Hindawi
Journal of Mathematics
Volume 2022, Article ID 7034529, 10 pages
https://doi.org/10.1155/2022/7034529

Research Article

A Simple Algorithm for Prime Factorization and Primality Testing

Kabenge Hamiss [1,2]

[1]*Department of Mathematics and Statistics, Islamic University in Uganda, Mbale 2555, Uganda*
[2]*Department of Mathematical and Computer Sciences, University of Gezira, Wad Medani 20, Sudan*

Correspondence should be addressed to Kabenge Hamiss; kabenhami@gmail.com

Received 1 September 2022; Revised 31 October 2022; Accepted 7 November 2022; Published 15 December 2022

Academic Editor: Niansheng Tang

We propose a new simple and faster algorithm to factor numbers based on the nature of the prime numbers contained in such composite numbers. It is well known that every composite number has a unique representation as a product of prime numbers. In this study, we focus mainly on composite numbers that contain a product of prime numbers that are greater than or equal to 5 which are of the form $6k + 1$ or $6k + 5$. Therefore, we use the condition that every prime or composite P of primes greater than or equal to 5 satisfies $P^2 \equiv 1 \pmod{24}$. This algorithm is very fast especially when the difference in the prime components of a composite number (prime gap) is not so large. When the difference between the factors (prime gap) is not so large, it often requires just a single iteration to obtain the factors.

1. Introduction

An integer p is prime if $p \geq 2$ and has exactly two positive divisors, namely, 1 and p itself [1–5]. An integer n is called a composite if $n \geq 2$ and n have more than two positive divisors [6–9].

Any composite number (integer) can be decomposed into smaller integers called prime factors, for which their multiplication produces the original integer. The process of decomposing such numbers is called integer factorization [7, 10–12].

Over the years, the prime factorization of large numbers has drawn much attention due to its practical applications and the associated challenges [13, 14]. In computing applications, encryption algorithms such as the Rivest–Shamir–Adleman (RSA) cryptosystems are widely used for information security, where the keys (public and private) of the encryption code are represented using large prime factors [15–21]. Since prime factorization of large numbers is extremely hard, RSA cryptosystems take advantage of this property to ensure information security [10, 22, 23].

Many efforts have been made to develop an effective method of factoring numbers and to know whether a number is prime or not [24, 25]. They include Sieve of Eratosthenes, Pollard's Algorithm, special-purpose factorization algorithm, general-purpose, Special Generic Factorizations, Williams' $P + 1$ Method, and Lenstra's Elliptic Curve Method, among others [2, 22, 26–30].

1.1. Congruences. We say that a divides b if there is some integer c such that $b = ac$. If a divides b, we write $a \mid b$, and if a does not divide b we write $a \nmid b$.

If $m \mid (a - b)$, we write

$$a \equiv b \pmod{m}, \tag{1}$$

and say that a is congruent to b modulo m. The quantity m is called the modulus and all numbers congruent (or equivalent) to $a \pmod{m}$ are said to constitute a congruence (or equivalence) class [7, 31–33]. According to [34], an algorithm is a precise step-by-step series of rules that leads to a product or to the solution to a problem. Some steps in an algorithm depend on what happened or was learned in earlier steps.

2. The Main Result

Let p and q be prime numbers greater than or equal to 5. Porras Ferreira and Willian De Jesus [35] proved that prime numbers p and q are representatives of $5 \pmod{6}$ or $1 \pmod{6}$ implying

$$p \equiv 5 \ (\text{mod}6),$$
$$q \equiv 1 \ (\text{mod}6). \tag{2}$$

Then, for some integers t and r,

$$p = 6t + 5,$$
$$q = 6r + 1. \tag{3}$$

Now, as it was earlier proven by Porras Ferreira and Willian De Jesus [35] that if m is a composite of primes greater or equal to 5, then $m^2 \equiv 1$ (mod6).

Theorem 1. *Let m be a composite containing at least one prime $s < 5$; then,*

$$m^2 \equiv s^{2k} \ (\text{mod}24), \tag{4}$$

where k is a positive integer.

Proof. Let p_i (where $i = 1, 2, ..., n$) be primes greater or equal to 5 and s be a prime less than 5 such that $m = s^k p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ be a composite of primes.

Since k and k_i are positive integers, then

$$p_1^{2k_1} \equiv 1 \ (\text{mod}24),$$
$$p_2^{2k_2} \equiv 1 \ (\text{mod}24), \ldots, \tag{5}$$
$$p_n^{2k_n} \equiv 1 \ (\text{mod}24).$$

From the property in [7] of multiplication, then multiplying p_i^2 in (5) together, we obtain

$$p_1^{2k_1} p_2^{2k_2} \ldots p_n^{2k_n} \equiv 1 \ (\text{mod}24). \tag{6}$$

Multiplying s^{2k} both side in (6), we obtain

$$s^{2k} p_1^{2k_1} p_2^{2k_2} \ldots p_n^{2k_n} \equiv s^{2k} \ (\text{mod}24). \tag{7}$$

However, $m^2 = s^{2k} p_1^{2k_1} p_2^{2k_2} \ldots p_n^{2k_n}$ implying

$$m^2 \equiv s^{2k} \ (\text{mod}24). \tag{8}$$

Thus, the theorem is proven.

This indicates that any composite number that contains at least one prime less than 5 does not satisfy the condition of 1 (mod24).

Therefore, from this point, we can analyze the conditions that will determine any integer to be a prime or a composite. □

2.1. Composite of the Form $6k + 1$. As stated earlier, not all numbers of the form $6k + 1$ are primes, now, we prove to back up the statement.

