Elementary Formulas for Greatest Common Divisors and Semiprime Factors

Joseph M. Shunia

June 19, 2024
Revised: August 7, 2024
Version 3

Abstract

We present new formulas for computing greatest common divisors (GCDs) and extracting the prime factors of semiprimes using only elementary arithmetic operations: addition, subtraction, multiplication, floored division, and exponentiation. Our GCD formula simplifies a formula of Mazzanti and is derived using Kronecker substitution techniques from our earlier research. By combining this GCD formula with our recent result on an arithmetic term for $\sqrt{n}$, we derive explicit expressions for the prime factors of a semiprime $n = pq$.

Keywords: elementary formula; arithmetic term; modular arithmetic; semiprime; integer factorization; Kronecker substitution.

2020 Mathematics Subject Classification: 11A05, 11A25, 11A51.

1 Introduction

The greatest common divisor (GCD) of two integers a and b, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b. Euclid's algorithm for computing the GCD is one of the oldest known algorithms, dating back to ancient Greece [1].

Semiprimes, numbers with exactly two prime factors, play a key role in number theory and cryptography. The problem of factoring a semiprime $n = pq$ into its constituent primes p and q is believed to be computationally intractable for large n. This property forms the basis for widely used cryptosystems such as RSA [2]. Efficient algorithms for factoring semiprimes would have major implications for the security of these systems. While our new formulas are computationally impractical, they may yield novel insights into the distribution and properties of GCDs and semiprime factors.

In this paper, we present new results on arithmetic term formulas for the GCD and semiprime factorization. Building on work by Mazzanti and Marchenkov [3, 4], we derive a simplified polynomial form for the GCD that can be expressed in terms of an arbitrary integer base. We also obtain arithmetic terms for the prime factors of a non-square semiprime $n = pq$.

To appreciate the significance of our results, it is important to understand what constitutes an arithmetic term. An **arithmetic term** is a mathematical expression which uses only elementary arithmetic operations. Formally, let $\mathbf{A}$ denote the class of arithmetic terms. We have

$$\mathbf{A} = [\{1, a + b, a \dot{-} b, ab, \lfloor a/b \rfloor, a^b\}],$$

where $\dot{-}$ represents the **bounded subtraction** operation, defined as: $a \dot{-} b = \max(a - b, 0)$ [3]. Throughout this paper, we may use the standard subtraction notation $a - b$ when it is clear that the result is non-negative.

It is also worth noting that the modulo operation is implicitly included in $\mathbf{A}$, since it can be expressed as

$$a \bmod b = a \dot{-} b \lfloor a/b \rfloor .$$

1.1 Background

We denote by $\mathbf{P}$ the class of primitive recursive functions. The class of Kalmar functions, denoted by $\mathbf{K}$, is an elementary class of functions, which is a subclass of $\mathbf{P}$.

Kalmar functions were introduced by Laszlo Kalmar in the 1940s. Kalmar aimed to characterize the class of functions that can be computed using a certain restricted form of recursion, known as "Kalmar elementary recursion" or "bounded recursion" (hence the term "bounded subtraction" in the definition of $\mathbf{A}$). It is well-established that $\mathbf{K}$ contains many important functions, such as the arithmetic operations, the exponential function, and the bounded μ operator (which is used to define the floored division operation). However, it does not contain all primitive recursive functions [5].

It was long conjectured, and finally proved by Mazzanti, that the class $\mathbf{A}$ generates the class $\mathbf{K}$ [3, 6]. As mentioned above, $\mathbf{K}$ is known to be a proper subclass of $\mathbf{P}$. In particular, $\mathbf{K} = \mathcal{E}^3$ in the Grzegorczyk hierarchy, a framework categorizing primitive recursive functions by complexity [7]. Formally, we have

$$[\mathbf{A}] = \mathbf{K} = \mathcal{E}^3 \subset \mathbf{P}.$$

In 1970, Matiyasevich, building on the work of Robinson [8] and Davis et al. [9], proved that all computable functions can be expressed as Diophantine equations [10]. Matiyasevich's results imply that there exists a Diophantine equation for calculating the n-th prime number [11]. However, no arithmetic term for the n-th prime is known [12]. Similarly, while Matiyasevich's theorem suggests the existence of an Diophantine equation formula for semiprime factorization, an arithmetic term that computes the factors remained to be discovered. Our work presents the first arithmetic terms for the problem.

