\}$. If $J(p,\varepsilon) > 0$, then there exists an integer u such that $0 \leq u < p$, $\left(\frac{u^2-4}{p}\right) = \varepsilon$, and $T_{u,p}$ is of order $p-\varepsilon$ in the group $G(u,p)$.*

Proof. Case $\varepsilon = 1$. It is well known that the multiplicative group $GF^*(p) = (\mathbb{Z}/(p))^*$, of nonzero elements of the finite field $GF(p) = \mathbb{Z}/(p)$, is cyclic, of order $p-1$. Let θ be one of its generators. Then θ is of order $p-1$. Since $J(p,1) > 0$, it follows that $p-1 > 2$ and $\theta \neq \theta^{-1}$. Put $u = \theta + \theta^{-1} \in \mathbb{Z}/(p)$; then

$$0 \leq u < p, \left(\frac{u^2-4}{p}\right) = \left(\frac{(\theta-\theta^{-1})^2}{p}\right) = 1 \text{ and } \theta^2 - u\theta + 1 \equiv 0 \mod p.$$

The lemma follows.

Case $\varepsilon = -1$. It is well known that the multiplicative group $GF^*(p^2)$ of nonzero elements of the finite field $GF(p^2)$ is cyclic, of order p^2-1. Let θ be one of its generators. Put $\alpha = \theta^{p-1}$. Then α is of order $p+1$. Put $u = \alpha + \alpha^{-1} = \alpha + \alpha^p \in \mathbb{Z}/(p)$; then

$$0 \leq u < p,\ \alpha^2 - u\alpha + 1 \equiv 0 \mod p \text{ and } \left(\frac{u^2-4}{p}\right) = -1.$$

The lemma follows. □

Lemma 3.3. *Let* p *be an odd prime,* $k\ (\geq 2) \in \mathbb{Z}$, *and* $\varepsilon \in \{1,-1\}$. *If* $J(p,\varepsilon) > 0$, *then there exists an integer* u *such that*

$$0 \leq u < p^2, \left(\frac{u^2-4}{p}\right) = \varepsilon,$$

and T_{u,p^k} *is of order* $p^{k-1}(p-\varepsilon)$ *in the group* $G(u,p^k)$.

Proof. By Lemma 3.2, there exists an integer v such that $0 \leq v < p, \left(\frac{v^2-4}{p}\right) = \varepsilon$, and $\alpha = T_{v,p}$ is of order $p-\varepsilon$ in the group $G(v,p)$, with $\alpha^2 - v\alpha + 1 \equiv 0 \mod p$. Put $\alpha_1 = v - \alpha = \alpha^{-1} \mod p$, the other root of $x^2 - vx + 1 \equiv 0 \mod p$.

Case $\varepsilon = 1$. If $\alpha^{p-1} \neq 1 \mod p^2$, take

$$\beta = \alpha \text{ and } \beta_1 = \alpha_1 + hp \text{ with } h = \alpha_1 \frac{1-\alpha\alpha_1}{p} \mod p;$$

otherwise take

$$\beta = \alpha + p,\ \beta_1 = \alpha_1 + hp \text{ with } h = -\alpha_1\left(\alpha_1 + \frac{\alpha\alpha_1 - 1}{p}\right) \mod p.$$

We have $\beta\beta_1 \equiv 1 \mod p^2$. Let $u = \beta + \beta_1 \mod p^2$.

Case $\varepsilon = -1$. If $\alpha^{p+1} \neq 1 \mod p^2$, take $\beta = \alpha$ and $u = v$; otherwise take

$$\beta \equiv \frac{\alpha+p}{|\,\alpha+p\,|} \equiv (a+p)(1-2^{-1}vp) \equiv (1-2^{-1}vp)\alpha + p \mod p^2,$$

$$\beta_1 \equiv (1-2^{-1}vp)\alpha_1 + p \mod p^2,$$

and

$$u = \beta + \beta_1 = (1-2^{-1}vp)v + 2p \mod p^2,$$

where 2^{-1} stands for $2^{-1} \mod p$. Then

$$\begin{aligned}\beta^{p+1} &\equiv (\alpha+p)^{p+1}(1-2^{-1}vp)^{p+1} \equiv 1 + \alpha^p p - 2^{-1}vp \\ &\equiv 1 + (2^{-1}v - \alpha)p \neq 1 \mod p^2.\end{aligned}$$

In both cases ($\varepsilon = 1$ and $\varepsilon = -1$), we have

$$0 \le u < p^2, \ \left(\frac{u^2-4}{p}\right) = \varepsilon, \text{ and } \beta^2 - u\beta + 1 \equiv 0 \mod p^2.$$

Write $\beta^{p-\varepsilon} = 1 + \gamma p$ with $p \nmid \gamma$. By induction on k it is easy to prove that $1 + \gamma p \pmod{p^k}$ is of order p^{k-1}. Thus $\beta^{p^{k-1}(p-\varepsilon)} \equiv 1 \mod p^k$. To prove that the order of $\beta \pmod{p^k}$ is $p^{k-1}(p-\varepsilon)$, it is sufficient to prove that

$$\text{if } \beta^m \equiv 1 \mod p^k, \text{ then } p^{k-1}(p-\varepsilon) \mid m.$$

Since $(1+\gamma p)^m = \beta^{(p-\varepsilon)m} \equiv 1 \mod p^k$, we have $p^{k-1} \mid m$. Write $m = p^{k-1}m'$. Since $\beta \ (\equiv \alpha) \pmod{p}$ is of order $p - \varepsilon$, $\beta^p \equiv \beta^\varepsilon \mod p$. Thus $1 \equiv \beta^m = \left(\beta^{p^{k-1}}\right)^{m'} \equiv \left(\beta^{m'}\right)^{\varepsilon^{k-1}} \mod p$, and therefore $\beta^{m'} \equiv 1 \mod p$. We have $(p-\varepsilon) \mid m'$ and $p^{k-1}(p-\varepsilon) \mid m$, as required. The lemma follows. □

Lemma 3.4. *Let p be an odd prime, $k \ (\ge 1) \in \mathbb{Z}$, and $\varepsilon \in \{1, -1\}$ with $J(p, \varepsilon) > 0$. Let an integer u be such that $\left(\frac{u^2-4}{p}\right) = \varepsilon$ and T_{u,p^k} is of order $p^{k-1}(p-\varepsilon)$ in the group $G(u, p^k)$ (cf. Lemma 3.3). Let $\xi \in R_u/(p^k)$, and let H be the cyclic (sub-) group generated by T_{u,p^k}. Then the necessary and sufficient condition for*

$$\xi \in H \text{ and } \xi \ne \pm 1 \mod p$$

is that

$$\xi^2 - w\xi + 1 \equiv 0 \mod p^k \text{ for some integer } w \text{ with } 0 \le w < p^k \text{ and } \left(\frac{w^2-4}{p}\right) = \varepsilon.$$

Proof. Put $\beta = T_{u,p^k}$. Then $H = (\beta)$ is of order $p^{k-1}(p-\varepsilon)$. If $\xi \in H$, then $\xi = \beta^t$ for some integer t. Let $w = \xi + \xi^{-1} \equiv \beta^t + \beta^{-t} \mod p^k$. Then $0 \le w < p^k$ and $\xi^2 - w\xi + 1 \equiv 0 \mod p^k$. Put

$$A = \{\xi : \xi \in H \text{ and } \xi \ne \pm 1 \mod p\}$$

and

$$B = \{w : 0 \le w < p^k, \ \xi^2 - w\xi + 1 \equiv 0 \mod p^k \text{ for some } \xi \in A\}.$$

Then $|A| = p^{k-1}(p-\varepsilon-2)$ and $|B| = |A|/2 = p^{k-1}(p-\varepsilon-2)/2$. Put

$$C = \left\{w : 0 \le w < p^k, \left(\frac{w^2-4}{p}\right) = \varepsilon\right\}.$$

By induction on j, we see that

$$\beta^j - \beta^{-j} = (\beta - \beta^{-1})(\beta^{j-1} + \beta^{-(j-1)}) + \beta^{j-2} - \beta^{-(j-2)} = a_j(\beta - \beta^{-1}) \tag{3.3}$$

for some $a_j \in \mathbb{Z}/(p^k)$.

If $w \in B$, then there exists a $\xi \in H$ such that $\xi \ne \pm 1 \pmod{p}$ and $\xi^2 - w\xi + 1 \equiv 0 \mod p^k$. Since $\xi \ne \pm 1 \pmod{p}$, $\xi \ne \xi^{-1} \pmod{p}$. Thus $\gcd(\xi - \xi^{-1}, p) = 1$ and

$$\left(\frac{w^2-4}{p}\right) = \left(\frac{(\xi+\xi^{-1})^2-4}{p}\right) = \left(\frac{(\xi-\xi^{-1})^2}{p}\right) = \left(\frac{(\beta-\beta^{-1})^2}{p}\right) = \left(\frac{u^2-4}{p}\right) = \varepsilon$$

by (3.3). Therefore $w \in C$. This means that $B \subseteq C$. On the other hand, $| C | = p^{k-1}(p - \varepsilon - 2)/2 = | B |$ by Lemma 3.1. Thus $C = B$, and the lemma follows. □

Lemma 3.5. *Let p be an odd prime, k $(\geq 1) \in \mathbb{Z}$, $\varepsilon \in \{1, -1\}$, and m a positive integer with* $\gcd(m, p) = 1$. *Put*

$$X(p^k, \varepsilon, m) = \#\left\{u : 0 \leq u < p^k, \left(\frac{u^2 - 4}{p}\right) = \varepsilon,\ T_u^m \equiv 1 \mod p^k\right\}. \tag{3.4}$$

Then

$$X(p^k, \varepsilon, m) = \begin{cases} \frac{\gcd(p-\varepsilon, m)}{2} - 1, & \text{for } m \text{ even,} \\ \frac{\gcd(p-\varepsilon, m)-1}{2}, & \text{for } m \text{ odd.} \end{cases}$$

Proof. If $J(p, \varepsilon) = 0$, then $p = 3$, $\varepsilon = 1$ and $X(3^k, 1, m) = 0$, so the lemma is valid.

Now suppose $J(p, \varepsilon) > 0$. By Lemmas 3.2 and 3.3 there exists an integer v such that

$$0 \leq v < p^2, \quad \left(\frac{v^2 - 4}{p}\right) = \varepsilon,$$

and T_{v,p^k} is of order $p^{k-1}(p - \varepsilon)$ in the group $G(v, p^k)$. Put

$$d = \gcd(p^{k-1}(p - \varepsilon), m) = \gcd(p - \varepsilon, m);$$
$$h = p^{k-1}(p - \varepsilon)/d; \text{ and } \beta = T_{v,p^k} = T_v \mod p^k.$$

Since $H = (\beta)$ is a cyclic group of order $p^{k-1}(p - \varepsilon)$, the equation $x^m \equiv 1 \mod p^k$ has exactly d solutions in H : $\beta^h, \beta^{2h}, \cdots, \beta^{dh} = 1$, including $\pm 1 \pmod{p^k}$ for m even or including $+1 \pmod{p^k}$ for m odd. Since both β^{ih} and $\beta^{(d-i)h}$ satisfy the same equation

$$y^2 - u_i y + 1 \equiv 0 \mod p^k,$$

where

$$u_i = \beta^{ih} + \beta^{(d-i)h} \mod p^k,$$

and the $u_i \pmod{p^k}$ are distinct for $1 \leq i < d/2$, we have, by Lemma 3.4,

$$X(p^k, \varepsilon, m) = \begin{cases} \frac{d-2}{2} = \frac{\gcd(p-\varepsilon, m)}{2} - 1, & \text{for } m \text{ even,} \\ \frac{d-1}{2} = \frac{\gcd(p-\varepsilon, m)-1}{2}, & \text{for } m \text{ odd.} \end{cases}$$

□

Lemma 3.6. *Let p be an odd prime, k $(\geq 1) \in \mathbb{Z}$, $\varepsilon \in \{1, -1\}$, $p - \varepsilon = 2^r t$ with t odd, and q a positive odd integer with* $\gcd(q, p) = 1$. *For $i \geq 0$, put*

$$Y_i(p^k, \varepsilon, q) = \#\left\{u :\ 0 \leq u < p^k,\ \left(\frac{u^2 - 4}{p}\right) = \varepsilon,\ T_u^{2^i q} \equiv -1 \mod p^k\right\}.$$

Then

$$Y_i(p^k, \varepsilon, q) = \begin{cases} \frac{\gcd(q,t)-1}{2}, & \text{for } i = 0; \\ 2^{i-1}\gcd(q, t), & \text{for } 1 \leq i < r; \\ 0, & \text{for } i \geq r. \end{cases}$$

Proof. If $J(p,\varepsilon)=0$, then $p=3,\varepsilon=1,r=t=1$ and $Y_i(3^k,1,q)=0$ for $i\geq 0$, so the lemma is valid.

Now suppose $J(p,\varepsilon)>0$. By Lemmas 3.2 and 3.3 there exists an integer v such that

$$0\leq v<p^2,\ \left(\frac{v^2-4}{p}\right)=\varepsilon,$$
$$\text{and } T_{v,p^k} \text{ is of order } p^{k-1}(p-\varepsilon) \text{ in the group } G(v,p^k).$$

Put $\beta=T_{v,p^k}=T_v \mod p^k$. Since $H=(\beta)$ is a cyclic group of order $p^{k-1}(p-\varepsilon)$, the equation

$$x^{2^iq}\equiv -1 \mod p^k$$

has exactly d_i solutions in H, where $d_i=0$ for $i\geq r$, and

$$\begin{aligned} d_i &= \#\left\{\xi\in H:\ \xi^{2^{i+1}q}\equiv 1 \mod p^k\right\}-\#\left\{\xi\in H:\ \xi^{2^iq}\equiv 1 \mod p^k\right\}\\ &= \gcd\left(2^{i+1}q,p^{k-1}(p-\varepsilon)\right)-\gcd\left(2^iq,p^{k-1}(p-\varepsilon)\right)\\ &= 2^{i+1}\gcd(q,t)-2^i\gcd(q,t)=2^i\gcd(q,t),\ \text{for } 0\leq i<r; \end{aligned}$$

but for $i=0$, including the solution $x=-1 \pmod{p^k}$.

Since both ξ and ξ^{-1} satisfy the same equation

$$y^2-u_\xi y+1\equiv 0 \mod p^k,$$

where $u_\xi=\xi+\xi^{-1} \pmod{p^k}$, the lemma follows by Lemma 3.4. □

Now we are ready to prove Theorem 1.