Case 1. Let m be a composite of at least two prime say of the form $6t + 1$ and $6r + 1$, that is, $m = (6t + 1)(6r + 1)$:

$$m = 36tr + 6(r + t) + 1,$$
$$m = 6[6rt + (r + t)] + 1. \tag{9}$$

Let $6rt + (r + t) = k$ be an integer. Then,

$$m = 6k + 1. \tag{10}$$

Case 2. Let m be a composite of at least two primes of the form $6t + 5$ and $6r + 5$; that is, $m = (6t + 5)(6r + 5)$:

$$m = 36tr + 30(r + t) + 25,$$
$$m = 6[6tr + 5(r + t) + 4] + 1. \tag{11}$$

Let $n = 6tr + 5(r + t) + 4$ an integer. Then,

$$m = 6n + 1. \tag{12}$$

2.2. Composite of the Form $6k + 5$. Let m be a composite of at least two primes of the form $6t + 5$ and $6r + 1$; that is, $m = (6t + 5)(6r + 1)$:

$$m = 36tr + 6t + 30r + 5,$$
$$m = 6[6tr + (5r + t)] + 5. \tag{13}$$

Let $k = 6tr + (5r + t)$ an integer. Then,

$$m = 6k + 5. \tag{14}$$

Equations (10), (12), and (14) really show that not all numbers of the form $6k + 1$ or $6k + 5$ are primes. Some of which are pseudoprimes and others just ordinary odd numbers.

As we can observe from the above mentioned equations, the values of r and t will determine whether the number is prime or not a prime.

We also observe that it is difficult to distinguish between composites of the form $(6t + 1)(6r + 1)$ and $(6t + 5)(6r + 5)$ because they both give the same result, that is, $6k + 1$.

2.3. Composites of the Form $6k + 1$ and Their Factorization

Case 3. $P = (6t + 1)(6r + 1)$.

Theorem 2. *Let*

$$P = (6t + 1)(6r + 1). \tag{15}$$

Then, there exists some integer A such that

$$A \equiv (r + t) \quad (\text{mod}6). \tag{16}$$

Proof. From

$$P = (6t + 1)(6r + 1) = 6[6tr + (r + t)] + 1. \tag{17}$$

Then,

$$P - 1 = 6[6tr + (r + t)]. \tag{18}$$

Dividing through by 6, we obtain

$$\frac{P - 1}{6} = (r + t) + 6rt. \tag{19}$$

Now, let $A = (P - 1/6)$ and $u = rt$ implying that 20 becomes

$$A = (r + t) + 6u. \tag{20}$$

Hence, we obtain

$$A \equiv (r + t) \pmod 6. \tag{21}$$

□

Lemma 1. *If $r + t = A$, then either $r = A$, $t = 0$ or $r = 0$, $t = A$ is a solution (trivial solution) to (16).*

Proof. Let $r + t = A$. We know that $u = tr = 0$. Then, it implies that $r = A - t$:

$$t(A - t) = 0. \tag{22}$$

Thus, $t = 0$ or $t = A$.

When $t = 0$, $r = A$ or when $t = A$, $r = 0$, therefore, A and 0 is the trivial solution to (16). □

Corollary 1. *Let P be a number of the form $6k + 1$ for any integer $k \geq 1$; then, for some P is a prime, if and only if $A = k$ and 0 (trivial solution) is the only solution to (16).*

Proof. $P = 6k + 1$ can be written in the form $(6t + 1)(6r + 1)$ and clearly; if A and 0 is the only solution, then

$$P = (6A + 1)(6 \cdot 0 + 1) = \left(6\frac{P - 1}{6} + 1\right)1 = (P - 1 + 1)1, \quad P = P \cdot 1. \tag{23}$$

Conversely, let $P = 6k + 1$ be a prime. Clearly, $P = (6k + 1)(6 \cdot 0 + 1)$; thus, $A = k, 0$ is the solution. □

Corollary 2. *If $P = (6t + 1)(6r + 1)$ has at least one more integral solution other than the trivial, then P is a composite.*

Proof. Suppose there exists a suitable value of $r + t$ say $r + t = s \neq A$. Then, $u = tr \neq 0$.

Let $rt = u$; then, $t(s - t) = u$:

$$st - t^2 - u = 0, \quad t^2 - st + u = 0. \tag{24}$$

We use the quadratic formula given by

$$t = \frac{s \pm \sqrt{s^2 - 4u}}{2}. \tag{25}$$

If the integer numbers for t exist say $t = (s \pm \sqrt{s^2 - 4u}/2)$ are integers, then

$$m = \left(6\left(\frac{s + \sqrt{s^2 - 4u}}{2}\right) + 1\right)\left(6\left(\frac{s - \sqrt{s^2 - 4u}}{2}\right) + 1\right). \tag{26}$$

Thus, it is a composite. □

2.4. Factorizing the Composite of Case 3. Suppose $P = (6t + 1)(6r + 1)$ is a composite with at least two prime factors; then, there exists some positive integer A such that $A \equiv t + r \pmod 6$ as in (17). Let

$$t + r = a_o + 6f, \tag{27}$$

such that $A - a_o$ is divisible by 6, where $f = 0, 1, 2, \ldots, n$ and a_o is the smallest positive residue. Then,

$$rt = B - f, \tag{28}$$

where $B = (A - a_o/6)$.

From (28) and (29), we obtain

$$t^2 - (a_o + 6f)t + (B - f) = 0. \tag{29}$$

Since we are interested in the positive integer solution, then

$$(a_o + 6f)^2 - 4(B - f) \geq 0. \tag{30}$$

By expanding, we obtain

$$36f^2 + (12a_o + 4)f - 4B + a_o^2 \geq 0. \tag{31}$$

Then, let h be the least positive integer solution for f satisfying (32). Then, $f_n = h + n$, where $n = 0, 1, \ldots, \eta$. This implies that $f_{\min} = h$ for the real solution in (30).