1.2 Recent Developments

Recently, we discovered a formula for the r-th roots of positive integers $\sqrt[r]{n}$ as the limit of a quotient of two arithmetic terms [13]. By combining our results with an arithmetic term for factorials [8, 12], along with a simplified version of Mazzanti's GCD formula (Lemma 1) [3], we obtain the first closed-form expressions for semiprime factors as arithmetic terms. This answers a question from Shamir (1978), who first hypothesized the existence of such formulas when describing an algorithmic approach to integer factorization using arithmetic terms [14].

2 Greatest Common Divisor

Lemma 1 (Mazzanti's GCD Formula)**.**

$$\forall a, b \in \mathbb{Z}^+, \quad \gcd(a,b) = \left\lfloor \frac{(2^{a^2b(b+1)} - 2^{a^2b})(2^{a^2b^2} - 1)}{(2^{a^2b} - 1)(2^{ab^2} - 1)2^{a^2b^2}} \right\rfloor \bmod 2^{ab}.$$

Proof. The formula and its proof are due to Mazzanti (2002) [3]. □

Applying Kronecker substitution techniques from our previous works [15, 13], we find that Mazzanti's GCD formula can be simplified. We begin with a theorem that expresses Mazzanti's GCD formula in a polynomial form.

Theorem 2.

$$\forall a, b \in \mathbb{Z}^+, \quad \gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

Proof. Consider Mazzanti's greatest common divisor formula (Lemma 1), which is given by

$$\gcd(a,b) = \left\lfloor \frac{(2^{a^2b(b+1)} - 2^{a^2b})(2^{a^2b^2}-1)}{(2^{a^2b}-1)(2^{ab^2}-1)2^{a^2b^2}} \right\rfloor \bmod 2^{ab}.$$

Observe that all integer powers in the arithmetic term are divisible by 2^{ab}. Factoring these, we obtain

$$\gcd(a,b) = \left\lfloor \frac{((2^{ab})^{a(b+1)} - (2^{ab})^a)((2^{ab})^{ab}-1)}{((2^{ab})^a-1)((2^{ab})^b-1)(2^{ab})^{ab}} \right\rfloor \bmod 2^{ab}.$$

Substituting with $2^{ab} = x$ yields

$$\gcd(a,b) = \left\lfloor \frac{(x^{a(b+1)} - x^a)(x^{ab}-1)}{(x^a-1)(x^b-1)x^{ab}} \right\rfloor \bmod x.$$

Simplifying the fraction, we see

$$\gcd(a,b) = \left\lfloor \frac{x^{a-ab}(x^{ab}-1)^2}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

This fraction can be expanded as the sum

$$\gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} + \frac{x^{a-ab}}{(x^a-1)(x^b-1)} + \frac{-2x^a}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

Since we are reducing the quotient mod x, we need only consider the term in the fraction which yields the constant term in the polynomial, which is $\gcd(a,b)$.

From Marchenkov [6], we have the following alternative GCD formula:

$$\gcd(a,b) = \left\lfloor \frac{(2^{a^2b(b+1)} - 2^{a^2b})(2^{a^2b^2}-1)}{(2^{a^2b}-1)(2^{ab^2}-1)2^{a^2b^2}} \right\rfloor \bmod 2^{ab}.$$

Factoring out 2^{ab}, we obtain

$$\gcd(a,b) = \left\lfloor \frac{((2^{ab})^{a(b+1)} - (2^{ab})^b)((2^{ab})^{ab}-1)}{((2^{ab})^a-1)((2^{ab})^b-1)(2^{ab})^{ab}} \right\rfloor \bmod 2^{ab}.$$

Replacing $2^{ab} = x$, we get

$$\gcd(a,b) = \left\lfloor \frac{(x^{a(b+1)} - x^b)(x^{ab}-1)}{(x^a-1)(x^b-1)x^{ab}} \right\rfloor \bmod x.$$

Expanding this as a sum, we obtain

$$\gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} + \frac{x^{b-ab}}{(x^a-1)(x^b-1)} + \frac{-x^a}{(x^a-1)(x^b-1)} + \frac{-x^b}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

In summary, we have two expressions for $\gcd(a,b)$ derived from different formulas.