Proof of Theorem 1. By the Chinese Remainder Theorem and Lemmas 3.5 and 3.6 we have

$$\begin{aligned} \mathrm{B}(n,\varepsilon) &= \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}}\ \prod_{i=1}^{s}X(p_i^{r_i},\varepsilon_i,n-\varepsilon)\\ &= \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}}\ \prod_{i=1}^{s}\left(\frac{\gcd(n-\varepsilon,p_i-\varepsilon_i)}{2}-1\right); \end{aligned}$$

and

$$\begin{aligned}
\mathrm{SB}(n,\varepsilon) &= \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}} \left(\prod_{i=1}^{s} X(p_i^{r_i},\varepsilon_i,q_\varepsilon) + \sum_{j=0}^{m(\varepsilon_1,\cdots,\varepsilon_s)-1}\prod_{i=1}^{s} Y_j(p_i^{r_i},\varepsilon_i,q_\varepsilon)\right)\\
&= \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}} \left(2\prod_{i=1}^{s}\frac{\gcd(q_\varepsilon,q_{i,\varepsilon_i})-1}{2}\right.\\
&\qquad\left. + \sum_{j=1}^{m(\varepsilon_1,\cdots,\varepsilon_s)-1}\prod_{i=1}^{s} 2^{j-1}\gcd(q_\varepsilon,q_{i,\varepsilon_i})\right)\\
&= \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}} \left(2\prod_{i=1}^{s}\frac{\gcd(q_\varepsilon,q_{i,\varepsilon_i})-1}{2}\right.\\
&\qquad\left. + \sum_{j=0}^{m(\varepsilon_1,\cdots,\varepsilon_s)-2} 2^{sj}\prod_{i=1}^{s}\gcd(q_\varepsilon,q_{i,\varepsilon_i})\right)\\
&= \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s\in\{1,-1\}\\ \varepsilon_1^{r_1}\varepsilon_2^{r_2}\cdots\varepsilon_s^{r_s}=\varepsilon}} \left(2\prod_{i=1}^{s}\frac{\gcd(q_\varepsilon,q_{i,\varepsilon_i})-1}{2}\right.\\
&\qquad\left. + \frac{2^{s(m(\varepsilon_1,\cdots,\varepsilon_s)-1)}-1}{2^s-1}\prod_{i=1}^{s}\gcd(q_\varepsilon,q_{i,\varepsilon_i})\right).
\end{aligned}$$

□

Corollary 3.1. *Let $n=p_1p_2$ be the product of two different odd primes with $p_i-\varepsilon_i$ as expressed in equation (2.10). Then we have*

$$\mathrm{B}(n,1) = \left(\frac{\gcd(p_1-1,p_2-1)}{2}-1\right)^2 + \left(\frac{\gcd(p_1+1,p_2+1)}{2}-1\right)^2;$$
$$\mathrm{B}(n,-1) = \left(\frac{\gcd(p_1-1,p_2+1)}{2}-1\right)^2 + \left(\frac{\gcd(p_1+1,p_2-1)}{2}-1\right)^2;$$

$$\begin{aligned}
\mathrm{SB}(n,1) &= \frac{1}{2}\big(\gcd(q_{1,1},q_{2,1})-1\big)^2 + \frac{4^{min\{k_{1,1},k_{2,1}\}-1}-1}{3}\big(\gcd(q_{1,1},q_{2,1})\big)^2\\
&\quad + \frac{1}{2}\big(\gcd(q_{1,-1},q_{2,-1})-1\big)^2 + \frac{4^{\min\{k_{1,-1},k_{2,-1}\}-1}-1}{3}\big(\gcd(q_{1,-1},q_{2,-1})\big)^2;
\end{aligned}$$

$$\begin{aligned}
\mathrm{SB}(n,-1) &= \frac{1}{2}\big(\gcd(q_{1,1},q_{2,-1})-1\big)^2 + \frac{4^{min\{k_{1,1},k_{2,-1}\}-1}-1}{3}\big(\gcd(q_{1,1},q_{2,-1})\big)^2\\
&\quad + \frac{1}{2}\big(\gcd(q_{1,-1},q_{2,1})-1\big)^2 + \frac{4^{\min\{k_{1,-1},k_{2,1}\}-1}-1}{3}\big(\gcd(q_{1,-1},q_{2,1})\big)^2.
\end{aligned}$$

The following two examples give comparisons of $\mathrm{SL}(n)$ with $\mathrm{B}(n)$ and $\mathrm{SB}(n)$.

Example 3.1. Let $n = 1000037 \cdot 1000039 = 1000076001443$. Then

$$\mathrm{B}(n,1) = 0, \quad \mathrm{B}(n) = \mathrm{B}(n,-1) = 1 + (500019-1)^2 = 250018000325,$$
$$\mathrm{SB}(n,1) = 0, \quad \mathrm{SB}(n) = \mathrm{SB}(n,-1) = 1 + (500019-1)^2/2 = 125009000163.$$

Note that, as shown in [3], $\mathrm{SL}(2,n) = 500037000685$ and $1/2 - \mathrm{SL}(2,n)/n < 10^{-6}$. Thus we have

$$\frac{\mathrm{SL}(2,n)}{\mathrm{B}(n)} > 2, \quad \frac{\mathrm{SL}(2,n)}{\mathrm{SB}(n)} > 4, \text{ and } 1/8 - \mathrm{SB}(n)/n < 5 \cdot 10^{-7}.$$

This example also explains Remark 2.5.

Example 3.2. Let $n = 5 \cdot 41 \cdot 101 = 20705$. Then

$$\mathrm{B}(n,1) = 3, \ \mathrm{B}(n,-1) = 2000, \ \mathrm{B}(n) = 3 + 2000 = 2003;$$
$$\mathrm{SB}(n,1) = 1, \ \mathrm{SB}(n,-1) = 500, \ \mathrm{SB}(n) = 1 + 500 = 501.$$

Note that, as shown in [3], $\mathrm{SL}(7,n) = 5213$ and $\mathrm{SL}(7,n)/n = 0.25177\cdots$. Thus we have

$$\frac{\mathrm{SL}(7,n)}{\mathrm{B}(n)} = 2.60\cdots, \quad \frac{\mathrm{SL}(7,n)}{\mathrm{SB}(n)} = 10.405\cdots, \quad \frac{n}{\mathrm{SB}(n)} = 41.327\cdots.$$

4. Proof of Theorem 2

Lemma 4.1. *Let $n = p^k$ with p an odd prime and $k \geq 2$. Then $\mathrm{B}(n) = p - 2 \leq 3n/25$.*

Proof. By Theorem 1, we have, for odd k,

$$\mathrm{B}(p^k,1) = \frac{\gcd(p-1,p^k-1)}{2} - 1 = \frac{p-3}{2},$$
$$\mathrm{B}(p^k,-1) = \frac{\gcd(p+1,p^k+1)}{2} - 1 = \frac{p-1}{2};$$

and for even k,

$$\mathrm{B}(p^k,1) = \frac{\gcd(p-1,p^k-1)}{2} - 1 + \frac{\gcd(p+1,p^k-1)}{2} - 1$$
$$= \frac{p-3}{2} + \frac{p-1}{2} = p-2,$$
$$\mathrm{B}(p^k,-1) = 0.$$

In both cases (either odd k or even k), we have

$$\mathrm{B}(p^k) = \mathrm{B}(p^k,1) + \mathrm{B}(p^k,-1) = p-2, \text{ and } \frac{\mathrm{B}(n)}{n} = \frac{p-2}{p^k} \leq \frac{3}{25}.$$

□

Lemma 4.2. *If a, b, and c are positive integers with $a \mid c$ and $b \mid c$, then*

$$a + b \leq c + \gcd(a,b).$$

Proof. Obvious. □

Lemma 4.3. *Let $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ be the prime decomposition of an odd number n, with $s \geq 2$ and each $r_i \geq 1$. Then*

$$\mathrm{B}(n) < \frac{1}{2} \prod_{i=1}^{s} (p_i - 1) < \frac{n}{2}.$$

Proof. For $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s \in \{1, -1\}$ and $\varepsilon = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s$, define

$$h(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s) = \prod_{i=1}^{s} \Big(\frac{\gcd\big(n - \varepsilon, p_i - \varepsilon_i\big)}{2} - 1 \Big) = \prod_{i=1}^{s} \Big(\gcd\Big(\frac{n - \varepsilon}{2}, \frac{p_i - \varepsilon_i}{2} \Big) - 1 \Big).$$

Then

$$\begin{aligned}
&h(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}, 1) + h(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}, -1) \\
&\quad = h(\varepsilon_1, \cdots, \varepsilon_{s-1}, \varepsilon_s) + h(\varepsilon_1, \cdots, \varepsilon_{s-1}, -\varepsilon_s) \\
&\quad = \Big(\gcd\Big(\frac{n - \varepsilon}{2}, \frac{p_s - \varepsilon_s}{2} \Big) - 1 \Big) \prod_{i=1}^{s-1} \Big(\gcd\Big(\frac{n - \varepsilon}{2}, \frac{p_i - \varepsilon_i}{2} \Big) - 1 \Big) \\
&\qquad + \Big(\gcd\Big(\frac{n + \varepsilon}{2}, \frac{p_s + \varepsilon_s}{2} \Big) - 1 \Big) \prod_{i=1}^{s-1} \Big(\gcd\Big(\frac{n + \varepsilon}{2}, \frac{p_i - \varepsilon_i}{2} \Big) - 1 \Big) \\
&\quad \leq \frac{p_s - 1}{2} \prod_{i=1}^{s-1} \Big(\gcd\Big(\frac{n - \varepsilon}{2}, \frac{p_i - \varepsilon_i}{2} \Big) + \gcd\Big(\frac{n + \varepsilon}{2}, \frac{p_i - \varepsilon_i}{2} \Big) - 2 \Big) \\
&\quad \leq \frac{p_s - 1}{2} \prod_{i=1}^{s-1} \Big(\frac{p_i - \varepsilon_i}{2} + 1 - 2 \Big) \\
&\quad \leq \frac{p_s - 1}{2} \prod_{i=1}^{s-1} \frac{p_i - 1}{2}
\end{aligned}$$

(the next to last inequality holds by Lemma 4.2, since $\gcd\Big(\frac{n-\varepsilon}{2}, \frac{n+\varepsilon}{2} \Big) = 1$). Thus we have

$$\begin{aligned}
\mathrm{B}(n) &= \mathrm{B}(n, 1) + \mathrm{B}(n, -1) \\
&\leq \sum_{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1} \in \{1, -1\}} \Big(h(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}, 1) + h(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}, -1) \Big) \\
&\leq \frac{p_s - 1}{2} \prod_{i=1}^{s-1} (p_i - 1) = \frac{1}{2} \prod_{i=1}^{s} (p_i - 1) < \frac{n}{2}.
\end{aligned}$$

□

Example 4.1. Let $n = 443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$. It is a Carmichael number ([11, A13] and [17]) with $(p^2 - 1) \mid (n - 1)$ for every prime $p \mid n$. We have $\mathrm{B}(n) = \mathrm{B}(n, 1) = 156038017948313$, and $\mathrm{B}(n)/n = 1/2.84\cdots$. (cf. Remark 2.4)

Lemma 4.4. *Let $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ be the prime decomposition of an odd number n, with $s \geq 2$ and each $r_i \geq 1$. Then*

$$\mathrm{SB}(n) < \frac{1}{2^s} \prod_{i=1}^{s} (p_i - 1).$$

Proof. For $\varepsilon \in \{1,-1\}$ and $1 \le i \le s$, let $k_\varepsilon, q_\varepsilon, k_{i,\varepsilon}, q_{i,\varepsilon}$ be as given in (2.10). For $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s \in \{1,-1\}$ and $\varepsilon = \varepsilon_1\varepsilon_2\cdots\varepsilon_s$, define

$$f(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s) = 2\prod_{i=1}^{s}\frac{\gcd(q_\varepsilon, q_{i,\varepsilon_i})-1}{2} + \frac{2^{s(m(\varepsilon_1,\cdots,\varepsilon_s)-1)}-1}{2^s-1}\prod_{i=1}^{s}\gcd(q_\varepsilon, q_{i,\varepsilon_i}),$$

where $m(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s) = \min\{k_{1,\varepsilon_1}, k_{2,\varepsilon_2},\cdots,k_{s,\varepsilon_s}\}$ as defined in (2.11).