Substituting $f_n = h + n$ in (30), we obtain

$$t_n^2 - (a_o + 6h + 6n)t_n + (B - h - n) = 0. \tag{32}$$

However, we know that P has at least one prime factor not exceeding $\sqrt{P}$ [36]. Then, $6t + 1 \leq \sqrt{P}$, or $t \leq \sqrt{P} - 1/6$. Substituting for t in (33) to determine the maximum value for $n = \eta$, we obtain

$$n \leq \frac{(\sqrt{P} - 1)^2 - 6(a_o + 6h)(\sqrt{P} - 1) + 36(B - h)}{36\sqrt{P}} \approx \frac{\sqrt{P}}{36}. \tag{33}$$

For maximum η, we choose the negative integer solution of f in (32).

Suppose h_o is the negative value of f; then, we obtain

$$\eta \leq \frac{(\sqrt{P} - 1)^2 - 6(a_o + 6h_o)(\sqrt{P} - 1) + 36(B - h_o)}{36\sqrt{P}} \approx \frac{\sqrt{P}}{36}. \tag{34}$$

Then, we can now obtain the exact integer solution for t recursively in simply $\leq \eta + \omega$ iterations, where ω is the error in n.

During the iterations, we may reach a point when we cannot obtain the integer solution for t, and as we reach t_η, the values of t tend to converge to some real number say τ, and this requires us to do more iteration so that we can reach at least $t = 1$. So, to reduce the iterations, we decide to simply list down the remaining values of t if $t_\eta = \tau > 1$ right from 1 to $\tau - 1$ and do the trial divisions, and this is the error we assume to be ω.

When we obtain exact integer solutions for t, then it implies that, at least one of the t values gives a prime or a number that divides P.

Case 4. $P = (6t + 5)(6r + 5)$.

Theorem 3. *Let*

$$P = (6t + 5)(6r + 5). \tag{35}$$

Then, there exists some integer A such that

$$A \equiv 5(r + t) \pmod{6}. \tag{36}$$

Proof. From

$$P = (6t + 5)(6r + 5) = 6[6tr + 5(r + t)] + 25, \tag{37}$$

then

$$P - 25 = 6[6tr + 5(r + t)]. \tag{38}$$

Dividing through by 6, we obtain

$$\frac{P - 25}{6} = 5(r + t) + 6rt. \tag{39}$$

Now, let $A = (P - 25/6)$ and $u = rt$ imply that (41) becomes

$$A = 5(r + t) + 6u. \tag{40}$$

Hence, we obtain

$$A \equiv 5(r + t) \pmod{6}. \tag{41}$$

□

Lemma 2. *If $5(r + t) = A$ and A is divisible by 5, then P is divisible by 5.*

Proof. Let $5(r + t) = A$. We know that $u = tr = 0$. Then, it implies that $r = A/5 - t$:

$$t\left(\frac{A}{5} - t\right) = 0. \tag{42}$$

Thus, $t = 0$ or $t = (A/5)$.

When $t = 0$, $r = (A/5)$ or when $t = (A/5)$, $r = 0$, since we know that 5 divides A, now, let $\zeta = A/5$; substituting for either t or r in equation (37),

$$P = (6\zeta + 5)(6 \cdot 0 + 5) = (6\zeta + 5)5. \tag{43}$$

Thus, P in (37) is divisible by 5, and therefore, P is not a prime. □

Corollary 3. *If $P = (6t + 5)(6r + 5)$ has at least a nonzero integer solution, then P is a composite.*

Proof. Suppose there exists a suitable value of $5(r + t)$ say $5(r + t) = s \neq A$. Then, $u = tr \neq 0$.

Let $rt = u$. Then, $t(s/5 - t) = u$:

$$\begin{aligned} st - 5t^2 - 5u &= 0, \\ 5t^2 - st + 5u &= 0. \end{aligned} \tag{44}$$

We use the quadratic formula given by

$$\begin{aligned} t &= \frac{s \pm \sqrt{s^2 - 100u}}{10}, \\ m &= \left(6\left(\frac{s + \sqrt{s^2 - 100u}}{10}\right) + 5\right)\left(6\left(\frac{s - \sqrt{s^2 - 100u}}{10}\right) + 5\right). \end{aligned} \tag{45}$$

Thus, a composite provided the values for t and r are integers.

Clearly, if the values of t and r are not integers, then P is a prime. □

2.5. Factorizing the Composite of Case 4. Suppose $P = (6t + 5)(6r + 5)$ is a composite. Then, there exists some positive integer A such that $A \equiv 5(t + r) \pmod{6}$ as in (38). Let

$$5(t + r) = a_o + 6f, \tag{46}$$

such that $A - a_o$ is divisible by 6, where $f = 0, 1, 2, \ldots, n$ and a_o is the smallest positive residue. Then,

$$rt = B - f, \tag{47}$$

where $B = A - a_o/6$

From (48) and (49), we obtain

$$5t^2 - (a_o + 6f)t + 5(B - f) = 0. \tag{48}$$

Since we are interested in the positive integer solution, then

$$(a_o + 6f)^2 - 100(B - f) \geq 0. \tag{49}$$

By expanding, we obtain

$$36f^2 + (12a_o + 100)f - 100B + a_o^2 \geq 0. \tag{50}$$

Then, let h be the least positive integer solution for f satisfying (52). Then, $f_n = h + n$, where $n = 0, 1, \ldots, \eta$. This implies that $f_{\min} = h$ for the real solution in (50).