(i) From Mazzanti's formula:

$$\gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} + \frac{x^{a-ab}}{(x^a-1)(x^b-1)} + \frac{-2x^a}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

(ii) From Marchenkov's formula:

$$\gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} + \frac{x^{b-ab}}{(x^a-1)(x^b-1)} + \frac{-x^a}{(x^a-1)(x^b-1)} + \frac{-x^b}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

The term $\frac{x^{a+ab}}{(x^a-1)(x^b-1)}$ is present in both expressions and will contribute to the constant term. One can verify for several pairs a, b that

$$\left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} \right\rfloor \bmod x = \gcd(a,b),$$

and it is easy to see that

$$\frac{x^{a-ab} - 2x^a}{(x^a-1)(x^b-1)} \neq \frac{x^{b-ab} - x^a - x^b}{(x^a-1)(x^b-1)}.$$

Thus, only the term $\frac{x^{a+ab}}{(x^a-1)(x^b-1)}$ may contribute a constant after reduction modulo x. Otherwise, the formulas of Mazzanti (i) and Marchenkov (ii) could not possibly yield the same result for all a, b. We conclude

$$\gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

□

Corollary 3. *Let $a, b, n \in \mathbb{Z}^+$ such that $n > 2$ and $n > \gcd(a,b)$. Then*

$$\gcd(a,b) = \left\lfloor \frac{n^{a+ab}}{(n^a-1)(n^b-1)} \right\rfloor \bmod n.$$

Proof. Consider the polynomial formula given by Theorem 2. Substituting with $x = n$ yields the given formula. By Theorem 2 in [13], the substitution is valid since n is greater than the evaluation, which is $\gcd(a,b)$.

However, we also have to consider the form of the fraction. Suppose $n = 2$, then

$$\left\lfloor \frac{2^{a+ab}}{(2^a-1)(2^b-1)} \right\rfloor = \left\lfloor \frac{2^{a+ab}}{2^{ab+a} - 2^a - 2^b + 1} \right\rfloor = 2k,$$

for some $k \in \mathbb{Z}^+$. That is, the fraction always yields an even number of the form $2k$. This would imply

$$\gcd(a,b) = \left\lfloor \frac{2^{a+ab}}{(2^a-1)(2^b-1)} \right\rfloor = 2k \equiv 0 \pmod 2 \quad \text{(contradiction)},$$

which is a contradiction, since $\gcd(a,b)$ is nonzero by definition. □

Theorem 4.

$$\forall a, b \in \mathbb{Z}^+, \quad \gcd(a,b) \equiv -\left(x^{a+ab} \bmod \left((x^a-1)(x^b-1)\right)\right) \pmod x.$$

Proof. Consider the formula given by Theorem 2, which is

$$\gcd(a,b) = \left\lfloor \frac{x^{a+ab}}{(x^a-1)(x^b-1)} \right\rfloor \bmod x.$$

Recall the following well-known identity for the floor function

$$\left\lfloor \frac{a}{b} \right\rfloor = \frac{a - (a \bmod b)}{b}.$$

Applying this to the formula from Theorem 2, we get

$$\gcd(a,b) \equiv \frac{x^{a+ab} - \left(x^{a+ab} \bmod \left((x^a-1)(x^b-1)\right)\right)}{x^{a+b} - x^a - x^b + 1} \pmod{x}.$$

