Elementary Formulas for Greatest Common Divisors and Semiprime Factors

Joseph M. Shunia

June 19, 2024
Revised: June 22, 2024
Version 2

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 result of Mazzanti, and is derived using Kronecker substitution techniques from our previous work. We utilize the GCD formula, along with recent developments on arithmetic terms for square roots and factorials, to derive explicit expressions for the prime factors of a semiprime $n = pq$.

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, which are numbers with exactly two prime factors, also 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 and 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.

An "arithmetic term" is a mathematical expression which uses only the operations of addition $(a + b)$, subtraction $(a - b)$, multiplication (ab), floored division $(\lfloor a/b \rfloor)$, and exponentiation a^b. Note that the modulo operation $(a \bmod b)$ is implied, since it can be expressed using subtraction, multiplication, and floored division as

$$a \bmod b = a - b \lfloor a/b \rfloor .$$

Let $\mathbf{A}$ denote the class of arithmetic terms. Formally, we have

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

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 term formulas for the prime factors of a non-square semiprime $n = pq$, using only the operations of addition, subtraction, multiplication, floored division, and exponentiation.

1.1 Background

Our new arithmetic term formulas for GCDs and semiprime factors, while entirely impractical, are of theoretical importance. We provide a brief overview and some historical context to demonstrate their significance.

1.2 Kalmar Functions

Firstly, 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 $\mathbf{P}$, defined as

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

where the notation $\dot{-}$ represents so-called "bounded" or "modified" subtraction (See [3] for a precise definition).

Kalmar functions were introduced by Laszlo Kalmar in the 1940s as a subclass $\mathbf{P}$. 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 $\mathbf{K}$) [5]. 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.

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 summary, we have

$$[\mathbf{A}] = \mathbf{K} \subset \mathbf{P}.$$

In 1970, Matiyasevich, building on the work of Davis et al [7], proved that all computable functions can be expressed as Diophantine equations [8, 9]. Matiyasevich's result implies that there exists a Diophantine equation for calculating the n-th prime number. However, no arithmetic term for the n-th prime is known [10]. 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 explicit arithmetic term formulas for this problem.

1.3 Latest Discoveries

Recently, Prunescu and Sauras-Altuzarra (2024) discovered an arithmetic term for computing the factorial function $n!$ [10]. Coincidentally, at approximately the same time, we discovered an arithmetic term for the n-th roots of positive integers $\sqrt[n]{a}$ [11]. By combining these results, along with a simplified version of Mazzanti's GCD formula (Lemma 1), we obtain the first explicit arithmetic terms for semiprime factors. This answers a question from Shamir (1978), who first hypothesized the existence of such a formula when describing an algorithmic approach to integer factorization using arithmetic terms [12].

2 Greatest Common Divisor

Lemma 1 (Mazzanti)**.**

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

Proof. The lemma and proof belong to Mazzanti (2002) [3]. □

Applying Kronecker substitution techniques from our previous works [13, 11], we find that Mazzanti's formula can be simplified and expressed 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

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

The substitution is valid, since $2^{ab} > \gcd(a,b)$ and the substitution $2^{ab} = x$ essentially inverts the Kronecker substitution with the base 2^{ab} (See Theorem 1 in [13]).

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 $\gcd(a,b)$. We find

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

$\square$

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 [11], 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. $\square$

Theorem 4.

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

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

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

Taking the numerator and denominator mod x, we find

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

Hence, we can say

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

□

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

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

Proof. Consider the polynomial formula given by Theorem 2. Substituting with $x = n$ yields the given formula. By Theorem 2 in [11], 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. □

3 Semiprime Factors

Using our results on the greatest common divisor function (§ 2), as well as results from our earlier works [13, 11] and those of Mazzanti [3], Prunescu and Sauras-Altuzarra [10], we discover arithmetic term formulas for the prime factors of a non-square semiprime $n = pq$.

Theorem 6. *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

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

Proof. From Shunia (2024) [11], 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) [10], we also have the factorial formula

$$\begin{aligned} n! &= \left\lfloor 2^{n\cdot(n+1)\cdot(n+2)} \Big/ \binom{2^{(n+1)\cdot(n+2)}}{n} \right\rfloor \\ &= \left\lfloor \frac{2^{n\cdot(n+1)\cdot(n+2)}}{\left\lfloor \left(2^{2^{(n+1)\cdot(n+2)}-n} + 2^{-n}\right)^{2^{(n+1)\cdot(n+2)}} \right\rfloor \bmod 2^{2^{(n+1)\cdot(n+2)}}} \right\rfloor. \end{aligned}$$

The factorial formula of Prunescu and Sauras-Altuzarra is derived from an identity of Matiyasevich (1993) [9], which is

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

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 $p \le \lfloor\sqrt{n}\rfloor$ and $q > \lfloor\sqrt{n}\rfloor$. Hence, $p = \gcd(n, \lfloor\sqrt{n}\rfloor!)$, which we showed is equivalent to the formula in the theorem. □

Corollary 7. *Let $n = pq$ be a non-square semiprime. Then*

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

Proof. The proof follows immediately from Theorem 6, since $\frac{n}{p} = q$ in this case. □

Corollary 8. *Let $\varphi(n)$ represent Euler's totient function for $n = pq$, a non-square semiprime. Then*

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

Proof. The proof follows immediately from Theorem 6, 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 Kal'mar 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] 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.

[8] 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.

[9] Y. Matiyasevich. *Hilbert's Tenth Problem*. MIT press, 1993. ISBN 0-262-13295-8. See p. 46, formula 3.4.6.

[10] 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.

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

[12] 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.

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