Substituting $f_n = h + n$ in (50), we obtain

$$5t_n^2 - (a_o + 6h + 6n)t_n + 5(B - h - n) = 0. \tag{51}$$

However, we know that $6t + 5 \leq \sqrt{P}$; then, $t \leq (\sqrt{P} - 5/6)$. Substituting for t in (53) to determine the maximum value for $n = \eta$, we obtain

$$n \leq \frac{5(\sqrt{P} - 5)^2 - 6(a_o + 6h)(\sqrt{P} - 5) + 180(B - h)}{36\sqrt{P}} \approx \frac{5\sqrt{P}}{36}. \tag{52}$$

For maximum η, we choose the negative integer solution of f in (52).

Suppose h_o is the negative value of f; then, we obtain

$$\eta \leq \frac{5(\sqrt{P} - 5)^2 - 6(a_o + 6h_o)(\sqrt{P} - 5) + 180(B - h_o)}{36\sqrt{P}} \approx \frac{5\sqrt{P}}{36}. \tag{53}$$

Then, we can now obtain the exact integer solution for t recursively in simply $\leq \eta + \omega$ iterations. When we obtain exact integer solutions for t, then it implies that at least one of the t values gives a prime or a number that divides P.

3. Composites of the Form $(6k+5)$ and Their Factorization

Theorem 4. *Let $P = (6t+5)(6r+1)$; then, there exist some integer A such that*

$$A \equiv (5r+t) \pmod{6}. \tag{54}$$

Proof. From

$$P = (6t+5)(6r+1) = 6[6tr + (5r+t)] + 5, \tag{55}$$

then

$$P - 5 = 6[(5r+t) + 6tr]. \tag{56}$$

Dividing through by 6, we obtain

$$\frac{P-5}{6} = (5r+t) + 6tr. \tag{57}$$

Let $A = P - 5/6$ and $k = tr$; then,

$$A = (5r+t) + 6k, \tag{58}$$

implying

$$A \equiv (5r+t) \pmod{6}. \tag{59}$$

□

Lemma 3. *If $5r + t = A$, then either $r = (A/5)$, $t = 0$ or $r = 0$, $t = A$ is a trivial solution to (56).*

Proof. Let

$$5r + t = A. \tag{60}$$

Then,

$$rt = 0, \tag{61}$$

implying that

$$r = \frac{A-t}{5} \Rightarrow t\left(\frac{A-t}{5}\right) = 0. \tag{62}$$

Thus, $t = 0$ or $t = A$, when $t = 0$, $r = (A/5)$ and when $t = A$, $r = 0$. □

Corollary 4. *When the trivial solution in Lemma 3 is the only solution to (56), then P is either prime or divisible by 5.*

Proof. From (56), we need to show that P is either divisible by 5 or has exactly two divisors that is 1 and P itself:

$$P = (6r+1)(6t+5). \tag{63}$$

When $t = 0$, $r = (A/5)$, then

$$P = \left(6\frac{A}{5} + 1\right)(6 \cdot 0 + 5) = \left(6\frac{P-5}{30} + 1\right)5. \tag{64}$$

Then, P is divisible by 5, provided 5 divides A.
Or when $t = A$, $r = 0$, then

$$P = (6 \cdot 0 + 1)(6A + 5) = 1 \cdot \left(6\frac{P-5}{6} + 5\right),$$
$$P = 1 \cdot P. \tag{65}$$

Implying if (56) has only a trivial solution, then 1 and P are the only divisors of P. □

Corollary 5. *If there exists one more solution (nontrivial solution) of (56), then P is a multiple of primes greater than or equal to 5.*

Proof. Let $s \neq A$ and $u \neq 0$ be the suitable integers such that $5r + t = s$ and $tr = u$; then,

$$r = \frac{s-t}{5},$$
$$\Rightarrow \left(\frac{s-t}{5}\right)t - u = 0, \tag{66}$$
$$t^2 - st + 5u = 0.$$

Applying quadratic formula, we obtain

$$t = \frac{s \pm \sqrt{s^2 - 20u}}{2}. \tag{67}$$

The solution is either $(s + \sqrt{s^2 - 20u}/2)$ or $(s - \sqrt{s^2 - 20u}/2)$.

Substituting the solution in (56), we obtain

$$P = \left(6\frac{s + \sqrt{s^2 - 20u}}{2} + 5\right)\left(6\frac{s - \sqrt{s^2 - 20u}}{10} + 1\right) \tag{68}$$

or

$$P = \left(6\frac{s - \sqrt{s^2 - 20u}}{2} + 5\right)\left(6\frac{s + \sqrt{s^2 - 20u}}{10} + 1\right). \tag{69}$$

Thus, P is a composite provided $(s + \sqrt{s^2 - 20u}/2)$ and $(s - \sqrt{s^2 - 20u}/2)$ are integers. □

3.1. Factorizing the Composite $P = (6t+5)(6r+1)$. Suppose $P = (6t+5)(6r+1)$ is a composite. Then, there exists some positive integer A such that $A \equiv 5r + t \pmod{6}$ as in (56).

Let

$$5r + t = a_o + 6f, \tag{70}$$

such that $A - a_o$ is divisible by 6, where $f = 0, 1, 2, \ldots, n$ and a_o is the smallest positive residue. Then,

$$rt = B - f, \tag{71}$$

where $B = (A - a_o/6)$.