Taking the numerator and denominator mod x, we find

$$\begin{aligned}
\gcd(a,b) &= \frac{(x^{a+ab} \bmod x) - \left(\left(x^{a+ab} \bmod \left((x^a-1)(x^b-1)\right)\right) \bmod x\right)}{(x^a-1)(x^b-1) \bmod x} \\
&= \frac{0 - \left(\left(x^{a+ab} \bmod \left((x^a-1)(x^b-1)\right)\right) \bmod x\right)}{1} \\
&= -\left(x^{a+ab} \bmod \left((x^a-1)(x^b-1)\right)\right) \bmod x.
\end{aligned}$$

Hence, we can say

$$\gcd(a,b) \equiv -\left(x^{a+ab} \bmod \left((x^a-1)(x^b-1)\right)\right) \pmod{x}.$$

□

Corollary 5. *Let $a, b, n \in \mathbb{Z}^+$ such that $n > 2$ and $n > \gcd(a,b)$. Then*

$$\gcd(a,b) \equiv -\left(n^{a+ab} \bmod \left((n^a-1)(n^b-1)\right)\right) \pmod{n}.$$

Proof. Consider the polynomial formula given by Theorem 2. Substituting with $x = n$ yields the given formula. By Theorem 2 in [13], the substitution is valid since n is greater than the evaluation, which is $\gcd(a,b)$.

However, we also have to consider the form of the remainder. Suppose $n = 2$, then the expression

$$2^{a+ab} \bmod (2^{a+b} - 2^a - 2^b + 1)$$

can yield either an even or odd remainder, depending on the choice of (a,b). Now, suppose the remainder is even and of the form $2k$ for some $k \in \mathbb{Z}^+$. This would imply

$$\gcd(a,b) = 2k \equiv 0 \pmod 2 \quad \text{(contradiction)},$$

which is a contradiction, since $\gcd(a,b)$ is nonzero by definition. □

2.1 Coprimality Function

Experimentally, starting from our result in Theorem 4, we found a coprimality function, which we were able to prove as a theorem.

Theorem 6. *Define the integer-valued function*

$$\epsilon(a,b) = \begin{cases} 0 & \text{if } \gcd(a,b) > 1, \\ 1 & \text{if } \gcd(a,b) = 1. \end{cases}$$

Then

$$\forall a, b \in \mathbb{Z}^+, \quad \epsilon(a,b) = -\left(x^{ab-b+1} \bmod \left((x^a-1)(x^b-1)\right)\right) \bmod x.$$

Proof. Let a, b in $\mathbb{Z}_{>1}$. First, we examine the case where $\gcd(a,b) > 1$. From Graham and others, we have the following identity [16]:

$$\begin{aligned} \forall a, b \in \mathbb{Z}_{>1}, \quad & \gcd(x^a-1, x^b-1) = x^{\gcd(a,b)} - 1 \\ \implies & (x^{\gcd(a,b)} - 1) \mid \left((x^a-1)(x^b-1)\right). \end{aligned}$$

For the remainder of $x^{ab-b+1} \bmod \left((x^a-1)(x^b-1)\right)$ to be zero mod x, the remainders of x^{ab-b+1} mod the factors (x^a-1) and (x^b-1) must combine to be a multiple of x. More precisely, we must have

$$x^{ab-b+1} \equiv f(x)x \pmod{(x^a-1)(x^b-1)},$$

for some $f(x) \in \mathbb{Z}[x]$. Now, since we are given $(ab-b+1) > a, b$ and $a, b \geq \gcd(a,b)$, the reduction of x^{ab-b+1} mod the factors of $(x^a-1)(x^b-1)$ will yield remainders that are x times a power of x. That is,

$$x^{ab-b+1} \equiv x^{k+1} \equiv x^k x \pmod{x^a-1},$$

and

$$x^{ab-b+1} \equiv x^{j+1} \equiv x^j x \pmod{x^b-1},$$

where $k, j \in \mathbb{Z}$. The specific k, j depend on the choice of a, b. However, we do not require any particular values here. We merely need to show that modding x^{ab-b+1} by $(x^a-1)(x^b-1)$ also yields a remainder that is a multiple of x.