As mentioned in Section 2, there exist $e_1, e_2, \cdots, e_s \in \{1,-1\}$ such that $m(e_1,e_2,\cdots,e_s) = m_0 \ge 2$, and $m(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s) = 1$ for all other 2^s-1 s-tuples $(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s)$. Put $e = e_1e_2\cdots e_s$, $e' = (-1)^{s-1}e$. We bound $\mathrm{SB}(n)$ via three parts:

$$\mathrm{SB}(n) \le S_1 + S_2 + S_3$$

with

$$S_1 = f(e_1,\cdots,e_{s-1},e_s) + f(e_1,\cdots,e_{s-1},-e_s) = S_{10} + S_{11},$$

where

$$S_{10} = 2\prod_{i=1}^{s}\frac{\gcd(q_e,\, q_{i,e_i})-1}{2} + \big(\gcd(q_{-e},\, q_{s,-e_s})-1\big)\prod_{i=1}^{s-1}\frac{\gcd(q_{-e},\, q_{i,e_i})-1}{2},$$

and

$$S_{11} = \frac{2^{s(m_0-1)}-1}{2^s-1}\prod_{i=1}^{s}\gcd(q_e,\, q_{i,e_i});$$

$$S_2 = f(-e_1,\cdots,-e_{s-1},e_s) + f(-e_1,\cdots,-e_{s-1},-e_s);$$

and

$$S_3 = \sum_{\substack{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{s-1}\in\{1,-1\}\\ (\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{s-1})\ne\pm(e_1,e_2,\cdots,e_{s-1})}} \Big(f(\varepsilon_1,\cdots,\varepsilon_{s-1},1) + f(\varepsilon_1,\cdots,\varepsilon_{s-1},-1)\Big).$$

If $p_1 = 3$, then $q_{1,\pm1} = 1$. Thus $S_{10} = S_2 = S_3 = 0$, and therefore

$$\begin{aligned}
\mathrm{SB}(n) = S_{11} &\le \frac{2^{s(m_0-1)}-1}{2^s-1}\prod_{i=1}^{s}q_{i,e_i} \le \frac{2^{s(m_0-1)}-1}{2^s-1}\prod_{i=1}^{s}\frac{p_i-e_i}{2^{m_0}}\\
&= \frac{2^{sm_0}-2^s}{(2^s-1)2^s2^{sm_0}}\prod_{i=1}^{s}(p_i-e_i) < \frac{\prod_{i=1}^{s}(p_i-1)}{(2^s-1)2^s}\prod_{p_i\equiv3 \mod 4}\frac{p_i+1}{p_i-1}\\
&\le \frac{\prod_{i=1}^{s}(p_i-1)}{(2^s-1)2^s}\cdot\frac{3+1}{3-1}\cdot\Big(\frac{7+1}{7-1}\Big)^{s-1} \le \frac{8/9}{2^s}\prod_{i=1}^{s}(p_i-1).
\end{aligned}$$

Now suppose $p_1 \geq 5$. Note that $m(-e_1, -e_2, \cdots, -e_{s-1}, \pm 1) = 1$. Then we have

$$\begin{aligned}
S_2 &= \Big(\gcd\big(q_{e'}, q_{s,e_s}\big) - 1\Big) \prod_{i=1}^{s-1} \frac{\gcd\big(q_{e'}, q_{i,-e_i}\big) - 1}{2} \\
&\quad + \Big(\gcd\big(q_{-e'}, q_{s,-e_s}\big) - 1\Big) \prod_{i=1}^{s-1} \frac{\gcd\big(q_{-e'}, q_{i,-e_i}\big) - 1}{2} \\
&\leq \frac{p_s - 1}{2^s} \left(\prod_{i=1}^{s-1} \Big(\gcd\big(q_{e'}, q_{i,-e_i}\big) - 1\Big) + \prod_{i=1}^{s-1} \Big(\gcd\big(q_{-e'}, q_{i,-e_i}\big) - 1\Big) \right) \\
&\leq \frac{p_s - 1}{2^s} \prod_{i=1}^{s-1} \Big(\gcd\big(q_{e'}, q_{i,-e_i}\big) + \gcd\big(q_{-e'}, q_{i,-e_i}\big) - 2\Big) \\
&\leq \frac{p_s - 1}{2^s} \prod_{i=1}^{s-1} \big(q_{i,-e_i} - 1\big) \qquad \big(\text{by Lemma 4.2, since } \gcd(q_{e'}, q_{-e'}) = 1\big) \\
&\leq \frac{p_s - 1}{2^s} \prod_{i=1}^{s-1} \Big(\frac{p_i + e_i}{2} - 1\Big) \leq \frac{1}{2^{2s-1}} \prod_{i=1}^{s} (p_i - 1).
\end{aligned}$$

In the summation of S_3 there are $2^{s-1} - 2$ pairs of f-functions. Since

$$(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}) \neq \pm(e_1, e_2, \cdots, e_{s-1}),$$

there exists at least one j with $1 \leq j \leq s-1$ such that $\varepsilon_j = e_j$, and thus $k_{j,\varepsilon_j} \geq m_0 \geq 2$. We have

$$\begin{aligned}
&f(\varepsilon_1, \cdots, \varepsilon_{s-1}, 1) + f(\varepsilon_1, \cdots, \varepsilon_{s-1}, -1) \\
&\quad \leq \frac{p_s - 1}{2^s} \prod_{i=1}^{s-1} \big(q_{i,\varepsilon_i} - 1\big) \leq \frac{p_s - 1}{2^s 2^{s-2} 2^{m_0}} \prod_{i=1}^{s-1} (p_i - 1) \\
&\quad \leq \frac{1}{2^{2s}} \prod_{i=1}^{s} (p_i - 1).
\end{aligned}$$

Thus we have

$$S_3 \leq \frac{2^{s-1} - 2}{2^{2s}} \prod_{i=1}^{s} (p_i - 1),$$

and therefore

$$S_2 + S_3 \leq \frac{0.5}{2^s} \prod_{i=1}^{s} (p_i - 1). \tag{4.1}$$

Suppose $s \geq 3$ (still $p_1 \geq 5$). By the same arguments as in the evaluation of S_2 we have

$$\begin{aligned}
S_{10} &\leq \frac{p_s - 1}{2^s} \prod_{i=1}^{s-1} \big(q_{i,e_i} - 1\big) \leq \frac{p_s - 1}{2^s} \prod_{i=1}^{s-1} \left(\frac{p_i - e_i}{2^{m_0}} - 1 \right) \\
&\leq \frac{1}{2^{s+(s-1)m_0}} \prod_{i=1}^{s} (p_i - 1) \leq \frac{1}{2^{3s-2}} \prod_{i=1}^{s} (p_i - 1) \leq \frac{0.0625}{2^s} \prod_{i=1}^{s} (p_i - 1)
\end{aligned}$$

and

$$S_{11} = \frac{2^{s(m_0-1)}-1}{2^s-1}\prod_{i=1}^{s}\gcd(q_e, q_{i,e_i}) \le \frac{2^{s(m_0-1)}-1}{2^s-1}\prod_{i=1}^{s} q_{i,e_i}$$
$$\le \frac{2^{s(m_0-1)}-1}{2^s-1}\prod_{i=1}^{s}\frac{p_i-e_i}{2^{m_0}} = \frac{2^{sm_0}-2^s}{(2^s-1)2^s 2^{sm_0}}\prod_{i=1}^{s}(p_i-e_i)$$
$$< \frac{1}{(2^s-1)2^s}\cdot\frac{7+1}{7-1}\cdot\frac{11+1}{11-1}\cdot\Big(\frac{19+1}{19-1}\Big)^{s-2}\prod_{i=1}^{s}(p_i-1)$$
$$= \frac{(5/9)^s(8/5)(9/10)^2}{2^s-1}\prod_{i=1}^{s}(p_i-1) < \frac{0.223}{2^s-1}\prod_{i=1}^{s}(p_i-1) < \frac{0.255}{2^s}\prod_{i=1}^{s}(p_i-1).$$

Adding the three parts together, we have

$$\mathrm{SB}(n) < \frac{0.255+0.0625+0.5}{2^s}\prod_{i=1}^{s}(p_i-1) < \frac{0.818}{2^s}\prod_{i=1}^{s}(p_i-1).$$

Now suppose $s=2$ (still $p_1 \ge 5$). We have

$$S_1 = \frac{1}{2}\big(\gcd(q_e, q_{1,e_1})-1\big)\big(\gcd(q_e, q_{2,e_2})-1\big)$$
$$+ \frac{4^{m_0-1}-1}{3}\gcd(q_e, q_{1,e_1})\gcd(q_e, q_{2,e_2})$$
$$+ \frac{1}{2}\big(\gcd(q_{-e}, q_{1,e_1})-1\big)\big(\gcd(q_{-e}, q_{2,-e_2})-1\big).$$

If $q_{1,e_1} \mid q_e$, then $\gcd(q_{-e}, q_{1,e_1})-1=0$, and thus

$$S_1 \le \frac{1}{2}(q_{1,e_1}-1)(q_{2,e_2}-1) + \frac{4^{m_0-1}-1}{3}q_{1,e_1}q_{2,e_2}$$
$$\le \frac{1}{2}\cdot\frac{p_1-1}{2^{m_0}}\cdot\frac{p_2-1}{2^{m_0}} + \frac{4^{m_0-1}-1}{3}\cdot\frac{p_1-e_1}{2^{m_0}}\cdot\frac{p_2-e_2}{2^{m_0}}$$
$$\le \frac{(p_1-1)(p_2-1)}{4}\Big(\frac{1}{8}+\frac{1}{12}\cdot\frac{7+1}{7-1}\cdot\frac{11+1}{11-1}\Big) = \frac{31/120}{4}(p_1-1)(p_2-1).$$

If $q_{1,e_1} \nmid q_e$, then $\gcd(q_e, q_{1,e_1}) \le \frac{q_{1,e_1}}{3}$, and thus

$$S_1 \le \frac{p_2-1}{4}(q_{1,e_1}-1) + \frac{4^{m_0-1}-1}{3}\cdot\frac{q_{1,e_1}}{3}\cdot q_{2,e_2}$$
$$\le \frac{p_2-1}{4}\cdot\frac{p_1-1}{4} + \frac{4^{m_0-1}-1}{9}\cdot\frac{p_1-e_1}{2^{m_0}}\cdot\frac{p_2-e_2}{2^{m_0}}$$
$$\le \frac{(p_1-1)(p_2-1)}{4}\Big(\frac{1}{4}+\frac{1}{9}\cdot\frac{7+1}{7-1}\cdot\frac{11+1}{11-1}\Big) = \frac{77/180}{4}(p_1-1)(p_2-1).$$

By (4.1) we have, for either $q_{1,e_1} \mid q_e$ or $q_{1,e_1} \nmid q_e$,

$$\mathrm{SB}(n) = S_1+S_2+S_3 < \frac{(p_1-1)(p_2-1)}{4},$$

for $s=2$. □

Corollary 4.1. *In Lemma 4.4, if $s \ge 3$ or $s=2$ with $r_1+r_2 \ge 3$, then* $\mathrm{SB}(n) < n/8$.

The following six lemmas are devoted to the proof of Theorem 2 for the case when $n = p_1p_2$, the product of two different primes.

Lemma 4.5. *Let $n = p_1p_2$ be the product of two twin primes with $p_1 + 1 = p_2 - 1$. Then*

$$\mathrm{B}(n) \le \frac{(p_1-1)(p_2-1)}{4} < n/4 \quad \textit{and} \quad \mathrm{SB}(n) \le \frac{(p_1-1)(p_2-1)}{8} < n/8.$$

Proof. Since $n = p_1p_2$ with $p_1 + 1 = p_2 - 1$, we have, by Corollary 3.1 to Theorem 1,

$$\begin{aligned}\mathrm{B}(n) = \mathrm{B}(n,-1) &= \left(\frac{\gcd(p_1-1, p_1+3)}{2} - 1\right)^2 + \left(\frac{p_1+1}{2} - 1\right)^2 \\ &= \begin{cases} \left(\frac{p_1-1}{2}\right)^2, & \text{for } p_1 \equiv 3 \mod 4; \\ \left(\frac{p_1-1}{2}\right)^2 + 1, & \text{for } p_1 \equiv 1 \mod 4 \end{cases} \\ &\le \left(\frac{p_1-1}{2}\right)^2 + 1 \le \frac{(p_1-1)(p_2-1)}{4}.\end{aligned}$$

Write $p_1 + 1 = p_2 - 1 = 2^k q$ with q odd. We have

$$\mathrm{SB}(n) = \mathrm{SB}(n,-1) = \begin{cases} \frac{(q-1)^2}{2} + \frac{4^{k-1}-1}{3}q^2, & \text{for } p_1 \equiv 3 \mod 4; \\ \frac{(q-1)^2}{2} + 1, & \text{for } p_1 \equiv 1 \mod 4. \end{cases}$$

Case $p_1 \equiv 1 \mod 4$. In this case, we have $k = 1$, and

$$\mathrm{SB}(n) = \frac{1}{2}\left(\frac{p_1-1}{2}\right)^2 + 1 \le \frac{(p_1-1)(p_2-1)}{8}.$$

Case $p_1 \equiv 3 \mod 4$. In this case, we have $k \ge 2$.

If $p_1 = 3$ (and thus $p_2 = 5$, $n = 15$), then $\mathrm{SB}(n) = 1 = (p_1-1)(p_2-1)/8$. Now suppose $p_1 \ge 7$. Then we have

$$\begin{aligned}\mathrm{SB}(n) &= \frac{1}{2}\left(\frac{p_1+1}{2^k} - 1\right)^2 + \frac{(4^{k-1}-1)(p_1+1)^2}{3 \cdot 4^k} \\ &< \frac{1}{8}\left(\frac{(p_1-3)^2}{4} + \frac{2(p_1+1)^2}{3}\right) = \frac{11p_1^2 - 2p_1 + 35}{96} < \frac{(p_1-1)(p_2-1)}{8}.\end{aligned}$$

□

Lemma 4.6. *Let $n = p_1p_2$ be the product of two odd primes with $p_2 - 1 = k(p_1 - 1)$ and $k \ge 2$. Then $\mathrm{B}(n) \le (p_1-1)(p_2-1)/8 < n/8$.*

Proof. Since $n = p_1p_2$ with $p_2 - 1 = k(p_1 - 1)$ and $k \ge 2$, we have

$$\mathrm{B}(n) = \left(\frac{p_1-3}{2}\right)^2 + \left(\gcd\left(\frac{p_1+1}{2}, k\right) - 1\right)^2 + \left(\gcd\left(\frac{p_1+1}{2}, k-1\right) - 1\right)^2.$$

Case $k = 2$. In this case we have

$$\mathrm{B}(n) \le \left(\frac{p_1-3}{2}\right)^2 + 1 = \frac{p_1^2 - 6p_1 + 13}{4} \le \frac{(p_1-1)(p_2-1)}{8}.$$

Case $k = 3$. In this case we have

$$\mathrm{B}(n) = \begin{cases} 1 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 3 \ (p_2 = 7, \ n = 21); \\ 5 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 5 \ (p_2 = 13, \ n = 65); \end{cases}$$

and, for $p_1 \geq 7$,

$$\mathrm{B}(n) \leq \left(\frac{p_1-3}{2}\right)^2 + 5 = \frac{p_1^2 - 6p_1 + 29}{4} \leq \frac{(p_1-1)(p_2-1)}{12}.$$

Case $k \geq 4$. In this case we have, by Lemma 4.2,

$$\mathrm{B}(n) \leq \left(\frac{p_1-3}{2}\right)^2 + \left(\frac{p_1+1}{2}+1-2\right)^2 = \left(\frac{p_1-3}{2}\right)^2 + \left(\frac{p_1-1}{2}\right)^2 < \frac{(p_1-1)^2}{2}$$
$$= \frac{(p_1-1)(p_2-1)}{2k} \leq \frac{(p_1-1)(p_2-1)}{8}.$$

□

Lemma 4.7. *Let $n = p_1p_2$ be the product of two odd primes with $p_2 - 1 = k(p_1+1)$ and $k \geq 2$. If $n = 119 = 7 \cdot 17$, then $\mathrm{B}(n) < (p_1-1)(p_2-1)/7$ and $\mathrm{SB}(n) < (p_1-1)(p_2-1)/8$. Otherwise we have $\mathrm{B}(n) < (p_1-1)(p_2-1)/8$.*