From (72) and (73), we obtain

$$t^2 - (a_o + 6f)t + 5(B - f) = 0. \tag{72}$$

Since we are interested in the positive integer solution, then

$$(a_o + 6f)^2 - 20(B - f) \geq 0. \quad (73)$$

By expanding, we obtain

$$36f^2 + (12a_o + 20)f - 20B + a_o^2 \geq 0. \quad (74)$$

Then, let h be the least positive integer solution for f satisfying (76). Then, $f_n = h + n$, where $n = 0, 1, \ldots, \eta$. This implies that $f_{\min} = h$ for the real solution in (75). Substituting $f_n = h + n$ in (75), we obtain

$$t_n^2 - (a_o + 6h + 6n)t_n + 5(B - h - n) = 0. \quad (75)$$

However, we know from [7] that $6t + 5 \leq \sqrt{P}$; then, $t \leq (\sqrt{P} - 5/6)$. Substituting for t in (77) to determine the maximum value for $n = \eta$, we obtain

$$n \leq \frac{(\sqrt{P} - 5)^2 - 6(a_o + 6h)(\sqrt{P} - 5) + 180(B - h)}{36\sqrt{P}} \approx \frac{\sqrt{P}}{36}. \quad (76)$$

For maximum η, we choose the negative integer solution of f in (76).

Suppose h_o is the negative value of f; then, we obtain

$$\eta \leq \frac{(\sqrt{P} - 5)^2 - 6(a_o + 6h_o)(\sqrt{P} - 5) + 180(B - h_o)}{36\sqrt{P}} \approx \frac{\sqrt{P}}{36}. \quad (77)$$

Then, we can now obtain the exact integer solution for t recursively in simply $\leq \eta$ iterations. When we obtain exact integer solutions for t, then it implies that at least one of the t values gives a prime or a number that divides P.

4. General Outline of the Algorithm

We outline the steps of factorizing primes based on the proofs above.

Given an integer P

(1) Check if P satisfies $P^2 \equiv 1 \pmod{24}$.

(2) Does (1) hold? If so, do step (4), and if not, do step (3).

(3) Check if it is either divisible by 2 or by 3 and reduced it by dividing by 2 or 3 until the Quotient is no longer divisible by 2 or 3. If the resulting Quotient is greater than 3, we can call it P and do step (4).

(4) Check if P is either of the form $6k + 1$ or $6k + 5$ by subtracting 1 or 5 from P and check if the difference is divisible by 6.

(5) If P is of the form $6k + 1$, then

Either Case 3

(i) We determine integer A from $A = (P - 1/6)$.

(ii) We write down the congruence:

$$A \equiv r + t \pmod{6}. \quad (78)$$

(iii) We determine B and a_o, where a_o is the least positive residue such that $B = A - a_o/6$ is a positive integer

(iv) We obtain the least positive integer $f_{\min} = h$ such that

$t^2 - (a_o + 6f)t + (B - f) = 0$ has a real solution.

This is obtained from $(a_o + 6f)^2 - 4(B - f) \geq 0$.

(v) We obtain the integer n from $n = \eta \leq (\sqrt{P}/36)$, where $h_o = -h$.

(vi) $n = 0, 1, 2, \ldots, \eta$, $f_o = h$, $f_n = h + n$, and $t_o = ((a_o + 6h) \pm \sqrt{(a_o + 6h)^2 - 4(B - h)}/2)$.

If the integer solution does not exist at $n = 0$, we do step (vii)

(vii) We perform at most η iterations to obtain the integer solutions for t from

$$t_n = \frac{(a_o + 6h + 6n) \pm \sqrt{(a_o + 6h + 6n)^2 - 4(B - h - n)}}{2}. \quad (79)$$

Remark: If the values of t seem to converge at some point on a real line, then it is better to list the integer values of t from the point of convergence (integer value of convergence) to as small as 1; that is, if the integer value of convergence of t is τ, then we list them such that $t = \tau - 1, \ldots, 1$ and do the trial divisions from $P/6t + 1$.

If there is no integer value of t such that $(P/6t + 1)$ is an integer, then we try Case 4.

OR Case 4

(i) We determine integer A from $A = (P - 25/6)$.

(ii) We write down the congruence:

$$A \equiv 5(r + t) \pmod{6}. \quad (80)$$

(iii) We determine B and a_o, where a_o is the least positive residue such that $B = (A - a_o/6)$ is a positive integer.

(iv) We obtain the least positive integer $f_{\min} = h$ such that

$5t^2 - (a_o + 6f)t + 5(B - f) = 0$ has a real solution.

This is obtained from $(a_o + 6f)^2 - 100(B - f) \geq 0$.

(v) We obtain the integer n from $n = \eta \leq (5\sqrt{P}/36)$, where $h_o = -h$.

(vi) $n = 0, 1, 2, \ldots, \eta$, $f_o = h$, $f_n = h + n$, and $t_o = ((a_o + 6h) \pm \sqrt{(a_o + 6h)^2 - 100(B - h)}/10)$.

If the integer solution does not exist at $n = 0$, we do step (vii).

(vii) We perform at most η iterations to obtain the integer solutions for t from

$$t_n = \frac{(a_o + 6h + 6n) \pm \sqrt{(a_o + 6h + 6n)^2 - 100(B - h - n)}}{10}. \quad (81)$$

Remark: If the values of t seem to converge at some point on a real line, then it is better to list the integer values of t from the point of