Due to the common factor, which is $x^{\gcd(a,b)} - 1$, the moduli (x^a-1) and (x^b-1) are not coprime and so we cannot apply the standard version of the Chinese Remainder Theorem (CRT). However, we can apply a variant which allows for non-coprimality, called the General Chinese Remainder Theorem (GCRT) [17]. Applying the GCRT for $\gcd(x^a-1, x^b-1) = x^{\gcd(a,b)} - 1$, we have

$$\begin{aligned} x^{ab-b+1} &\equiv \left(\frac{v(x^a-1)x^k x + u(x^b-1)x^j x}{x^{\gcd(a,b)} - 1}\right) \\ &\equiv \left(\frac{v(x^a-1)x^k x}{x^{\gcd(a,b)} - 1} + \frac{u(x^b-1)x^j x}{x^{\gcd(a,b)} - 1}\right) \pmod{(x^a-1)(x^b-1)}, \end{aligned}$$

where $u, v \in \mathbb{Z}[x]$ are the Bézout coefficients returned by the Extended Euclidean algorithm for $\gcd(x^a - 1, x^b - 1)$. Next, we set $q_a = (x^a-1)/(x^{\gcd(a,b)} - 1)$, $q_b = (x^b-1)/(x^{\gcd(a,b)} - 1)$, followed by factoring, to obtain

$$\begin{aligned} x^{ab-b+1} &\equiv v q_a x^k x + u q_b x^j x \\ &\equiv x(v q_a x^k + u q_b x^j) \pmod{(x^a-1)(x^b-1)}. \end{aligned}$$

Clearly, the remainder of x^{ab-b+1} modulo $(x^a-1)(x^b-1)$ is a multiple of x when $\gcd(a,b) > 1$. Therefore, we conclude

$$\forall a, b \in \mathbb{Z}_{>1} : \gcd(a,b) > 1, \quad \left(x^{ab-b+1} \bmod \left((x^a-1)(x^b-1)\right)\right) \bmod x = 0.$$

This corresponds to the case $\gcd(a,b) > 1$ from the formula in the theorem.

Next, we consider the case where $\gcd(a,b) = 1$. Here, we have

$$x^{\gcd(a,b)} - 1 = x^1 - 1 = x - 1 \equiv -1 \pmod{x}.$$

The reduction of x^{ab-b+1} modulo $(x^a-1)(x^b-1)$ can be represented as a polynomial of the form

$$g(x) := x^{ab-b+1} + (x^a-1)(x^b-1) \in \mathbb{Z}[x].$$

Considering $(x^{\gcd(a,b)} - 1) = (x-1) \mid (x^a-1)(x^b-1)$, we can simply g as

$$g(x) = x^{ab-b+1} + (x-1).$$

Reducing $g \bmod x$, we find

$$g(x) = x^{ab-b+1} + (x-1) \equiv (0) + (-1) \equiv -1 \pmod{x}.$$

Thus, we conclude

$$\forall a, b \in \mathbb{Z}_{>1} : \gcd(a,b) = 1, \quad -\left(x^{ab-b+1} \bmod \left((x^a-1)(x^b-1)\right)\right) \bmod x = 1.$$

This corresponds to the case $\gcd(a,b) = 1$ from the formula in the theorem.

The proof is complete, as we have shown that the two cases $\gcd(a,b) > 1$ and $\gcd(a,b) = 1$ in the given formula both yield the expected result. □

Corollary 7. *Let $a, b, n \in \mathbb{Z}_{>1}$ such that $n > 2$. Then*

$$\epsilon(a,b) = -\left(n^{ab-b+1} \bmod \left((n^a-1)(n^b-1)\right)\right) \bmod n$$

Proof. The proof is the same as in Corollary 3, replacing the formula for $\gcd(a,b)$ with the given formula for $\epsilon(a,b)$. □

Our coprimality formula in Corollary 7 leads us to a conjecture on Euler's totient function.