Proof. Since $n = p_1p_2$ with $p_2 - 1 = k(p_1+1)$ and $k \geq 2$, we have

$$\mathrm{B}(n) = \left(\frac{p_1-1}{2}\right)^2 + \left(\gcd\left(\frac{p_1-1}{2}, k\right) - 1\right)^2 + \left(\gcd\left(\frac{p_1-1}{2}, k+1\right) - 1\right)^2.$$

Case $k = 2$. In this case we have, for $p_1 = 5$ ($p_2 = 13$, $n = 65$),

$$\mathrm{B}(n) = 5 < (p_1-1)(p_2-1)/9;$$

and, for $p_1 = 7$ ($p_2 = 17$, $n = 119$),

$$\mathrm{B}(n) = 13 < (p_1-1)(p_2-1)/7,$$

and

$$\mathrm{SB}(n) = \mathrm{SB}(n,-1) = 7 < (p_1-1)(p_2-1)/8;$$

and, for $p_1 \geq 11$,

$$\mathrm{B}(n) \leq \left(\frac{p_1-1}{2}\right)^2 + 5 = \frac{p_1^2 - 2p_1 + 21}{4} \leq \frac{(p_1-1)(p_2-1)}{8}.$$

Case $k = 3$. In this case we have

$$\mathrm{B}(n) = \begin{cases} 1 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 3\ (p_2 = 13,\ n = 39); \\ 5 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 5\ (p_2 = 19,\ n = 95); \end{cases}$$

and, for $p_1 \geq 11$,

$$\mathrm{B}(n) \leq \left(\frac{p_1-1}{2}\right)^2 + 13 = \frac{p_1^2 - 2p_1 + 53}{4} \leq \frac{(p_1-1)(p_2-1)}{8}.$$

Case $k \geq 4$. In this case we have, by Lemma 4.2,

$$\mathrm{B}(n) \leq \left(\frac{p_1-1}{2}\right)^2 + \left(\frac{p_1-1}{2}+1-2\right)^2 = \left(\frac{p_1-1}{2}\right)^2 + \left(\frac{p_1-3}{2}\right)^2$$
$$= \frac{p_1^2 - 4p_1 + 5}{2} \leq \frac{(p_1-1)(p_1+1)}{2} = \frac{(p_1-1)(p_2-1)}{2k} \leq \frac{(p_1-1)(p_2-1)}{8}.$$

□

Lemma 4.8. *Let $n = p_1p_2$ be the product of two odd primes with $p_2+1 = k(p_1-1)$ and $k \geq 2$, except for the case where $p_1 = 5$ and $p_2 = 7$ (cf. Lemma 4.5) and except for the case where $p_1 = 7$ and $p_2 = 17$ (cf. Lemma 4.7). Then we have $B(n) \leq (p_1-1)(p_2-1)/8 < n/8$.*

Proof. Since $n = p_1p_2$ with $p_2 + 1 = k(p_1 - 1)$ and $k \geq 2$, we have

$$B(n) = \left(\frac{p_1-3}{2}\right)^2 + \left(\gcd\left(\frac{p_1+1}{2}, k\right) - 1\right)^2 + \left(\gcd\left(\frac{p_1+1}{2}, k+1\right) - 1\right)^2.$$

Case $k = 2$. In this case we have $p_1 \geq 7$, since $p_1 \neq 5$. Thus we have

$$B(n) \begin{cases} = 5 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 7 \ (p_2 = 11,\ n = 77); \\ \leq \left(\frac{p_1-3}{2}\right)^2 + 5 = \frac{p_1^2-6p_1+29}{4} < \frac{(p_1-1)(p_2-1)}{8}, & \text{for } p_1 \geq 11. \end{cases}$$

Case $k = 3$. In this case we have $p_1 \neq 7$ ($p_2 \neq 17$, $n \neq 119$). Thus

$$B(n) = \begin{cases} 1 = (p_1-1)(p_2-1)/8, & \text{for } p_1 = 3 \ (p_2 = 5,\ n = 15); \\ 5 = (p_1-1)(p_2-1)/8, & \text{for } p_1 = 5 \ (p_2 = 11,\ n = 55); \end{cases}$$

and, for $p_1 \geq 11$,

$$\begin{aligned} B(n) &\leq \left(\frac{p_1-3}{2}\right)^2 + 2^2 + 3^2 = \left(\frac{p_1-3}{2}\right)^2 + 13 \\ &= \frac{p_1^2 - 6p_1 + 61}{4} < \frac{(p_1-1)(p_2-1)}{8}. \end{aligned}$$

Case $k \geq 4$. In this case we have, by Lemma 4.2,

$$\begin{aligned} B(n) &\leq \left(\frac{p_1-3}{2}\right)^2 + \left(\frac{p_1+1}{2} + 1 - 2\right)^2 = \left(\frac{p_1-3}{2}\right)^2 + \left(\frac{p_1-1}{2}\right)^2 \\ &= \frac{p_1^2 - 4p_1 + 5}{2} < \frac{(p_1-1)(p_2-1)}{2k} \leq \frac{(p_1-1)(p_2-1)}{8}. \end{aligned}$$

□

Lemma 4.9. *Let $n = p_1p_2$ be the product of two odd primes with $p_2+1 = k(p_1+1)$ and $k \geq 2$. Then $B(n) \leq (p_1-1)(p_2-1)/8 < n/8$.*

Proof. Since $n = p_1p_2$ with $p_2 + 1 = k(p_1 + 1)$ and $k \geq 2$, we have

$$B(n) = \left(\frac{p_1-1}{2}\right)^2 + \left(\gcd\left(\frac{p_1-1}{2}, k\right) - 1\right)^2 + \left(\gcd\left(\frac{p_1-1}{2}, k-1\right) - 1\right)^2.$$

Case $k = 2$. If $p_1 = 3$ ($p_2 = 7$), then the lemma is valid by Lemma 4.6; else we have

$$B(n) \leq \left(\frac{p_1-1}{2}\right)^2 + 1 = \frac{p_1^2 - 2p_1 + 5}{4} \leq \frac{(p_1-1)(p_2-1)}{8}.$$

Case $k = 3$. In this case we have

$$B(n) = \begin{cases} 1 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 3 \ (p_2 = 11,\ n = 33); \\ 5 < (p_1-1)(p_2-1)/8, & \text{for } p_1 = 5 \ (p_2 = 17,\ n = 85); \end{cases}$$

and, for $p_1 \geq 7$,

$$\mathrm{B}(n) \leq \left(\frac{p_1-1}{2}\right)^2 + 5 = \frac{p_1^2 - 2p_1 + 21}{4} < \frac{(p_1-1)(p_2-1)}{8}.$$

Case $k \geq 4$. In this case we have, by Lemma 4.2,

$$\begin{aligned}\mathrm{B}(n) &\leq \left(\frac{p_1-1}{2}\right)^2 + \left(\frac{p_1-1}{2}+1-2\right)^2 = \left(\frac{p_1-1}{2}\right)^2 + \left(\frac{p_1-3}{2}\right)^2 \\ &= \frac{p_1^2-4p_1+5}{2} < \frac{(p_1-1)(p_2-1)}{2k} \leq \frac{(p_1-1)(p_2-1)}{8}.\end{aligned}$$

□

Lemma 4.10. *Let* $n = p_1p_2$ *be the product of two odd primes* $p_1 < p_2$, *not considered in Lemmas 4.5-4.9, i.e.,* $p_1 \pm 1$ *not dividing* $p_2 \pm 1$. *Then we have* $\mathrm{B}(n) < (p_1-1)(p_2-1)/8 < n/8$.

Proof. Write $p_1 - 1 = 2^k q$ with q odd. Put $x = \gcd(p_1-1, p_2-1)$ and $y = \gcd(p_1-1, p_2+1)$. Then $\gcd(x,y) = 2$ and $x + y \leq 2^{k-1}q + 2 = (p_1+3)/2$, since $p_1 - 1$ does not divide $p_2 \pm 1$. Thus

$$\left(\frac{x}{2}-1\right)^2 + \left(\frac{y}{2}-1\right)^2 \leq \left(\frac{x+y}{2}-2\right)^2 \leq \left(\frac{p_1-5}{4}\right)^2.$$

By the same reasoning, we have

$$\left(\frac{\gcd(p_1+1, p_2-1)}{2}-1\right)^2 + \left(\frac{\gcd(p_1+1, p_2+1)}{2}-1\right)^2 \leq \left(\frac{p_1-3}{4}\right)^2.$$

Therefore by Corollary 3.1 to Theorem 1, we have

$$\begin{aligned}\mathrm{B}(n) &= \left(\frac{\gcd(p_1-1, p_2-1)}{2}-1\right)^2 + \left(\frac{\gcd(p_1-1, p_2+1)}{2}-1\right)^2 \\ &\quad + \left(\frac{\gcd(p_1+1, p_2-1)}{2}-1\right)^2 + \left(\frac{\gcd(p_1+1, p_2+1)}{2}-1\right)^2 \\ &\leq \frac{(p_1-5)^2}{16} + \frac{(p_1-3)^2}{16} < \frac{(p_1-1)(p_2-1)}{8}.\end{aligned}$$

□

Now we are ready to prove Theorem 2.

Proof of Theorem 2. The theorem follows by Lemmas 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, and 4.10, and from the fact that $\mathrm{SB}(n) \leq \mathrm{B}(n)$. □

5. Proof of Theorem 3

Theorem 3 follows by (2.9) and the following Lemmas 5.1, 5.2, 5.4, 5.6, 5.7, 5.8, and 5.9.

Lemma 5.1. *We have* $\tau_0(n) < \frac{1}{n^{4/3}}$ *for* $n = p^k$ *with* p *an odd prime and* $k > 1$.

Proof. If k is even, then $\mathrm{B}(n,-1)=0$, and thus $\tau_0(n)=0$. Now suppose k is odd ≥ 3. For $\varepsilon\in\{1,-1\}$, we have, by Theorem 1,

$$\tau_0(n,\varepsilon)=\frac{\mathrm{B}(p^k,\varepsilon)}{(n-\varepsilon-2)/2}=\frac{p-\varepsilon-2}{n-\varepsilon-2}<\frac{1}{p^{k-1}}=\frac{1}{n^{1-1/k}}.$$

Thus

$$\tau_0(n)=\tau_0(n,1)\tau_0(n,-1)<\frac{1}{n^{2-2/k}}\leq\frac{1}{n^{4/3}}.$$

□

Lemma 5.2. *We have* $\tau_0(n)<\frac{1}{n^{2/3}}$ *for* $n=p_1p_2$ *with* $p_1<p_2$ *odd primes.*

Proof. If $p_1=3$, then either $\mathrm{B}(n,1)=0$ or $\mathrm{B}(n,-1)=0$; thus $\tau_0(n)=0$. Now suppose $p_1\geq 5$ and $p_2\geq 7$. Put

$$a=\frac{\gcd(p_1-1,p_2-1)}{2},\ b=\frac{\gcd(p_1+1,p_2+1)}{2},$$
$$c=\frac{\gcd(p_1-1,p_2+1)}{2},\ d=\frac{\gcd(p_1+1,p_2-1)}{2}.$$

Since both a and d divide $(p_2-1)/2$, and $\gcd(a,d)=1$, we have $ad\leq(p_2-1)/2$. Thus

$$(a-1)(d-1)=ad-a-d+1\leq(p_2-7)/2. \tag{5.1}$$

Since a divides $(p_1-1)/2$ and d divides $(p_1+1)/2$, we have $ad\leq(p_1^2-1)/4$. Thus

$$(a-1)(d-1)=ad-a-d+1\leq(p_1^2-13)/4. \tag{5.2}$$

By (5.1) and (5.2) we have

$$(a-1)^3(d-1)^3\leq\frac{(p_1^2-13)(p_2-7)^2}{16}<\frac{n^2-13n}{16}.$$

Thus

$$(a-1)^2(d-1)^2\leq\frac{(n^2-13n)^{2/3}}{4\cdot 2^{2/3}}. \tag{5.3}$$

Analogously we have

$$(b-1)^2(c-1)^2\leq\frac{(n^2-13n)^{2/3}}{4\cdot 2^{2/3}}. \tag{5.4}$$

Since both a and c divide $(p_1-1)/2$, and $\gcd(a,c)=1$, we have $ac\leq(p_1-1)/2$. Since both b and d divide $(p_1+1)/2$, and $\gcd(b,d)=1$, we have $bd\leq(p_1+1)/2$. Thus

$$(a-1)(c-1)=ac-a-c+1\leq(p_1-5)/2$$

and

$$(b-1)(d-1)=bd-b-d+1\leq(p_1-5)/2;$$

therefore

$$(a-1)^2(c-1)^2+(b-1)^2(d-1)^2\leq\frac{(p_1-5)^2}{2}\leq\frac{n-35}{2} \tag{5.5}$$

and

$$(a-1)(d-1)(b-1)(c-1)\leq\frac{(p_1-5)^2}{4}\leq\frac{n-35}{4}. \tag{5.6}$$

By (5.3), (5.4) and (5.6) we have

(5.7)
$$(a-1)^2(d-1)^2+(b-1)^2(c-1)^2 \le \frac{(n^2-13n)^{2/3}}{4\cdot 2^{2/3}}+\frac{(n-35)^2/16}{(n^2-13n)^{2/3}/(4\cdot 2^{2/3})}.$$

By Theorem 1, (5.5) and (5.7) we have

$$\begin{aligned}\tau_0(n) &= \frac{(a-1)^2(d-1)^2+(b-1)^2(c-1)^2+(a-1)^2(c-1)^2+(b-1)^2(d-1)^2}{(n-1)(n-3)/4}\\ &\le \frac{\frac{(n^2-13n)^{2/3}}{2^{2/3}}+\frac{2^{2/3}(n-35)^2}{(n^2-13n)^{2/3}}+2(n-35)}{(n-1)(n-3)}.\end{aligned}$$

Thus

$$\begin{aligned}\tau_0(n)n^{2/3} &\le \frac{(n^3-13n^2)^{2/3}}{2^{2/3}(n-1)(n-3)}+\frac{2^{2/3}(n-35)^2}{(n-1)(n-3)(n-13)^{2/3}}+\frac{2(n-35)n^{2/3}}{(n-1)(n-3)}\\ &< \begin{cases}\frac{1}{2^{2/3}}+\frac{2^{2/3}}{(n-13)^{2/3}}+\frac{2}{n^{1/3}}<0.97, & \text{for } n>300;\\ 0.95, & \text{for } 35\le n<300.\end{cases}\end{aligned}$$