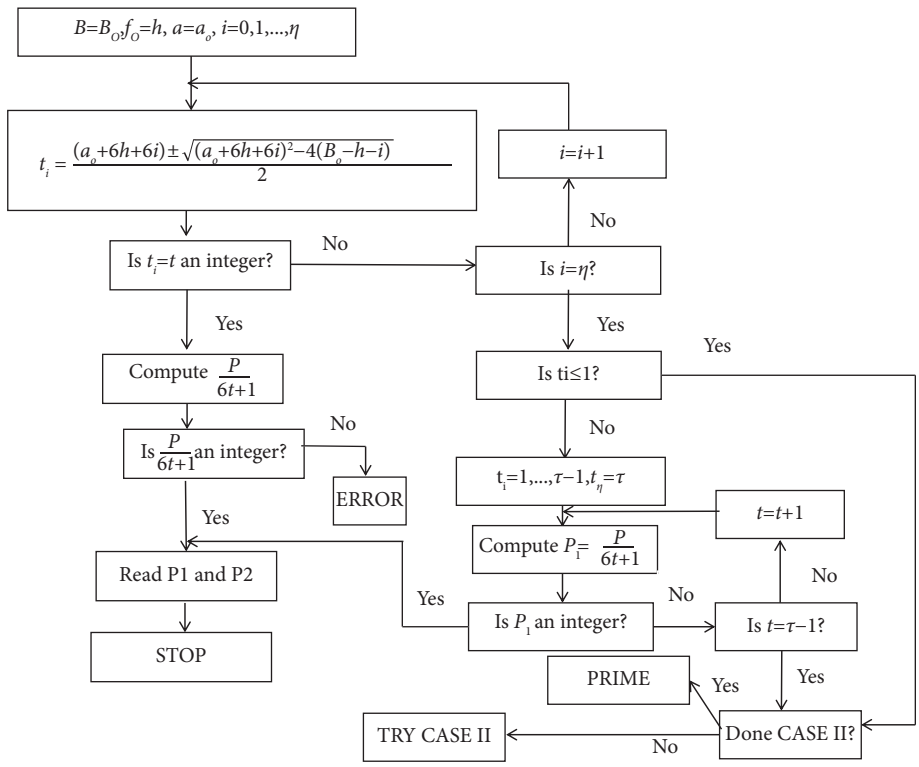

Figure 1: Algorithm for numbers of the form $6k+1$: Case 3.

convergence (integer value of convergence) to as small as 1; that is, if the integer value of convergence of t is τ, then we list them such that $t = \tau - 1, \ldots, 1$ and do the trial divisions from $P/6t + 5$.

If there is no integer value of t such that $(P/6t + 5)$ is an integer, then P is a prime.

(6) If P is of the form $6k + 5$, then

(i) We determine integer A from $A = (P - 5/6)$.

(ii) We write down the congruence:

$$A \equiv 5r + t \pmod 6. \tag{82}$$

(iii) We determine B and a_o, where a_o is the least positive residue such that $B = (A - a_o/6)$ is a positive integer.

(iv) We obtain the least positive integer $f_{\min} = h$ such that

$t^2 - (a_o + 6f)t + 5(B - f) = 0$ has a real solution.

This is obtained from $(a_o + 6f)^2 - 4(B - f) \geq 0$.

(v) We obtain the integer n from $n = \eta \leq (\sqrt{P}/36)$, where $h_o = -h$.

(vi) $n = 0, 1, 2, \ldots, \eta$, $f_o = h$, $f_n = h + n$, and $t_o = ((a_o + 6h) \pm \sqrt{(a_o + 6h)^2 - 20(B - h)})/2$.

If the integer solution does not exist at $n = 0$, we do step (vii).

(vii) We perform at most η iterations to obtain the integer solutions for t from

$$t_n = \frac{(a_o + 6h + 6n) \pm \sqrt{(a_o + 6h + 6n)^2 - 20(B - h - n)}}{2}. \tag{83}$$

Remark: if the values of t seem to converge at some point on a real line, then it is better to list the integer values of t from the point of convergence (integer value of convergence) to as small as 1; that is, if the integer value of convergence of t is τ, then we list them such that $t = \tau - 1, \ldots, 1$ and do the trial divisions from $P/6t + 5$.

If there is no integer value of t such that $(P/6t + 5)$ is an integer, then P is a prime.

Example 1. We consider the factorizing of number 1099551473989:

$$\begin{aligned} A &= 183258578994, \\ 183258578994 &\equiv 5(t + r) \pmod 6, \\ B &= 30543096499, a_o = 0, \\ 5t^2 - 6ft + 5(30543096499 - f) &= 0. \end{aligned} \tag{84}$$

For real solution for t, we obtain $36f^2 + 100f - 3054309649900 \geq 0$:

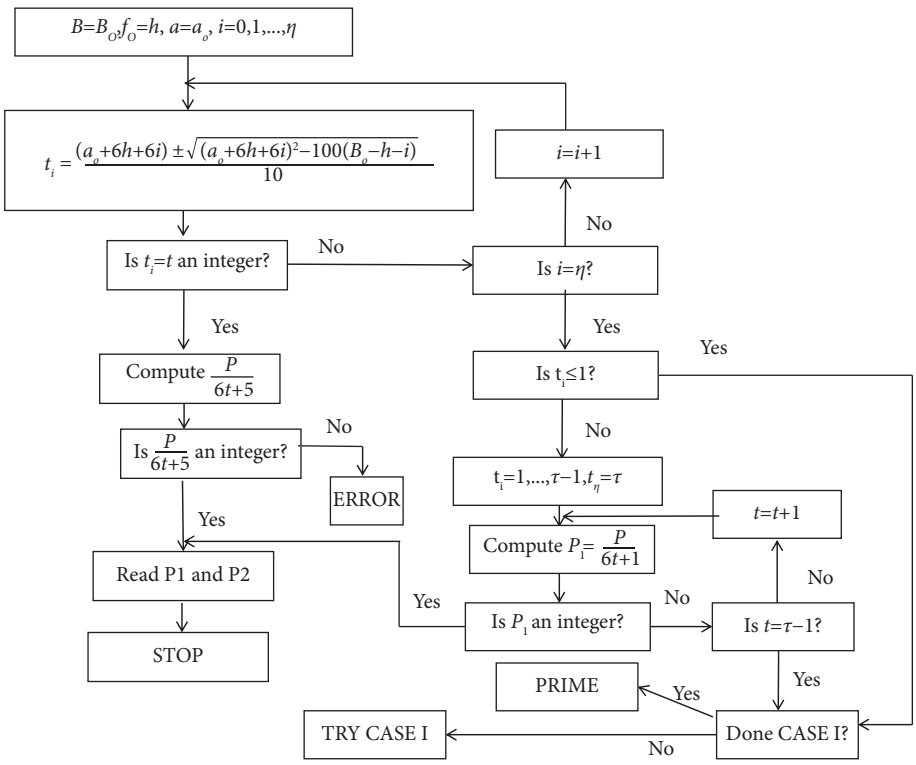

Figure 2: Algorithm for numbers of the form $6k+1$: Case 4.