Conjecture 1. *Let $n \in \mathbb{Z}_{>1}$. Define*

$$t(n) = \begin{cases} 0 & \text{if } n \equiv 2, 10 \pmod{12}, \\ 1 & \text{if } n \not\equiv 2, 10 \pmod{12}. \end{cases}$$

Then

$$\varphi(n) - t(n) = \left\lfloor \sum_{k=1}^{n-1} \frac{n^{nk-k+1}}{(n^n-1)(n^k-1)} \right\rfloor \bmod n,$$

where $\varphi(n)$ denotes Euler's totient function for n.

3 Exponent Reduction in GCD Calculations

We now prove a simple theorem which allows us to reduce the exponents used in our GCD formulas.

Theorem 8. *Let $a, b \in \mathbb{Z}^+$ such that $a \geq b$. Set $\ell = (a \bmod b)$. Then*

$$\gcd(a,b) = \left\lfloor \frac{x^{\ell+\ell b}}{(x^\ell - 1)(x^b - 1)} \right\rfloor \bmod x.$$

and

$$\gcd(a,b) = -\left(x^{\ell+\ell b} \bmod \left((x^\ell - 1)(x^b - 1)\right)\right) \bmod x.$$

Proof. These formulas follow immediately from Theorem 2 and Theorem 4 by a property of the GCD function, which is: $\forall a, b > 0,\ \gcd(a,b) = \gcd(a \bmod b, b) = \gcd(a, b \bmod a)$. □

Since $\gcd(a,b) = \gcd(b,a)$, we can apply Theorem 8 recursively to a and b to reduce the exponents even further. This procedure can be defined as a simple algorithm, which is essentially the same as the process of applying the Euclidean algorithm to calculate $\gcd(a,b)$.

Algorithm 1 (GCD Exponent Reduction)**. Inputs**: $a, b \in \mathbb{Z}^+$.

Steps:

1. If $b > a$, then swap the values of a and b, so that $a = \max(a,b)$ and $b = \min(a,b)$.
2. Set $a_0 = a$ and $b_0 = b$ and define the recurrence relations:
$$a_{i+1} = (a_i \bmod b_i),$$
$$b_{i+1} = (b_i \bmod a_{i+1}).$$
3. Starting from $i = 0$, step through the recurrences by setting $i = i + 1$ until we find $b_k = 0$ for some $k = i$, and then halt.
4. Set $\alpha = \min(a_k, b_{k-1})$ and $\beta = \max(a_k, b_{k-1})$.
5. Finally, calculate
$$\gcd(a,b) = -\left(x^{\alpha+\alpha\beta} \bmod ((x^\alpha - 1)(x^\beta - 1))\right) \bmod x.$$

Since Algorithm 1 mimics the process of calculating $\gcd(a,b)$ by way of the Euclidean algorithm, there is no practical sense in carrying it out to completion. However, when writing and evaluating arithmetic terms, performing a single iteration of the recursion and then setting the exponents to either a_1, b_0 or a_1, b_1 (depending on divisibility properties of a and b) can result in a significant performance improvement in the event $a \gg b$ or $b \gg a$.

4 Semiprime Factors

Using our results on the greatest common divisor function (§ 2), as well as results from our earlier works [15, 13] and those of Mazzanti [3], Robinson [8], Prunescu and Sauras-Altuzarra [12], we discover arithmetic term formulas for the prime factors of a non-square semiprime $n = pq$.