The lemma follows. □

Now let $n=p_1p_2p_3$ be the product of three odd primes with $p_1<p_2<p_3$. For $i=1,2,3$, put

$$a_i=\gcd\Big(\frac{n-1}{2},\frac{p_i-1}{2}\Big),\ a_i'=\gcd\Big(\frac{n+1}{2},\frac{p_i-1}{2}\Big),$$
$$b_i=\gcd\Big(\frac{n-1}{2},\frac{p_i+1}{2}\Big),\ b_i'=\gcd\Big(\frac{n+1}{2},\frac{p_i+1}{2}\Big),$$
$$x_i=a_i-1,\ x_i'=a_i'-1,\ y_i=b_i-1, y_i'=b_i'-1.$$

Then

(5.8)
$$\begin{cases}\mathrm{B}(n,1)=x_1x_2x_3+x_1y_2y_3+y_1x_2y_3+y_1y_2x_3,\\ \mathrm{B}(n,-1)=y_1'y_2'y_3'+y_1'x_2'x_3'+x_1'y_2'x_3'+x_1'x_2'y_3'.\end{cases}$$

Since $\gcd\big(\frac{n-1}{2},\frac{n+1}{2}\big)=1$, we have

(5.9)
$$\begin{aligned}&a_ia_i'\le\frac{p_i-1}{2},\ b_ib_i'\le\frac{p_i+1}{2},\\ &x_ix_i'\le a_ia_i'-1\le\frac{p_i-3}{2}, y_iy_i'\le b_ib_i'-1\le\frac{p_i-1}{2}.\end{aligned}$$

Since

$$a_i=\gcd\Big(\frac{n/p_i-1}{2},\frac{p_i-1}{2}\Big),\ a_i'=\gcd\Big(\frac{n/p_i+1}{2},\frac{p_i-1}{2}\Big),$$
$$b_i=\gcd\Big(\frac{n/p_i+1}{2},\frac{p_i+1}{2}\Big),\ b_i'=\gcd\Big(\frac{n/p_i-1}{2},\frac{p_i+1}{2}\Big),\gcd\Big(\frac{p_i-1}{2},\frac{p_i+1}{2}\Big)=1,$$

we have

(5.10)
$$\begin{cases}x_iy_i'\le a_ib_i'-1=\gcd\Big(\frac{n/p_i-1}{2},\frac{p_i^2-1}{4}\Big)-1<\min\Big\{\frac{n/p_i-1}{2},\frac{p_i^2-1}{4}\Big\};\\ x_i'y_i\le a_i'b_i-1=\gcd\Big(\frac{n/p_i+1}{2},\frac{p_i^2-1}{4}\Big)-1\le\min\Big\{\frac{n/p_i+1}{2},\frac{p_i^2-1}{4}\Big\}-1\\ \qquad\qquad\le\min\Big\{\frac{n/p_i-1}{2},\frac{p_i^2-1}{4}\Big\}.\end{cases}$$

By (5.9) and (5.10) we have

(5.11)
$$x_1x_2x_3y_1'x_2'x_3' = (x_1y_1')(x_2x_2')(x_3x_3') < \frac{p_1^2-1}{4}\cdot\frac{p_2-3}{2}\cdot\frac{p_3-3}{2} < \frac{p_1^2p_2p_3}{16} < \frac{n^{4/3}}{16}.$$

Similarly we have

$$x_1y_2y_3y_1'y_2'y_3' < \frac{n^{4/3}}{16};\ \ y_1x_2y_3x_1'x_2'y_3' < \frac{n^{4/3}}{16};\ \ y_1y_2x_3x_1'y_2'x_3' < \frac{n^{4/3}}{16}. \tag{5.12}$$

Also by (5.9) and (5.10) we have

$$x_1x_2x_3x_1'x_2'y_3' = (x_1x_1')(x_2x_2')(x_3y_3') < \frac{p_1-3}{2}\cdot\frac{p_2-3}{2}\cdot\min\Big\{\frac{p_1p_2-1}{2}, \frac{p_3^2-1}{4}\Big\}.$$

Thus $x_1x_2x_3x_1'x_2'y_3' < p_1^2p_2^2/8$ and $x_1x_2x_3x_1'x_2'y_3' < p_1p_2p_3^2/16$, so that

$$(x_1x_2x_3x_1'x_2'y_3')^3 < n^4/2^{11}.$$

Therefore

$$x_1x_2x_3x_1'x_2'y_3' < \frac{n^{4/3}}{2^{11/3}} < \frac{n^{4/3}}{12.6}. \tag{5.13}$$

Similarly we have

$$\begin{cases} x_1x_2x_3x_1'y_2'x_3' < \frac{n^{4/3}}{12.6};\ \ x_1y_2y_3x_1'y_2'x_3' < \frac{n^{4/3}}{12.6};\\ x_1y_2y_3x_1'x_2'y_3' < \frac{n^{4/3}}{12.6};\ \ y_1x_2y_3y_1'y_2'y_3' < \frac{n^{4/3}}{12.6};\\ y_1x_2y_3y_1'x_2'x_3' < \frac{n^{4/3}}{12.6};\ \ y_1y_2x_3y_1'y_2'y_3' < \frac{n^{4/3}}{12.6};\ \ y_1y_2x_3y_1'x_2'x_3' < \frac{n^{4/3}}{12.6}. \end{cases} \tag{5.14}$$

Lemma 5.3. *We have*

$$x_1x_2x_3y_1'y_2'y_3' < \frac{n^{8/5}}{3.917};\ x_1y_2y_3y_1'x_2'x_3' < \frac{n^{8/5}}{2.569};$$
$$y_1x_2y_3x_1'y_2'x_3' < \frac{n^{8/5}}{2.569};\ y_1y_2x_3x_1'x_2'y_3' < \frac{n^{8/5}}{7.155}.$$

Proof. If $p_1 < n^{1/5}$, then by (5.10) we have

$$x_1x_2x_3y_1'y_2'y_3' = (x_1y_1')(x_2y_2')(x_3y_3') < \frac{p_1^2}{4}\cdot\frac{p_1p_2}{2}\cdot\frac{p_1p_3}{2} = \frac{p_1^3n}{16} < \frac{n^{8/5}}{16};$$

and similarly

$$x_1y_2y_3y_1'x_2'x_3' < \frac{n^{8/5}}{16};\ \ y_1x_2y_3x_1'y_2'x_3' < \frac{n^{8/5}}{16};\ \ y_1y_2x_3x_1'x_2'y_3' < \frac{n^{8/5}}{16}.$$

Now suppose $p_1 > n^{1/5}$. By calculation the lemma is valid for $n = p_1p_2p_3 < 10^6$. Now suppose $n = p_1p_2p_3 > 10^6$. For $i = 1, 2$, and 3 put

$$h_i = \gcd\big(2(n/p_i - 1), p_i^2 - 1\big),\ u_i = 2(n/p_i - 1)/h_i,\ v_i = (p_i^2-1)/h_i,$$

$$h_i' = \gcd\big(2(n/p_i + 1), p_i^2 - 1\big),\ u_i' = 2(n/p_i + 1)/h_i',\ v_i' = (p_i^2-1)/h_i'.$$

Since $(p_i^2-1)(p_j^2-1) < (p_ip_j-1)^2$ for $1 \le i \ne j \le 3$, we have

$$\begin{aligned}(p_1^2-1)(p_2^2-1)(p_3^2-1) &< (p_1p_2-1)(p_2p_3-1)(p_1p_3-1)\\ &\le (p_1p_2 \pm 1)(p_2p_3 \pm 1)(p_1p_3 \pm 1).\end{aligned} \tag{5.15}$$

Then $u_1u_2u_3 \geq 8v_1v_2v_3 + 1$, and thus

$$1 + \frac{1}{8v_1v_2v_3} \leq \frac{u_1u_2u_3}{8v_1v_2v_3} = \frac{(p_1p_2-1)(p_2p_3-1)(p_1p_3-1)}{(p_1^2-1)(p_2^2-1)(p_3^2-1)}$$
$$< \frac{n^2}{n^2 - p_1^2p_2^2 - p_2^2p_3^2 - p_1^2p_3^2}$$
$$= \frac{1}{1-(1/p_1^2+1/p_2^2+1/p_3^2)} < \frac{1}{1-(2/n^{2/5}+1/n^{2/3})}.$$

Therefore

$$8v_1v_2v_3 > \frac{1}{2/n^{2/5}+1/n^{2/3}} - 1 = \frac{n^{2/5}}{2+1/n^{4/15}} - 1 > \frac{n^{2/5}}{2.042}. \tag{5.16}$$

Now by (5.10) and (5.16) we have

$$x_1x_2x_3y_1'y_2'y_3' = (x_1y_1')(x_2y_2')(x_3y_3') < \prod_{i=1}^{3} \gcd\Big(\frac{n/p_i-1}{2}, \frac{p_i^2-1}{4}\Big)$$
$$= \frac{h_1h_2h_3}{4^3} = \frac{\prod_{i=1}^3(p_i^2-1)}{4^3v_1v_2v_3} < \frac{n^{8/5}}{3.917}.$$

Thus the first inequality of the lemma is proved.

Since $p_1 > n^{1/5}$, we have $p_2^2 < p_2p_3 < n^{4/5}$; so $p_2 < n^{2/5}$. But $p_1p_2 > n^{2/5}$, and thus $p_3 < n^{3/5}$. By (5.15) we have

$$1 + \frac{1}{8v_1v_2'v_3'} \leq \frac{u_1u_2'u_3'}{8v_1v_2'v_3'} = \frac{(p_1p_2+1)(p_2p_3-1)(p_1p_3+1)}{(p_1^2-1)(p_2^2-1)(p_3^2-1)}$$
$$< \frac{n^2+n(p_2+p_3)}{n^2 - p_1^2p_2^2 - p_2^2p_3^2 - p_1^2p_3^2}$$
$$= \frac{1+(p_2+p_3)/n}{1-(1/p_1^2+1/p_2^2+1/p_3^2)} < \frac{1+1/n^{3/5}+1/n^{2/5}}{1-(2/n^{2/5}+1/n^{2/3})},$$

and therefore

$$8v_1v_2'v_3' > \frac{n^{2/5}-2-1/n^{4/15}}{3+1/n^{1/5}+1/n^{4/15}} > \frac{n^{2/5}}{3.114}. \tag{5.17}$$

Now by (5.10) and (5.17) we have

$$x_1y_2y_3y_1'x_2'x_3' < \frac{h_1h_2'h_3'}{4^3} = \frac{\prod_{i=1}^3(p_i^2-1)}{4^3v_1v_2'v_3'} < \frac{n^{8/5}}{2.569},$$

which is the second inequality of the lemma.

Again by (5.15) we have

$$1 + \frac{1}{8v_1'v_2v_3'} < \frac{n^2+n(p_1+p_3)}{n^2 - p_1^2p_2^2 - p_2^2p_3^2 - p_1^2p_3^2} < \frac{1+1/n^{3/5}+1/n^{2/5}}{1-(2/n^{2/5}+1/n^{2/3})}.$$

Thus

$$8v_1'v_2v_3' > \frac{n^{2/5}}{3.114}, \text{ and } y_1x_2y_3x_1'y_2'x_3' < \frac{h_1'h_2h_3'}{4^3} = \frac{\prod_{i=1}^3(p_i^2-1)}{4^3v_1'v_2v_3'} < \frac{n^{8/5}}{2.569},$$

which is the third inequality of the lemma.

Once again by (5.15) and the facts that $p_1 < n^{1/3}$ and $p_2 < n^{2/5}$ we have

$$1 + \frac{1}{8v_1'v_2'v_3} < \frac{n^2 + n(p_1+p_2)}{n^2 - p_1^2p_2^2 - p_2^2p_3^2 - p_1^2p_3^2} < \frac{1 + 1/n^{2/3} + 1/n^{3/5}}{1 - (2/n^{2/5} + 1/n^{2/3})};$$

therefore

$$8v_1'v_2'v_3 > \frac{n^{2/5} - 1 - 1/n^{4/15}}{1 + 1/n^{1/5} + 2/n^{4/15}} > \frac{n^{2/5}}{1.118}. \tag{5.18}$$

Now by (5.10) and (5.18) we have

$$y_1y_2x_3x_1'x_2'y_3' < \frac{h_1'h_2'h_3}{4^3} = \frac{\prod_{i=1}^3(p_i^2-1)}{4^3v_1'v_2'v_3} < \frac{n^{8/5}}{7.155},$$

which is the last inequality of the lemma. □

Lemma 5.4. *We have* $\tau_0(n) < \frac{1}{n^{2/7}}$ *for* $n = p_1p_2p_3$ *the product of three different odd primes.*

Proof. By computer calculation the lemma is valid for $n = p_1p_2p_3 < 10^6$. Now suppose $n = p_1p_2p_3 > 10^6$. By (5.8), (5.11), (5.12), (5.13), (5.14) and Lemma 5.3, we have

$$\tau_0(n) = \frac{\mathrm{B}(n,1)\mathrm{B}(n,-1)}{(n-1)(n-3)/4} < \frac{n^{4/3}(\frac{4}{16} + \frac{8}{12.6}) + n^{8/5}(\frac{1}{3.917} + \frac{2}{2.569} + \frac{1}{7.155})}{(n-1)(n-3)/4} < \frac{0.995}{n^{2/7}}.$$

□

Remark 5.1. In Lemma 5.4, $n^{2/7}$ can be improved to $n^{1/3}$, if one uses more complicated analysis and computation. But it cannot be improved to $n^{2/3}$, e.g.,

$$n = 62164241 = 41 \cdot 881 \cdot 1721,\ \mathrm{B}(n,1) = 636519,\ \mathrm{B}(n,-1) = 176000,$$
$$\tau_0(n) = \frac{18.19\cdots}{n^{2/3}}.$$

Remark 5.2. Williams [22] asked whether there are any Carmichael numbers n with an odd number of prime divisors and the additional property that for $p \mid n$, $p+1 \mid n+1$. Lemma 5.4 shows that if such a Carmichael number exists, it must have at least 5 prime divisors. But Pinch [17] found no such numbers up to 10^{15}.