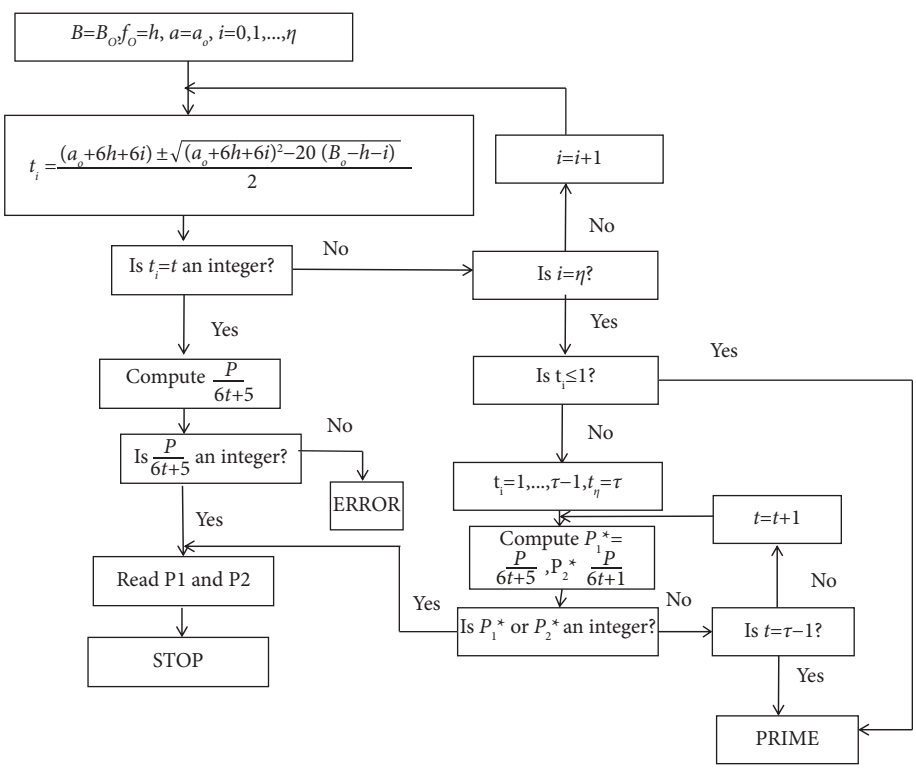

Figure 3: Algorithm for numbers of the form $6k+5$.

$$f_{\min} = h = 291275, \Rightarrow h_o = -291275. \quad (85)$$

Using $n_{\max} = \eta \leq (5(\sqrt{P} - 5)^2 - 6(a_o + 6h_o)(\sqrt{P} - 5) + 180(B - h_o)/36\sqrt{P})$, then $n = 0, 1, 2, \ldots, 582550$.

From $t_o = ((a_o + 6h_o) \pm \sqrt{(a_o + 6h_o)^2 - 100(B - h_o)}\ /10)$, we obtain

$$t_o = \frac{6 \times 291275 \pm \sqrt{100}}{10}. \quad (86)$$

Then, $t_o = 174766$ or $t_o = 174764$, and therefore, the prime divisors of 1099551473989 are 1048601 and 1048589.

The above procedures (general outline) can be summarized by the flowcharts in Figures 1–3, respectively.

4.1. Algorithm for Numbers of the Form 6k + 1: Case 3. $P, A = (P - 1/6), B = (A - a_o/6), (a_o + 6f_o)^2 - 4(B - f_o) \geq 0, h_o = -f_o, \eta \leq (\sqrt{P}/36)$

4.2. Algorithm for Numbers of the Form 6k + 1: Case 4. $P, A = P - 25/6, B = (A - a_o/6)(a_o + 6f_o)^2 - 100(B - f_o) \geq 0, h_o = -f_o, \eta \leq (5\sqrt{P}/36)$

4.3. Algorithm for Numbers of the Form 6k + 5: Case 4. $P, A = P - 5/6, B = (A - a_o/6)(a_o + 6f_o)^2 - 20(B - f_o) \geq 0, h_o = -f_o, \eta \leq (\sqrt{P}/36)$

5. Conclusion and Recommendations

This method is good especially when the difference (prime gap) between the prime divisors if relatively small.

Remark 1. Normally, when the prime divisors are close to each other, values of t_o are integer solutions. However, this may not guarantee for all such problems.

The algorithm is effective in prime factorization and primality testing, especially when dealing with relatively large numbers. However, there is need for a way of differentiating numbers of the form $(6t + 1)(6r + 1)$ from numbers of the form $(6t + 5)(6r + 5)$ because the end result is of the form $6k + 1$ which makes it difficult to choose which algorithm is suitable for such numbers. This forces one to randomly select either Case 3 formula or Case 4 which makes it more tiresome in case the first algorithm does not produce any result so you turn to another case before making any conclusion about the given problem.

In addition, this algorithm requires a computer program so that it carries a greater impact in the field of cryptography and mathematics.

Data Availability

The figures data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The author thank Dr. Osman, Prof Mogtaba M, and Dr. M. Sala for reading the work and helping prepare it and is indebted to them.