Theorem 9. *Let $n \in \mathbb{Z}^+$ such that $n = pq$ is a non-square semiprime and $p < q$ are the prime factors of n. Define*

$$\omega = \left\lfloor \frac{(n^{2n} + 1)^{2n+1} \bmod (n^{4n} - n)}{(n^{2n} + 1)^{2n} \bmod (n^{4n} - n)} \right\rfloor - 1.$$

Then, set

$$\gamma = \left\lfloor \frac{(\omega+1)^{\omega\cdot(\omega+2)}}{\left\lfloor \frac{\left((\omega+1)^{\omega\cdot(\omega+2)}+1\right)^{(\omega+1)^{\omega+2}}}{(\omega+1)^{\omega^2\cdot(\omega+2)}} \right\rfloor \bmod (\omega+1)^{\omega\cdot(\omega+2)}} \right\rfloor.$$

Finally, we have

$$p = \left\lfloor \frac{n^{n+n(\gamma \bmod n)}}{(n^n-1)(n^{\gamma \bmod n}-1)} \right\rfloor \bmod n.$$

Proof. From Shunia (2024) [13], for n that is not a square, we get the arithmetic term

$$\lfloor\sqrt{n}\rfloor = \left\lfloor \frac{(n^{2n}+1)^{2n+1} \bmod (n^{4n}-n)}{(n^{2n}+1)^{2n} \bmod (n^{4n}-n)} \right\rfloor - 1,$$

which matches our definition of ω. Hence, $\omega = \lfloor\sqrt{n}\rfloor$.

From Prunescu and Sauras-Altuzarra (2024) [12], we also have the factorial formula

$$n! = \left\lfloor \frac{2^{n(n+1)(n+2)}}{\left\lfloor \left(2^{2^{(n+1)(n+2)}-n}+2^{-n}\right)^{2^{(n+1)(n+2)}} \right\rfloor \bmod 2^{2^{(n+1)(n+2)}}.} \right\rfloor$$

The factorial formula of Prunescu and Sauras-Altuzarra is derived from an identity of Robinson (1952) [8], which is

$$\forall r \in \mathbb{Z} : r \geq (n+1)^{n+2}, \quad n! = \left\lfloor r^n / \binom{r^n}{n} \right\rfloor.$$

Hence, the formula is also valid for $r = (n+1)^{n+2}$, which grows more slowly than $2^{(n+1)\cdot(n+2)}$ as $n \to \infty$. Making the substitutions and simplifying, we find

$$n! = \left\lfloor \frac{(n+1)^{n\cdot(n+2)}}{\left\lfloor \frac{\left((n+1)^{n\cdot(n+2)}+1\right)^{(n+1)^{n+2}}}{(n+1)^{n^2\cdot(n+2)}} \right\rfloor \bmod (n+1)^{n\cdot(n+2)}} \right\rfloor.$$

Considering $\omega!$, this becomes

$$\omega! = \left\lfloor \frac{(\omega+1)^{\omega\cdot(\omega+2)}}{\left\lfloor \frac{\left((\omega+1)^{\omega\cdot(\omega+2)}+1\right)^{(\omega+1)^{\omega+2}}}{(\omega+1)^{\omega^2\cdot(\omega+2)}} \right\rfloor \bmod (\omega+1)^{\omega\cdot(\omega+2)}} \right\rfloor,$$

which matches the definition for γ. Hence, $\gamma = \omega! = \lfloor\sqrt{n}\rfloor!$. Applying Corollary 3, we have

$$\gcd(n, \lfloor\sqrt{n}\rfloor!) = \gcd(n, \gamma) = \left\lfloor \frac{n^{n+n\gamma}}{(n^n-1)(n^\gamma-1)} \right\rfloor \bmod n.$$

Since n is a non-square semiprime and $p < q$, we must have $p \leq \lfloor\sqrt{n}\rfloor$ and $q > \lfloor\sqrt{n}\rfloor$. Hence, $p = \gcd(n, \lfloor\sqrt{n}\rfloor!)$. To reduce the exponent γ, we apply Theorem 8, which yields

$$\gcd(n, \lfloor\sqrt{n}\rfloor!) = \left\lfloor \frac{n^{n+n(\gamma \bmod n)}}{(n^n-1)(n^{\gamma \bmod n}-1)} \right\rfloor \bmod n.$$

□

Corollary 10. *Let $n = pq$ be a non-square semiprime. Then*

$$q = \frac{n}{\left\lfloor \frac{n^{n+n(\gamma \bmod n)}}{(n^n-1)(n^{\gamma \bmod n}-1)} \right\rfloor \bmod n}.$$