Lemma 5.5. *Let* n *be odd with prime* $p \mid n$. *Then*

$$\Big(\frac{\gcd(p-1,n-1)}{2} - 1 + \frac{\gcd(p+1,n-1)}{2} - 1\Big) \times \Big(\frac{\gcd(p-1,n+1)}{2} - 1 + \frac{\gcd(p+1,n+1)}{2} - 1\Big) \le \frac{(p-1)(p-3)}{4}.$$

Proof. Let y be the value of the left part of the inequality and

$$a = \frac{\gcd(p-1,n-1)}{2},\ b = \frac{\gcd(p+1,n-1)}{2},$$
$$c = \frac{\gcd(p-1,n+1)}{2},\ d = \frac{\gcd(p+1,n+1)}{2}.$$

Then

$$y \le \frac{(a-1+c-1+b-1+d-1)^2}{4} \le \frac{1}{4}\Big(\frac{p-3}{2} + \frac{p-1}{2}\Big)^2 = \frac{(p-2)^2}{4}.$$

Since y is an integer and p is odd, the lemma follows. □

Lemma 5.6. *Let $n = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ be the prime decomposition of an odd number n. If $s \geq 3$ or $s = 2$ with $r_1 + r_2 \geq 3$, then*

$$\tau_0(n) < \frac{1}{4^{s-1}} \prod_{i=1}^{s} \frac{1}{p_i^{2(r_i-1)}} \quad \text{and} \quad \tau(n) < \frac{1}{4^s} \prod_{i=1}^{s} \frac{1}{p_i^{2(r_i-1)}}.$$

Proof. By Theorem 1 and Lemma 5.5 we have

$$\begin{aligned} &\mathrm{B}(n,1)\mathrm{B}(n,-1) \\ &\leq \prod_{i=1}^{s} \Big(\frac{\gcd(p_i-1,n-1)}{2} - 1 + \frac{\gcd(p_i+1,n-1)}{2} - 1 \Big) \\ &\quad \times \Big(\frac{\gcd(p_i-1,n+1)}{2} - 1 + \frac{\gcd(p_i+1,n+1)}{2} - 1 \Big) \\ &\leq \prod_{i=1}^{s} \frac{(p_i-1)(p_i-3)}{4}. \end{aligned}$$

Thus

$$\tau_0(n) = \frac{\mathrm{B}(n,1)\mathrm{B}(n,-1)}{(n-1)(n-3)/4} \leq \frac{\prod_{i=1}^{s}(p_i-1)(p_i-3)}{4^{s-1}(n-1)(n-3)} < \frac{1}{4^{s-1}} \prod_{i=1}^{s} \frac{1}{p_i^{2(r_i-1)}}.$$

Since $s \geq 3$ or $s = 2$ with $r_1 + r_2 \geq 3$, we have

$$\frac{1}{p_1^2} + \frac{1}{p_2^2} + \cdots + \frac{1}{p_s^2} > \frac{s}{(p_1p_2\cdots p_s)^{2/s}} > \frac{4}{n}.$$

Thus by Lemma 4.4 we have

$$\begin{aligned} \tau(n) &= \frac{\mathrm{SB}(n,1)\cdot \mathrm{SB}(n,-1)}{(n-1)(n-3)/4} < \frac{(\mathrm{SB}(n))^2}{n^2-4n} \leq \frac{\prod_{i=1}^{s}(p_i-1)^2}{4^s(n^2-4n)} < \frac{\prod_{i=1}^{s}(p_i^2-5)}{4^s(n^2-4n)} \\ &< \left(\frac{1}{4^s} \prod_{i=1}^{s} \frac{1}{p_i^{2(r_i-1)}} \right) \cdot \frac{1 - \frac{1}{p_1^2} - \frac{1}{p_2^2} - \cdots - \frac{1}{p_s^2}}{1 - 4/n} < \frac{1}{4^s} \prod_{i=1}^{s} \frac{1}{p_i^{2(r_i-1)}}. \end{aligned}$$

□

Lemma 5.7. *Let $n = p_1p_2\cdots p_s$ with $p_1 < p_2 < \cdots < p_s$ odd primes and s even ≥ 4. Then $\tau_0(n) < \frac{2}{p_1+1}$.*

Proof. Let $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s, e_1, e_2, \cdots, e_s \in \{1, -1\}$ with $\varepsilon_1\varepsilon_2\cdots\varepsilon_s = 1$ and $e_1e_2\cdots e_s = -1$. Define

$$f(\varepsilon_1, \cdots, \varepsilon_s) = \prod_{i=1}^{s} \Big(\frac{\gcd(p_i - \varepsilon_i, n-1)}{2} - 1 \Big)$$

and

$$g(e_1, \cdots, e_s) = \prod_{i=1}^{s} \Big(\frac{\gcd(p_i - e_i, n+1)}{2} - 1 \Big).$$

If $\varepsilon_i = e_i$, then

$$\Big(\frac{\gcd(p_i-\varepsilon_i, n-1)}{2} - 1 \Big) \Big(\frac{\gcd(p_i-e_i, n+1)}{2} - 1 \Big) \leq \frac{p_i - \varepsilon_i}{2} - 1 \leq \frac{p_i - 1}{2}.$$

If $\varepsilon_i = -e_i$, then

$$\Big(\frac{\gcd(p_i-\varepsilon_i, n-1)}{2} - 1 \Big) \Big(\frac{\gcd(p_i-e_i, n+1)}{2} - 1 \Big) \leq \frac{p_i^2 - 1}{4} - 1 = \frac{p_i^2 - 5}{4}.$$

Since s is even, there exists at least one j such that $\varepsilon_j = e_j$. Since $\frac{p_i-1}{2} \le \frac{p_i^2-5}{4}$, we have

$$f(\varepsilon_1,\cdots,\varepsilon_s)g(e_1,\cdots,e_s) \le \frac{p_j-1}{2}\prod_{i\neq j}\frac{p_i^2-5}{4} = \frac{(p_j^2-1)\prod_{i\neq j}(p_i^2-5)}{2^{2s-1}(p_j+1)}$$
$$< \frac{(p_1^2-1)\prod_{i=2}^{s}p_i^2}{2^{2s-1}(p_j+1)} < \frac{n^2-4n}{2^{2s-1}(p_1+1)}.$$

Thus

$$\tau_0(n) = \frac{\mathrm{B}(n,1)\mathrm{B}(n,-1)}{(n-1)(n-3)/4}$$
$$= \frac{4}{(n-1)(n-3)} \sum_{\substack{\varepsilon_1,\cdots,\varepsilon_s,e_1,\cdots,e_s\in\{1,-1\}\\ \varepsilon_1\cdots\varepsilon_s=1;\ e_1\cdots e_s=-1}} f(\varepsilon_1,\cdots,\varepsilon_s)g(e_1,\cdots,e_s)$$
$$< \frac{4}{(n-1)(n-3)}\cdot 2^{2s-2}\cdot\frac{n^2-4n}{2^{2s-1}(p_1+1)} < \frac{2}{p_1+1}.$$

□

In the following two lemmas let $\varepsilon,\delta\in\{1,-1\}$ and $q_\delta, q_{i,\varepsilon}$ be as given in (2.10). Put

$$d_{i,\varepsilon}^{(\delta)} = \gcd(q_\delta, q_{i,\varepsilon}), \quad \text{and} \quad a_{i,\varepsilon}^{(\delta)} = d_{i,\varepsilon}^{(\delta)} - 1.$$

Then we have

(5.19)

$$d_{i,\varepsilon}^{(1)}d_{i,\varepsilon}^{(-1)} \le q_{i,\varepsilon};\ \ a_{i,\varepsilon}^{(1)}a_{i,\varepsilon}^{(-1)} \le q_{i,\varepsilon}-1;\ \ a_{i,\varepsilon}^{(1)}a_{i,-\varepsilon}^{(-1)} \le q_{i,1}q_{i,-1}-1 \le \frac{1}{8}(p_i^2-9).$$

By Lemma 4.2 and the fact that $\gcd(q_1,q_{-1})=1$ we have

$$d_{i,\varepsilon}^{(1)} + d_{i,\varepsilon}^{(-1)} \le q_{i,\varepsilon}+1;\ \ a_{i,\varepsilon}^{(1)} + a_{i,\varepsilon}^{(-1)} \le q_{i,\varepsilon}-1. \tag{5.20}$$

Put

$$S_0 = \sum_{\substack{\varepsilon_1,\cdots,\varepsilon_s,e_1,\cdots,e_s\in\{1,-1\}\\ \varepsilon_1\cdots\varepsilon_s=1;\ e_1\cdots e_s=-1}} \prod_{i=1}^{s} a_{i,\varepsilon_i}^{(1)}a_{i,e_i}^{(-1)}. \tag{5.21}$$

Let $m(\varepsilon_1,\cdots,\varepsilon_s)$ be as given by (2.11).

Lemma 5.8. *Let $n=p_1p_2\cdots p_s$ with $p_1<p_2<\cdots<p_s$ odd primes, and s even ≥ 4. Then*

$$\tau(n) < \Big(\frac{1}{2^{3s-4}} + \frac{1}{2^{2s-3}(2^s-1)}\Big)\frac{1}{p_1+1} < \frac{1}{8^{s-4}\cdot 166(p_1+1)}.$$

Proof. Let $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s,e_1,e_2,\cdots,e_s\in\{1,-1\}$ with $\varepsilon_1\varepsilon_2\cdots\varepsilon_s=1$ and $e_1e_2\cdots e_s=-1$. Since s is even, there exists at least one j such that $\varepsilon_j=e_j$. For this j we have, by (5.19),

$$a_{j,\varepsilon_j}^{(1)}a_{j,e_j}^{(-1)} \le q_{j,\varepsilon_j}-1 \le \frac{p_j-1}{2}.$$

Since $\frac{p_i-1}{2} \le \frac{p_i^2-1}{8}$ and $a_{i,\varepsilon}^{(1)} a_{i,-\varepsilon}^{(-1)} \le \frac{p_i^2-9}{8} < \frac{p_i^2-1}{8}$, we have

$$\prod_{i=1}^{s} a_{i,\varepsilon_i}^{(1)} a_{i,e_i}^{(-1)} \le \frac{p_j-1}{2} \prod_{i\ne j} \frac{p_i^2-1}{8} = \frac{\prod_{i=1}^{s}(p_i^2-1)}{2^{3s-2}(p_j+1)} < \frac{n^2-4n}{2^{3s-2}(p_j+1)}.$$

Then

$$S_0 < 2^{2s-2} \frac{n^2-4n}{2^{3s-2}(p_1+1)} = \frac{n^2-4n}{2^s(p_1+1)}. \tag{5.22}$$

As mentioned in Section 2, there exist $\delta_1, \delta_2, \cdots, \delta_s \in \{1,-1\}$ such that $m(\delta_1,\delta_2,\cdots,\delta_s) = m_0 \ge 2$, and $m(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s) = 1$ for all other 2^s-1 s-tuples $(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s)$. Put $\delta = \delta_1\delta_2\cdots\delta_s$, and

$$W = \frac{2^{s(m_0-1)}-1}{2^s-1} \prod_{i=1}^{s} d_{i,\delta_i}^{(\delta)}.$$

Then

$$\mathrm{SB}(n,\delta) = W + \frac{1}{2^{s-1}} \sum_{\substack{\varepsilon_1,\cdots,\varepsilon_s\in\{1,-1\} \\ \varepsilon_1\cdots\varepsilon_s=\delta}} \prod_{i=1}^{s} a_{i,\varepsilon_i}^{(\delta)};$$

$$\mathrm{SB}(n,-\delta) = \frac{1}{2^{s-1}} \sum_{\substack{e_1,\cdots,e_s\in\{1,-1\} \\ e_1\cdots e_s=-\delta}} \prod_{i=1}^{s} a_{i,e_i}^{(-\delta)}.$$

Thus

$$\begin{aligned}\mathrm{SB}(n,1)\mathrm{SB}(n,-1) &= \frac{S_0}{2^{2s-2}} + \frac{W}{2^{s-1}} \sum_{\substack{e_1,\cdots,e_s\in\{1,-1\} \\ e_1\cdots e_s=-\delta}} \prod_{i=1}^{s} a_{i,e_i}^{(-\delta)} \\ &= \frac{S_0}{2^{2s-2}} + \frac{2^{s(m_0-1)}-1}{2^{s-1}(2^s-1)} \sum_{\substack{e_1,\cdots,e_s\in\{1,-1\} \\ e_1\cdots e_s=-\delta}} \prod_{i=1}^{s} d_{i,\delta_i}^{(\delta)} a_{i,e_i}^{(-\delta)},\end{aligned}$$

where S_0 is bounded by (5.22). Since $\delta_1\delta_2\cdots\delta_s = -e_1e_2\cdots e_s$ and s is even, there exists at least one j such that $e_j = \delta_j$. For this j we have, by (5.19),

$$d_{j,\delta_j}^{(\delta)} a_{j,e_j}^{(-\delta)} = d_{j,\delta_j}^{(\delta)} \left(d_{j,e_j}^{(-\delta)} - 1\right) \le q_{j,\delta_j} - 1 \le \frac{p_j-\delta_j}{2^{m_0}} - 1.$$

If $e_i = -\delta_i$ then

$$d_{i,\delta_i}^{(\delta)} a_{i,e_i}^{(-\delta)} = d_{i,\delta_i}^{(\delta)} \left(d_{i,-\delta_i}^{(-\delta)} - 1\right) \le q_{i,\delta_i} q_{i,-\delta_i} - 1 \le \frac{p_i^2-1}{2^{m_0+1}} - 1.$$

Since $\frac{p_i-\delta_i}{2^{m_0}} - 1 < \frac{p_i^2-1}{2^{m_0+1}} - 1$, we have

$$\begin{aligned}\prod_{i=1}^{s} d_{i,\delta_i}^{(\delta)} a_{i,e_i}^{(-\delta)} &\le \frac{p_j-\delta_j-2^{m_0}}{2^{m_0}} \prod_{i\ne j} \frac{p_i^2-1-2^{m_0+1}}{2^{m_0+1}} \le \frac{p_j-3}{2^{s(m_0+1)-1}} \prod_{i\ne j}(p_i^2-9) \\ &= \frac{\prod_{i=1}^{s}(p_i^2-9)}{2^{s(m_0+1)-1}(p_j+3)} < \frac{n^2-4n}{2^{s(m_0+1)-1}(p_1+1)}.\end{aligned}$$

Thus

$$\begin{aligned}\mathrm{SB}(n,1)\mathrm{SB}(n,-1) &< \frac{S_0}{2^{2s-2}} + \frac{2^{s(m_0-1)}-1}{2^{s-1}(2^s-1)} \cdot 2^{s-1} \cdot \frac{n^2-4n}{2^{s(m_0+1)-1}(p_1+1)} \\ &< \Big(\frac{1}{2^{3s-2}} + \frac{1}{2^{2s-1}(2^s-1)}\Big)\frac{n^2-4n}{p_1+1},\end{aligned}$$

and therefore

$$\begin{aligned}\tau(n) &= \frac{\mathrm{SB}(n,1)\mathrm{SB}(n,-1)}{(n-1)(n-3)/4} \\ &< \Big(\frac{1}{2^{3s-4}} + \frac{1}{2^{2s-3}(2^s-1)}\Big)\frac{1}{p_1+1} < \frac{1}{8^{s-4}\cdot 166(p_1+1)}.\end{aligned}$$

□

Remark 5.3. In Lemma 5.8, if $p_1 > 2000$ by trial divisions, then $\tau(n) < \frac{1}{8^{s-4}\cdot 332332}$.