References

[1] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, "New primality criteria and factorizations of $2^m \pm 1$," *Computing*, vol. 29, pp. 620–647, 1975.

[2] A. Granville, "It is easy to determine whether a given integer is prime," *Bulletin of the American Mathematical Society*, vol. 42, no. 1, pp. 3–38, 2004.

[3] S. K. Park and K. W. Miller, "Random number generators: good ones are hard to find," *Communications of the ACM*, vol. 31, no. 10, pp. 1192–1201, 1988.

[4] R. Jakimczuk, "Logarithm of the exponents in the prime factorization of the factorial," *International Mathematical Forum*, vol. 12, pp. 643–649, 2017.

[5] P. Erdós, "On the normal number of prime factors of P-1 and some related problems concerning euler's ø-function," *The Quarterly Journal of Mathematicsos*, pp. 205–213, 1935.

[6] H. L. Montgomery and R. C. Vaughan, "The large sieve," *Mathematika*, vol. 20, no. 2, pp. 119–134, 1973.

[7] K. H. Rosen, *Elementary Number Theory and its Applications*, ADDISON-WESLEY PUBLISHING COMPANY, Boston, MA, USA, 1986.

[8] M. O. Rabin, "Probabilistic algorithm for testing primality," *Journal of Number Theory*, vol. 12, no. 1, pp. 128–138, 1980.

[9] W. Edwin Clark, *Elementary Number Theory*, University of South Florida, Florida, FL, USA, 2003.

[10] J. Zalaket and J. Hajj-Boutros, "Prime factorization using square root approximation," *Computers & Mathematics with Applications*, vol. 61, no. 9, pp. 2463–2467, 2011.

[11] J. V Uspensky and M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill Book Company Inc, New York, NY, USA, 1939.

[12] O. Narutaka and P. Sorin, "Some prime factorization results for type II factors," *Inventiones Mathematicae*, vol. 156, pp. 223–234, 2004.

[13] A. Overmars and S. Venkatraman, "A fast factorisation of semi-primes using sum of squares," *Mathematical and Computational Applications*, 2019.

[14] J. F. McKee, "Turning euler's factoring method into a factoring algorithm," *Bulletin of the London Mathematical Society*, vol. 28, no. 4, pp. 351–355, 1996.

[15] R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," *SIAM Journal on Computing*, vol. 6, no. 1, pp. 84-85, 1977.

[16] S. Y. Yan, "Primality testing of large numbers in maple," *Computers & Mathematics with Applications*, vol. 29, no. 12, pp. 1–8, 1995.

[17] S. Y. Yan, "68 new large amicable pairs," *Computers & Mathematics with Applications*, vol. 28, no. 5, pp. 71–74, 1994.

[18] G. L. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and System Sciences*, vol. 13, no. 3, pp. 300–317, 1976.

[19] R. J. Baillie and S. S. Wagstaff, "Lucas pseudoprimes," *Mathematics of Computation*, vol. 35, no. 152, pp. 1391–1417, 1980.

[20] A. Dunn and A. Zaharescu, "Sums of kloosterman sums over primes in an arithmetic progression," *The Quarterly Journal of Mathematics*, vol. 70, no. 1, pp. 319–342, 2019.

[21] H.-M. Sun, M.-E. Wu, W.-C. Ting, and M. Hinek, "Dual RSA and its security analysis," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2922–2933, 2007.
[22] G. P. Michon, "Factoring into primes," 2020, http://www.numericana.com/answer/factoring.htm.
[23] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[24] M. Agrawal, N. Kayal, and N. Saxena, "PRIMES is in P," *Annals of Mathematics*, vol. 160, no. 2, pp. 781–793, 2004.
[25] C. Pomerance, "On the distribution of pseudoprimes," *Mathematics of Computation*, vol. 37, no. 156, pp. 587–593, 1981.
[26] R. Hans, *Prime Number And Computer Methods for Factorization Birkhauser*, p. pg3, Birkhäuser, Boston, MA, USA, 2012.
[27] L. M. Adleman, C. Pomerance, and R. S. Rumely, "On distinguishing prime numbers from composite numbers," *Annals of Mathematics*, 1983.
[28] R. Schoof, "Four primality testing algorithms," *Algorithmic Number Theory*, vol. 44, 2008.
[29] H. W. Lenstra, "Factoring integers with elliptic curves," *Annals of Mathematics*, vol. 126, no. 3, pp. 649–673, 1987.
[30] J. M. Pollard, "Theorems on factorization and primality testing," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 76, no. 3, pp. 521–528, 1974.
[31] C. Harvey, *Advanced Number Theory*, p. pg10, Dover Publications. Inc, New York, NY, USA, 1980.
[32] G. Tenenbaum and M. Mendes France, *The Prime Numbers and Their Distribution*, American Mathematical Society, Washington, WA, USA, 1997.
[33] R. D. Carmichael, "On composite numbers p which satisfy the Fermat congruence.a^{p-1}=1modp," *The American Mathematical Monthly*, vol. 19, pp. 22–27, 1912.
[34] M. L. Weber, "It's a wonderful world - and universe - out there," 2020, https://www.snexplores.org/article/explainer-what-is-an-algorithm.
[35] J. W. Porras Ferreira and C. G. Willian De Jesus, "An Analysis of the Congruence 1mod24 as a Generator of prime numbers Greater or Equal to 5," *Current Journal of Applied Science and Technology*, vol. 14, pp. 2231–0843, 2016, http://sciencedomain.org/review-history/13307.
[36] Z. Joseph and B. Joseph Hajj, "Prime factorization using square root approximation," *Computers & Mathematics with Applications*, vol. 61, 2011, http://www.sciencedirect.com/science/article/pii/S0898122111001131.