Proof. The proof follows immediately from Theorem 9, since $\frac{n}{p} = q$ in this case. □

Corollary 11. *Let $\varphi(n)$ represent Euler's totient function for $n = pq$, a non-square semiprime. Then*

$$\varphi(n) = \left(\left(\left\lfloor \frac{n^{n+n(\gamma \bmod n)}}{(n^n-1)(n^{\gamma \bmod n}-1)} \right\rfloor \bmod n \right) - 1 \right) \left(\left(\frac{n}{\left\lfloor \frac{n^{n+n(\gamma \bmod n)}}{(n^n-1)(n^{\gamma \bmod n}-1)} \right\rfloor \bmod n} \right) - 1 \right).$$

Proof. The proof follows immediately from Theorem 9, since $\varphi(n) = (p-1)(q-1)$ in this case. □

References

[1] D. E. Knuth. *The Art of Computer Programming, 3rd Edition*, volume 1. Addison Wesley Longman Publishing Co., Inc., USA, 1997. ISBN 0201896834.

[2] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM*, 21(2):120–126, feb 1978. ISSN 0001-0782. URL https://doi.org/10.1145/359340.359342.

[3] S. Mazzanti. Plain Bases for Classes of Primitive Recursive Functions. *Mathematical Logic Quarterly*, 48(1):93–104, 2002. ISSN 0942-5616.

[4] S. S. Marchenkov. A Superposition Basis in the Class of Kalmar Elementary Functions. *Mathematical Notes of the Academy of Sciences of the USSR*, 27(3):161–166, 1980. ISSN 0001-4346.

[5] G. T. Herman. A New Hierarchy of Elementary Functions. *Proceedings of the American Mathematical Society*, 20(2): 557–562, 1969. ISSN 0002-9939.

[6] S. S. Marchenkov. Superpositions of Elementary Arithmetic Functions. *Journal of Applied and Industrial Mathematics*, 1(3):351–360, 2007. ISSN 1990-4789.

[7] A. Grzegorczyk. Some Classes of Recursive Functions. *Rozprawy Matematyczne*, 4, 1953. URL http://matwbn.icm.edu.pl/ksiazki/rm/rm04/rm0401.pdf.

[8] J. Robinson. Existential Definability in Arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. ISSN 0002-9947.

[9] M. Davis, H. Putnam, and J. Robinson. The Decision Problem for Exponential Diophantine Equations. *Annals of Mathematics*, 74(3):425–436, 1961. ISSN 0003-486X.

[10] Y. Matiyasevich. A New Proof of the Theorem on Exponential Diophantine Representation of Enumerable Sets. *Journal of Soviet Mathematics*, 14(5):1475–1486, 1980. ISSN 0090-4104.

[11] Y. Matiyasevich. *Hilbert's Tenth Problem*. MIT press, 1993. ISBN 0-262-13295-8.

[12] M. Prunescu and L. Sauras-Altuzarra. An Arithmetic Term for the Factorial Function. *Examples and Counterexamples*, 5:100136, 2024. ISSN 2666-657X. URL https://sciencedirect.com/science/article/pii/S2666657X24000028.

[13] J. M. Shunia. Polynomial Quotient Rings and Kronecker Substitution for Deriving Combinatorial Identities, 2024. URL https://arxiv.org/abs/2404.00332.

[14] A. Shamir. Factoring Numbers in O(log n) Arithmetic Steps. *Information Processing Letters*, 8(1):28–31, 1979. ISSN 0020-0190. URL https://sciencedirect.com/science/article/pii/0020019079900875.

[15] J. M. Shunia. A Simple Formula for Single-Variable Multinomial Coefficients, 2023. URL https://arxiv.org/abs/2312.00301.

[16] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation For Computer Science*. Addison-Wesley Professional, 1994.

[17] O. Ore. The General Chinese Remainder Theorem. *The American Mathematical Monthly*, 59(6):365–370, 1952. URL https://doi.org/10.1080/00029890.1952.11988142.