Lemma 5.9. *Let $n = p_1p_2\cdots p_s$ be square free with each p_i an odd prime and s odd ≥ 5. Then*

$$\tau(n) < \frac{1}{2^{5s-4}} + \frac{1}{2^{3s-3}(2^s-1)} < \frac{1}{16^{s-5}\cdot 119726}. \tag{5.23}$$

Proof. Let $\delta_1, \delta_2, \cdots, \delta_s \in \{1,-1\}$ be such that $m(\delta_1,\delta_2,\cdots,\delta_s) = m_0 \geq 2$. Thus $m(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s) = 1$ for all other 2^s-1 s-tuples $(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_s)$. Put $\delta = \delta_1\delta_2\cdots\delta_s$. By (5.20) and (5.19) we have

$$\begin{aligned}&\Big(a_{i,1}^{(1)} + a_{i,-1}^{(1)}\Big)\Big(a_{i,1}^{(-1)} + a_{i,-1}^{(-1)}\Big) \\ &\quad\leq \Big(a_{i,1}^{(1)} + a_{i,1}^{(-1)}\Big)\Big(a_{i,-1}^{(1)} + a_{i,-1}^{(-1)}\Big) + a_{i,1}^{(1)}a_{i,1}^{(-1)} + a_{i,-1}^{(1)}a_{i,-1}^{(-1)} \\ &\quad\leq \big(q_{i,1}-1\big)\big(q_{i,-1}-1\big) + q_{i,1} - 1 + q_{i,-1} - 1 = q_{i,1}q_{i,-1} - 1 \\ &\quad\leq \frac{p_i^2-1}{2^{m_0+1}} - 1 \leq \frac{p_i^2-9}{2^{m_0+1}}.\end{aligned}$$

Let S_0 be as given by (5.21); then

$$S_0 \leq \prod_{i=1}^{s}\left(\Big(a_{i,1}^{(1)} + a_{i,-1}^{(1)}\Big)\Big(a_{i,1}^{(-1)} + a_{i,-1}^{(-1)}\Big)\right) \leq \prod_{i=1}^{s}\frac{p_i^2-9}{2^{m_0+1}} < \frac{n^2-4n}{2^{(m_0+1)s}}. \tag{5.24}$$

Again by (5.20) and (5.19) we have

$$\begin{aligned}d_{i,\delta_i}^{(\delta)}\Big(a_{i,1}^{(-\delta)} + a_{i,-1}^{(-\delta)}\Big) &= d_{i,\delta_i}^{(\delta)}\Big(d_{i,1}^{(-\delta)} - 1 + d_{i,-1}^{(-\delta)} - 1\Big) \\ &= d_{i,\delta_i}^{(\delta)}d_{i,\delta_i}^{(-\delta)} - d_{i,\delta_i}^{(\delta)} + d_{i,\delta_i}^{(\delta)}\Big(d_{i,-\delta_i}^{(-\delta)} - 1\Big) \\ &\leq q_{i,\delta_i} - 1 + q_{i,\delta_i}\big(q_{i,-\delta_i} - 1\big) = q_{i,1}q_{i,-1} - 1 \leq \frac{p_i^2-9}{2^{m_0+1}}.\end{aligned}$$

Thus

$$\begin{aligned}\mathrm{SB}(n,1)\mathrm{SB}(n,-1) &= \frac{S_0}{2^{2s-2}} + \frac{2^{s(m_0-1)}-1}{2^{s-1}(2^s-1)} \sum_{\substack{e_1,\cdots,e_s\in\{1,-1\}\\ e_1\cdots e_s=-\delta}} \prod_{i=1}^{s} d_{i,\delta_i}^{(\delta)} a_{i,e_i}^{(-\delta)} \\ &\le \frac{S_0}{2^{2s-2}} + \frac{2^{s(m_0-1)}-1}{2^{s-1}(2^s-1)} \prod_{i=1}^{s} d_{i,\delta_i}^{(\delta)} \left(a_{i,1}^{(-\delta)} + a_{i,-1}^{(-\delta)}\right) \\ &\le \frac{S_0}{2^{2s-2}} + \frac{2^{s(m_0-1)}-1}{2^{s-1}(2^s-1)} \prod_{i=1}^{s} \frac{p_i^2-9}{2^{m_0+1}} \\ &< \Big(\frac{1}{2^{(m_0+3)s-2}} + \frac{1}{2^{3s-1}(2^s-1)}\Big)(n^2-4n),\end{aligned}$$

where S_0 is bounded by (5.24). Therefore

$$\begin{aligned}\tau(n) = \frac{\mathrm{SB}(n,1)\mathrm{SB}(n,-1)}{(n-1)(n-3)/4} &< \frac{1}{2^{(m_0+3)s-4}} + \frac{1}{2^{3s-3}(2^s-1)} \\ &\le \frac{1}{2^{5s-4}} + \frac{1}{2^{3s-3}(2^s-1)} < \frac{1}{16^{s-5}\cdot 119726}.\end{aligned}$$

□

Remark 5.4. From the proof of Lemma 5.9 we see that if n in Lemma 5.9 satisfies the additional condition

$$k_{i,\delta_i} = m_0\ (\ge 2),\ q_{i,\delta_i} \mid q_\delta,\ \text{ and }\ q_{i,-\delta_i} \mid q_{-\delta},\ \text{for all } 1 \le i \le s, \tag{5.25}$$

where k_{i,δ_i}, q_{i,δ_i} are given by (2.10), then it seems that (5.23) is the limit of the analysis in this paper and cannot be significantly improved. Otherwise if n in Lemma 5.9 does not satisfy condition (5.25), or in other words, if it satisfies the condition

$$k_{j,\delta_j} > m_0\ (\ge 2),\ \text{ or } q_{j,\delta_j} \nmid q_\delta,\ \text{ or }\ q_{j,-\delta_j} \nmid q_{-\delta},\ \text{for some } j : 1 \le j \le s, \tag{5.26}$$

then

$$d_{j,\delta_j}^{(\delta)}\left(a_{j,1}^{(-\delta)} + a_{j,-1}^{(-\delta)}\right) \le \begin{cases} q_{j,1}q_{j,-1} - 1 \le \frac{p_j^2-17}{2^{m_0+2}}, & \text{if } k_{j,\delta_j} > m_0; \\ q_{j,1}q_{j,-1}/3 - 1 \le \frac{p_j^2-25}{2^{m_0+1}\cdot 3}, & \text{if } q_{j,\delta_j} \nmid q_\delta,\ \text{or }\ q_{j,-\delta_j} \nmid q_{-\delta}; \end{cases}$$

thus

$$\tau(n) < \frac{1}{2^{(m_0+3)s-4}} + \frac{1}{2^{3s-2}(2^s-1)} \le \frac{1}{2^{5s-4}} + \frac{1}{2^{3s-2}(2^s-1)} < \frac{1}{16^{s-5}\cdot 226521}. \tag{5.27}$$

Remark 5.5. Since condition (5.25) is very strict, most composites of Lemma 5.9 satisfy (5.26) instead of (5.25). So, $\tau(n)$ is bounded by (5.27) for most square free composites n having an odd number $s \ge 5$ of prime factors.

6. Proof of Theorem 4

For $\varepsilon \in \{1,-1\}$ and odd $n > 1$, let $J(n,\varepsilon)$ be as defined in (3.2). To prove Theorem 4 we need a lemma.

Lemma 6.1. *Let $n > 1$ be odd and $\varepsilon \in \{1,-1\}$. If n is not a perfect square, then*

$$J(n,\varepsilon) \le (n-\varepsilon-2)/2.$$

Proof. Case (I). $n = p^k$ with p prime and k odd. By Lemma 3.1 we have

$$J(p, \varepsilon) = (p - \varepsilon - 2)/2.$$

Thus we have

$$J(n, \varepsilon) = p^{k-1}(p - \varepsilon - 2)/2 \leq (n - \varepsilon - 2)/2.$$

Case (II). $n = p^k q$ with p prime, k odd, $q > 1$, and $\gcd(p, q) = 1$. By the Chinese Remainder Theorem we have

$$\begin{aligned} J(n, \varepsilon) &= J(p^k, 1)J(q, \varepsilon) + J(p^k, -1)J(q, -\varepsilon) \leq \frac{p^k - 3}{2} J(q, \varepsilon) + \frac{p^k - 1}{2} J(q, -\varepsilon) \\ &< \frac{p^k - 1}{2}(J(q, 1) + J(q, -1)) \leq \frac{p^k - 1}{2}(q - 2) < \frac{n - 3}{2} \leq \frac{n - \varepsilon - 2}{2}. \end{aligned}$$

□

Proof of Theorem 4. If n is a prime ≥ 5, then u and v in Steps 2 and 3 exist. Since the prime n is not a perfect square but a probable prime to both T_u and T_v, it passes the OPQBT.

If n is not declared composite in Steps $1 - 3$, then n is almost certainly prime with probability of error $\tau(n, \varepsilon)\tau(n, -\varepsilon) = \tau(n)$. □

Remark 6.1. One may relax the OPQBT so that the probable prime subtests in Steps 2 and 3 are no longer strong. Then the probability of error will be $\tau_0(n)$. In Step 2 one may chose $u = 3$ for odd $n > 5$. Thus $\varepsilon = (5/n)$. In Step 3 one chooses $v = 4, 5, \cdots$ in succession. There are 4152 $\mathrm{psp}(T_3)$'s $< 10^9$, not a single one of which passes Step 3 to bases as chosen in this way.

7. Proof of Theorem 5

Lemma 7.1. *It takes* $(2 + o(1)) \log_2 q$ *multiplications* $\bmod n$ *to check if* $T_u^q \equiv \pm 1 \bmod n$ *in the ring* $R_u = \mathbb{Z}[T]/(T^2 - uT + 1)$, *assuming that addition takes* $o(1)$ *multiplications* $\bmod n$.

Proof. The Lucas sequences U_i, V_i with parameters $P = u$ and $Q = 1$ defined by (1.3) are

$$\begin{aligned} &U_0 = 0,\ U_1 = 1,\ V_0 = 2,\ V_1 = u, \\ &U_i = uU_{i-1} - U_{i-2},\ V_i = uV_{i-1} - V_{i-2}, \quad \text{for } i \geq 2. \end{aligned} \tag{7.1}$$

Then (cf. Chap.12 of [5], or [24])

$$U_{2i} = U_i V_i,\ V_{2i} = V_i^2 - 2; \tag{7.2}$$

$$U_{i+j} = \frac{1}{2}(U_i V_j + U_j V_i),\ V_{i+j} = \frac{1}{2}(V_i V_j + (u^2 - 4)U_i U_j); \tag{7.3}$$

and in the ring R_u

$$T_u^q = U_q T_u + \frac{1}{2}(V_q - uU_q). \tag{7.4}$$

Thus

$$T_u^q \equiv \pm 1 \mod n \iff U_q \equiv 0 \mod n \text{ and } V_q \equiv \pm 2 \mod n.$$

So, our task is to compute $U_q \bmod n$ and $V_q \bmod n$. We use easily constructed addition chains (cf. page 441 of [13]) as follows.

Take $h = \lfloor \frac{1}{2} \log_2 \log_2 q \rfloor$, $m = 2^h < \log_2^{1/2} q$. Write

$$q = d_0 m^t + d_1 m^{t-1} + \cdots + d_{t-1} m + d_t, \quad \text{with } 0 \le d_i < m,\ 0 \le i \le t,\ d_0 \ge 1;$$

then $t = \lfloor \log_m q \rfloor + 1 < \frac{\log_2 q}{h} + 1$.

Step 1. Using (7.1) to compute U_i, V_i for $2 \le i \le m-1$ takes $2(m-2)$ multiplications mod n.

Step 2.1. Using (7.2) to compute $U_{2^j d_0}$, $V_{2^j d_0}$ for $1 \le j \le h$ takes $2h$ multiplications mod n.

Step 2.2. Using (7.3) to compute $U_{md_0+d_1}$, $V_{md_0+d_1}$ takes 7 multiplications mod n.

Step 3.1. Using (7.2) to compute $U_{2^j(md_0+d_1)}$, $V_{2^j(md_0+d_1)}$ for $1 \le j \le h$ takes $2h$ multiplications mod n.

Step 3.2. Using (7.3) to compute $U_{m^2d_0+md_1+d_2}$, $V_{m^2d_0+md_1+d_2}$ takes 7 multiplications mod n.

. . . . . .

Step t.1. Using (7.2) to compute

$$U_{2^j(m^{t-1}d_0+m^{t-2}d_1+\cdots+d_{t-1})},\ V_{2^j(m^{t-1}d_0+m^{t-2}d_1+\cdots+d_{t-1})}$$

for $1 \le j \le h$ takes $2h$ multiplications mod n.

Step t.2. Using (7.3) to compute U_q, V_q takes 7 multiplications mod n.

So it takes in total

$$2(m-2) + (2h+7)(t-1) < (2 + 7/h)\log_2 q + 2\log_2^{1/2} q - 4 = (2 + o(1))\log_2 q$$

multiplications mod n. □

Proof of Theorem 5. Write $n - \varepsilon = 2^k q$ with q odd. By Lemma 7.1, it takes $(2+o(1))$ multiplications mod n to compute U_q, V_q, and thus to check if $T_u^q \equiv \pm 1 \mod n$ in the ring $R_u = \mathbb{Z}[T]/(T^2 - uT + 1)$. By (7.4), we have

$$T_u^{2^i q} \equiv -1 \mod n \iff U_{2^i q} \equiv 0 \mod n \text{ and } V_{2^i q} \equiv -2 \mod n.$$

So the remaining task is using (7.2) to compute $U_{2^i q} \mod n$ and $V_{2^i q} \mod n$ for $1 \le i \le k-1$, which takes $2(k-1)$ multiplications mod n. Since $k + \log_2 q = \log_2(n-\varepsilon) \le \log_2(n+1) < \log_2 n + 1$, we get

$$(2 + o(1))\log_2 q + 2(k-1) < 2(k + \log_2 q) + o(1)\log_2 q < (2 + o(1))\log_2 n.$$

This means that it takes $(2 + o(1))\log_2 n$ multiplications mod n to do an sprp subtest in Step 2 or 3. Since the time it takes to check if n is a perfect square and to compute the Jacobi symbols is negligible, (an iteration of) the One-Parameter Quadratic-Base Test can be completed in the time it takes to perform at most $(4 + o(1))\log_2 n$ multiplications mod n. □

8. Comparisons

It is clear that comparisons between the OPQBT and either the Rabin-Miller test or the Lucas test are crucial. So, the main task of this section is to give comparisons between the RQFT and the OPQBT.

