Elementary Formulas for Greatest Common Divisors and Semiprime Factors

Joseph M. Shunia

June 19, 2024

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 elementary formulas for square roots and factorials, to derive explicit expressions for the prime factors of a semiprime $n = p_1 p_2$.

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 $n = p_1 p_2$ into its constituent primes p_1 and p_2 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.

In this paper, we present new results on arithmetic 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 elementary formulas for the prime factors of a non-square semiprime $n = p_1 p_2$, using only the operations of addition, subtraction, multiplication, floored division, and exponentiation.

1.1 Background

Our formulas, while entirely impractical, are of theoretical importance. We provide a brief overview and some historical context to demonstrate their significance.

Firstly, we denote by $\mathbf{E}$ the class of elementary functions.

In 1980, Matiyasevich proved that all computable functions can be expressed as Diophantine equations [5, 6]. This result was groundbreaking, as it implies that all computable functions are contained within the class **E**. However, Matiyasevich's proof is non-constructive, and it does not provide a formulaic or systematic approach for constructing such elementary representations. To put this into perspective, Matiyasevich's result implies that there exists an elementary formula for calculating the n-th prime number, even though no such elementary formula is currently known [7]. Similarly, the existence of an elementary formula for semiprime factors is also implied by Matiyasevich; we are the first to discover such a formula.

1.2 Arithmetic Terms

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 and floored division:

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

Let **A** denote the class of arithmetic terms. Formally, we have

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

1.3 Kalmar Functions

The class of Kalmar functions, denoted by **K**, is the class of functions 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 of the primitive recursive functions. 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 **K**) [8].

The class **K** is known to be a subset of **E**, though whether or not it is proper remains an open question. It was long conjectured, and finally proved by Mazzanti, that the class **A** generates the class **K** [3, 9]. Based on current knowledge, this means

$$\mathbf{A} \subseteq \mathbf{K} \subset \mathbf{E},$$

where the strictness of the second inclusion is unknown.

It is well-established that **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, the exact relationship between **K** and **E** remains an open problem in computability theory and mathematical logic. Some researchers conjecture that **K** is indeed a proper subset of **E**, meaning that there exist elementary functions that cannot be expressed using Kalmar elementary recursion. However, finding a specific example of such a function or proving that no such function exists has proven to be a challenging problem.

1.4 Latest Discoveries

Recently, Prunescu and Sauras-Altuzarra (2024) discovered an arithmetic term for computing the factorial function $n!$ [7]. Coincidentally, at approximately the same time, we discovered an elementary formula for the n-th roots of positive integers [10]. 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 [11].

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 [12, 10], 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 [12]).

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

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

□

Corollary 3. *Let $a, b, n \in \mathbb{Z}^+$ such that $n > \gcd(a,b)$. 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 [10], the substitution is valid since $n > \gcd(a,b)$. □

3 Semiprime Factors

Using our results on the greatest common divisor function (§ 2), as well as results from our earlier works [12, 10] and those of Mazzanti [3], Prunescu and Sauras-Altuzarra [7], we discover elementary formulas for the prime factors of a non-square semiprime $n = p_1 p_2$. We say these formulas are "elementary", since they require only addition, subtraction, multiplication, floored division, and exponentiation.

Theorem 4. *Let $n \in \mathbb{Z}^+$ such that $n = p_1 p_2$ is a non-square semiprime and $p_1 < p_2$ 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

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

Finally, we have

$$p_1 = \left\lfloor \frac{n^{n+n\gamma}}{(n^n - 1)(n^\gamma - 1)} \right\rfloor \bmod n.$$

Proof. From Shunia (2024) [10], 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) [7], we also have the factorial formula

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

Considering $\omega!$, this becomes

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

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 $p_1 < p_2$, we must have $p_1 < \lfloor \sqrt{n} \rfloor$ and $p_2 > \lfloor \sqrt{n} \rfloor$. Hence, $p_1 = \gcd(n, \lfloor \sqrt{n} \rfloor !)$, which we showed is equivalent to the formula in the theorem. □

Corollary 5.

$$p_2 = \frac{n}{\left\lfloor \frac{n^{n+n\gamma}}{(n^n-1)(n^\gamma-1)} \right\rfloor \bmod n}.$$

Proof. The proof follows immediately from Theorem 4, since $\frac{n}{p_1} = p_2$ 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] L. Adleman R. L. Rivest, A. Shamir. 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] Y. V. 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.

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

[7] 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.

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

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

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

[11] 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.

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