Let $\mathrm{Gran}(n)$ denote the error probability of the RQFT. From Lemma 2.7, Corollary 2.10, Lemma 2.11 and Lemma 2.12 of Grantham [9] we know that

(8.1)

$$\mathrm{Gran}(n) \le \begin{cases} 4/p, & \text{for } n \text{ nonsquare free with } p^2 \mid n,\ p \text{ prime;} \\ 2/B, & \text{for } n \text{ square free with } s \text{ even} \ge 2; \\ \frac{4}{B^2} + \frac{3(B^2+1)}{2(B^4-3B^2)} \approx \frac{5.5}{B^2}, & \text{for } n \text{ square free with } s = 3; \\ \frac{1}{2^{3s-2}} + \frac{1}{2^{4s-3}} + \frac{4}{B^2}, & \text{for } n \text{ square free with } s \text{ odd} \ge 5; \end{cases}$$

where $B \le p_1 - 1$, the trial division bound ($B = 50000$ suggested by [9]).

We see that for a nonsquare free composite n with a prime square factor p^2, $\mathrm{Gran}(n) < 4/p$, whereas $\tau(n) < 1/(4^s p^2)$. Moreover $\mathrm{Gran}(n)$ is bounded by constants for all square free composites—it is bounded by $2/B$ when s is even, and by $\frac{4}{B^2} + \frac{1}{2^{3s-2}} + \frac{1}{2^{4s-3}} \to \frac{4}{B^2}$ as $s \to \infty$ when s is odd; but $\tau(n) \to 0$ as $s \to \infty$ (s either even or odd, see Theorem 3). Most remarkable is that comparisons between $\mathrm{Gran}(n)$ and $\tau(n)$ for square free composites with 2 or 3 prime factors are crucial.

The worst case of both the RQFT and the OPQBT happens when $n = p_1 p_2 p_3 p_4 p_5$ is the product of 5 different odd primes. For such composites n,

$$\mathrm{Gran}(n) < 1/2^{13} + 1/2^{17} + 1/25000^2 \approx 1/7710,$$

which needs the additional condition $p_1 > B = 50000$; but (cf. Lemma 5.9 and Remark 5.4)

$$\tau(n) < \begin{cases} 1/119726, & \text{for } n \text{ satisfying (5.25);} \\ 1/226521, & \text{for } n \text{ satisfying (5.26);} \end{cases}$$

which does not need the condition $p_1 > 50000$. If we take $B = 3$, then the bound for $\mathrm{Gran}(n)$ would be about $4/9$, but the bound for $\tau(n)$ still remains $1/119726$ or $1/226521$.

The Rabin-Miller test takes $(1 + o(1)) \log_2 n$ multiplications mod n (Proposition 3.1 of [9]). Thus the running time of the OPQBT is asymptotically at most 4 times that of the Rabin-Miller test. Since most composites are not $\mathrm{spsp}(T_u)$, the OPQBT stops at Step 2, taking only twice the time it takes to do a Rabin-Miller test. But the running time of the RQFT is asymptotically 3 times that of the Rabin-Miller test for all numbers. So the OPQBT runs faster than the RQFT (3:2) for most composites.

Since the running time of the RQFT is asymptotically faster (4:3) than the OPQBT for the worst cases, one may ask the follow question: With equal work, one test is how many times as confident as the other for a given number n?

To make the answer unique, it is reasonable to make the following definition, which balances comparisons of the error probabilities and the running time of two tests.

Definition 8.1. Given two tests Test_1 and Test_2. Test_i has error probability $\le P_i = P_i(n)$ and running time $t_i = t_i(n)$ for a given number n. Define the function

$$\mathrm{Balance}(\mathrm{Test}_1, \mathrm{Test}_2, n) \approx \frac{(1/P_1)^{t_2/t_1}}{1/P_2}.$$

If $\mathrm{Balance}(\mathrm{Test}_1, \mathrm{Test}_2, n) \approx k$, then we say that, with equal work, Test_1 is k times as confident as Test_2 for the number n, and say that Test_1 is Balance-better (resp. the same or worse) than Test_2 for the number n if $k > 1$ (resp. $k = 1$, or $k < 1$).

Take

(8.2)

$$\text{Test}_1 = \text{RQFT}, \text{Test}_2 = \text{OPQBT}, t_2/t_1 = 4/3, P_1 = \text{Gran}(n), \text{ and } P_2 = \tau(n),$$

then by Theorem 3 and (8.1) we have (with $B = 50000 \le p_1 - 1$),

$$\text{Balance}(\text{RQFT}, \text{OPQBT}, n)$$

$$\approx \begin{cases} \frac{0.16}{n^{8/9}}, & \text{for } n \text{ nonsquare free with } s = 1; \\ \frac{731004}{n^{2/3}}, & \text{for } n \text{ square free with } s = 2; \\ \frac{3.495 \cdot 10^{11}}{n^{2/7}}, & \text{for } n \text{ square free with } s = 3; \\ \frac{351}{2^{3s}}, & \text{for } n \text{ square free with } s \text{ even} \ge 4; \\ 1.272, & \text{for } n \text{ square free satisfying (5.25) with } s = 5, 7, 9; \\ 0.673, & \text{for } n \text{ square free satisfying (5.26) with } s = 5, 7, 9; \\ \frac{0.266}{16^{s-11}}, & \text{for } n \text{ square free with } s \text{ odd} \ge 11; \\ \frac{\prod_{p_j^2 \mid n} (p_j/4)^{4/3}}{4^s \prod_{i=1}^{s} p_i^{2(r_i-1)}}, & \text{otherwise, i.e., for } n \text{ nonsquare free with } s \ge 2. \end{cases}$$

So, the RQFT is (slightly) Balance-better than the OPQBT only when n is square free satisfying (5.25) with $s = 5, 7, 9$. As mentioned in Remark 5.5, such numbers are rare. We challenge the reader to exhibit one. If there are none, then the OPQBT is Balance-better than the RQFT for all composites.

Remark 8.1. Even for the rare composites n square free satisfying (5.25) with $s = 5, 7, 9$, it is possible that the OPQBT is Balance-better than the RQFT. The running time of the RQFT is asymptotically $(3 + o(1)) \log_2 n$ multiplications mod n for all numbers n, and that of the OPQBT is asymptotically $(4 + o(1)) \log_2 n$ multiplications mod n for numbers n of the worst cases. Here both $o(1)$ represent

$$O\left(\frac{1}{\log_2 \log_2 n}\right)$$

but with different constants related to the big$-O$ notations. Since the RQFT works in the ring $\mathbb{Z}[x]/(n, x^2 - bx - c)$ and needs the additional Step 5, whereas the OPQBT works in the ring $\mathbb{Z}[x]/(n, x^2 - ux + 1)$, the constants related to the big$-O$ notations for the RQFT are larger than that for the OPQBT. So it is possible in (8.2) that t_2/t_1, say, $\approx 4.11/3.15$, for a range of numbers n, say, $n < 10^{1000}$. Then for n square free satisfying (5.25) with $s = 5, 7, 9$ we have

$$\text{Balance}(\text{RQFT}, \text{ OPQBT}, n) \approx \frac{7710^{4.11/3.15}}{119726} \approx 0.985.$$

Since both the RQFT and the OPQBT run very fast, it is not of great interests to analyze them in exact bit operations.

Remark 8.2. From Definition 2.2 we see that the OPQBT is a combination of two subtests to one-parameter quadratic bases with opposite Jacobi signs. The RQFT, in a sense, is a combination of an sprp subtest to a two-parameter quadratic base with negative Jacobi sign, and a Rabin-Miller subtest. The key difference between the OPQBT and the RQFT is that the bases of two subtests of the OPQBT are *independently* chosen, whereas the base of the Rabin-Miller subtest of the RQFT is *dependent* on the quadratic base of the two-parameter-quadratic-base subtest.

9. Conclusions

From Remarks 2.1 and 2.2 we see that an sprp(T_u) subtest with $\left(\frac{u^2-4}{n}\right) = 1$ is a generalized Rabin-Miller test, and an sprp(T_u) subtest with $\left(\frac{u^2-4}{n}\right) = -1$ is a stronger lprp(u,1) test. So, the OPQBT is in fact a more general and strict version of the Baille-PSW test. The worst case for each sprp(T_u) subtest with either $\left(\frac{u^2-4}{n}\right) = 1$ or $\left(\frac{u^2-4}{n}\right) = -1$ is the case where $n = p_1p_2$ is the product of two different odd primes; but this case becomes one of the best cases for the OPQBT. Thus Theorems 2, 3 and 4 have answered the question of why the Baille-PSW test seems much more secure than one might expect considering each subtest separately.

Theorems 3 and 4 have also answered the question of why it is difficult to find counter-examples to the Baille-PSW test although many such numbers exist, since the best heuristics for constructing such numbers [18] would produce square free composites n with a large number s of prime factors, but Theorem 3 (Lemmas 5.8 and 5.9) shows that $\tau(n)$ decreases rapidly for such composites n while s increases. We challenge the reader to exhibit a composite which passes the OPQBT to bases as chosen in Remark 6.1.

The OPQBT, based on one-parameter quadratic-base pseudoprimes, has clear finite group (field) structure and nice symmetry, so that explicit formulas for the base-counting functions and probability of error can be given, and thus bounds for these functions can be carefully investigated. While no explicit formulas are given, neither for the original versions of the Baille-PSW test nor for the RQFT, the OPQBT would be one of the most suitable candidates among existing probable prime tests, which would lead to infallible tests for primality.

Acknowledgments

I thank F. Arnault, W. Bosma, D.M. Bressoud, J. Grantham, A.K. Lenstra, H.W. Lenstra, Jr., C. Pomerance, S.S. Wagstaff, Jr., and H.C. Williams for sending me reprints concerning this subject or other topics in computational number theory. Especially I would like to thank C. Pomerance and the referees for helpful comments on the original version of this paper.

References

1. W.R.Alford, A.Granville and C.Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math., **140** (1994), 703–722. MR **95k:**11114
2. W.R.Alford, A.Granville and C.Pomerance, *On the difficulty of finding reliable witnesses*, Algorithmic Number Theory, pp.1-16, Lecture Notes in Computer Science, vol.877, Springer-Verlag, Berlin, 1994. MR **96d:**11136
3. F.Arnault, *The Rabin-Monier theorem for Lucas pseudoprimes*, Math.Comp., **66** (1997), 869-881. MR **97f :**11009
4. R.Baillie and Samuel S.Wagstaff,Jr., *Lucas pseudoprimes*, Math.Comp., **35** (1980), 1391-1417. MR **81j :**10005
5. D.M.Bressoud, *Factorization and primality testing*, Springer-Verlag, New York, 1989. MR **91e:**11150
6. H.Cohen, *A Course in Computational Algebraic Number Theory*, 3., corr. print. Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1996. MR **94i:**11105 (1st ed.)
7. H.Cohen and A.K.Lenstra, *Implementation of a new primality test*, Math.Comp., **48** (1987), 103-121. MR **88c:**11080
8. H.Cohen and H.W.Lenstra, Jr., *Primality testing and Jacobi sums*, Math.Comp., **42** (1984), 297–330. MR **86g:**11078

9. J. Grantham, *A probable prime test with high confidence*, J. Number Theory, **72** (1998), 32-47. MR **2000e:**11160
10. J. Grantham, *Frobenius Pseudoprimes*, Math.Comp., **70** (2001), 873–891. MR **2001g:**11191
11. R. K. Guy, *Unsolved Problems in Number Theory*, Second Edition, Springer-Verlag, New York, 1994. MR **96e:**11002
12. L.K.Hua, *An introduction to number theory*, Springer-Verlag, New York, 1982. MR **83f:**10001
13. D.E.Knuth, *The art of computer programming : Semi-numerical algorithms*,, Volume 2, 2nd ed., Addison Wesley, Reading Massachusetts, 1981. MR **83i:**68003
14. H.W.Lenstra, Jr., *Primality testing*, Computational Methods in Number Theory (H.W. Lenstra, Jr. and R.Tijdeman, eds.), Part I, Math. Centre Tract, vol.**154**, Amsterdam, 1982, pp.55-77. MR **85g:**11117
15. G.Miller, *Riemann's hypothesis and tests for primality*, J. Comput. and System Sci., **13** (1976),300-317. MR **58:**470ab
16. Louis Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science, **12** (1980), 97-108. MR **82a:**68078
17. R.G.E.Pinch, *The Carmichael numbers up to* 10^{15}, Math.Comp., **61** (1993), 381-389. MR **93m:**11137
18. C.Pomerance, *Are there counter-examples to the Baillie-PSW primality test?*, Dopo Le Parole aangeboden aan Dr. A.K. Lenstra (H.W.Lenstra, Jr., J.K.Lenstraand P.Van Emde Boas, eds.), Amsterdam,1984.
19. C.Pomerance, J.L.Selfridge and Samuel S.Wagstaff,Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math.Comp., **35** (1980), 1003-1026. MR **82g:**10030
20. M.O.Rabin, *The probabilistic algorithms for testing primality*, J.Number Theory, **12** (1980), 128-138. MR **81f :**10003
21. K.H.Rosen, *Elementary number theory and its applications*, Addison Wesley, Reading Massachusetts, 1984. MR **85m:**11002
22. H.C.Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bull. **20** (1977), 133-143. MR **56:**5414
23. Zhenxiang Zhang, *Finding strong pseudoprimes to several bases*, Math.Comp., **70** (2001), 863–872. MR **2001g:**11009
24. Zhenxiang Zhang, *Using Lucas sequences to factor large integers near group orders*, The Fibonacci Quarterly, **39** (2001), 228–237. MR **2002c:**11173

Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, P. R. China

E-mail address: zhangzhx@mail.ahwhptt.net.cn