ARITHMETIC-TERM REPRESENTATIONS FOR THE GREATEST COMMON DIVISOR

Mihai Prunescu
Research Center for Logic, Optimization and Security (LOS), Faculty of Mathematics and Computer Science,
University of Bucharest, Bucharest, Romania
and
Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania
mihai.prunescu@imar.ro, mihai.prunescu@gmail.com

Joseph M. Shunia
Ann Arbor, Michigan
jshunia@gmail.com

Received: 6/11/25, Accepted: 7/8/26, Published:

Abstract

We construct a new arithmetic-term representation for the greatest common divisor function $\gcd(a,b)$. As a byproduct, we also deduce a representation of $\gcd(a,b)$ by a modular term in integer arithmetic.

1. Introduction

In [3] Mazzanti proved the following identity:

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

for all $a, b \in \mathbb{N}$ with $a, b \geq 1$. Marchenkov later confirmed this formula; see [2]. This identity had been the missing puzzle-piece to show that every Kalmár elementary function is representable as an arithmetic term. Arithmetic terms are defined in [2] and [3] as terms built up in the language $L = \{+, \dot{-}, \cdot, /, x^y\}$ with variables and constants interpreted in the set of natural numbers. The modified difference $x \dot{-} y$ is defined to be 0 if $x < y$. For applications, see [8]. See also [5].

As Mazzanti's effective method to compute arithmetic-term representations depends explicitly on the arithmetic-term representation of the greatest common divisor, every simplification of this term has theoretical importance. Shunia conjectured

DOI: 10.5281/zenodo.21678383

in [7] specific simplified formulas for the greatest common divisor. Here we prove a different simplification by an independent generating-function method. We present a straightforward construction of a simpler term, independent of Mazzanti's, although both constructions use Lemma 1.

2. Prerequisites

Under $\mathbb{N}$ we understand the set of natural numbers including 0. We will need the following facts. The first lemma, from [1], will be used to make a connection between the value $\gcd(a, b)$ and the number of solutions in natural numbers of a particular linear Diophantine equation.

Lemma 1. *The Diophantine linear equation*

$$ax + by = c$$

has solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ if and only if $d = \gcd(a, b) \mid c$. If $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ is a solution of the equation $ax+by = c$, then all solutions are given by $x = x_0+(b/d)\cdot t$ and $y = y_0 - (a/d) \cdot t$ where $t \in \mathbb{Z}$ is arbitrary.

The second lemma is a tool, due to Prunescu and Sauras-Altuzarra [6], that has proved useful for representing sequences whose generating functions are rational as arithmetic terms.

Lemma 2. *Let $f \in \mathbb{N}[[z]]$ be a formal series with radius of convergence $R > 0$ at 0,*

$$f(z) = \sum_{n\geq 0} s(n)z^n.$$

Let $c, m \in \mathbb{N}$ be such that $c^{-1} < R$ and for all $n \geq m$, $s(n) < c^{n-2}$. Then for all $n \geq m$,

$$s(n) = \left\lfloor c^{n^2} f(c^{-n}) \right\rfloor \bmod c^n.$$

The third lemma is an identity in modular arithmetic.

Lemma 3. *Let $A, B, C \in \mathbb{Z}$ such that $A, B > 0$, $C \geq 2$, $C \mid A$, $B \nmid A$, $B \bmod C = 1$ and $\lfloor A/B \rfloor \bmod C \neq C - 1$. Then the following identity holds*

$$((-A) \bmod B) \bmod C = 1 + \lfloor A/B \rfloor \bmod C.$$

Proof. One observes that

$$\begin{aligned}
((-A) \bmod B) \bmod C &= ((-A) - B \cdot \lfloor (-A)/B \rfloor) \bmod C \\
&= ((-A) \bmod C - (B \bmod C) \cdot (\lfloor (-A)/B \rfloor \bmod C)) \bmod C \\
&= (0 - 1 \cdot (\lfloor (-A)/B \rfloor \bmod C)) \bmod C \\
&= (-(\lfloor (-A)/B \rfloor \bmod C)) \bmod C \\
&= (-\lfloor (-A)/B \rfloor) \bmod C.
\end{aligned}$$

On the other hand, for $A, B > 0$ such that $B \nmid A$,

$$-\lfloor(-A)/B\rfloor = \lfloor A/B\rfloor + 1,$$

so the quantity to compute is

$$(\lfloor A/B\rfloor + 1) \bmod C.$$

Further we recall that for $x \geq 0$ and $C \geq 2$ such that $x \not\equiv (C-1) \mod C$,

$$(1+x) \bmod C = 1 + (x \bmod C).$$

We apply this fact for $x = \lfloor A/B\rfloor$ to get

$$1 + \lfloor A/B\rfloor \bmod C. \qquad \square$$

3. A Family of C-Recursive Sequences

We use the following standard definition.

Definition 1. C-recursive sequences of order d are sequences $s : \mathbb{N} \to \mathbb{C}$ satisfying a relation of recurrence with constant coefficients

$$s(n+d) + a_1 s(n+d-1) + \cdots + a_{d-1} s(n+1) + a_d s(n) = 0$$

for all $n \geq 0$.

Theorem 4.1.1 in [9] and Theorem 1 in [4] imply the following characterization. The C-recursive sequences are exactly the sequences $(s(n))$ such that the generating function

$$f(z) = \sum_{n \geq 0} s(n) z^n$$

is a rational function $A(z)/B(z)$ with $\deg(A) < \deg(B)$.

We now introduce the family of sequences used below.

Definition 2. Let a, b be natural numbers with $a, b \geq 1$ and let $(s_{a,b}(n))$ be the sequence with generating function

$$f_{a,b}(z) := \frac{1}{(z^a - 1)(z^b - 1)}.$$

The generating function has the following elementary interpretation.

Lemma 4. *For all $a, b \in \mathbb{N}$, $a, b \geq 1$, the sequence $(s_{a,b}(n))$ consists of natural numbers. In particular,*

$$s_{a,b}(ab) = \gcd(a, b) + 1.$$

Proof. We observe that

$$\frac{1}{(z^a-1)(z^b-1)} = (1+z^a+z^{2a}+z^{3a}+\cdots)(1+z^b+z^{2b}+z^{3b}+\cdots).$$

Here the two sign flips from $z^a-1=-(1-z^a)$ and $z^b-1=-(1-z^b)$ cancel. It follows that for all $n\in\mathbb{N}$, $s_{a,b}(n)$ is indeed a natural number. Moreover, the value of $s_{a,b}(n)$ equals the number of solutions $(x,y)\in\mathbb{N}\times\mathbb{N}$ of the equation

$$ax+by=n.$$

For $n=ab$ we observe that $(x_0,y_0)=(b,0)$ is indeed a solution of the equation

$$ax+by=ab.$$

By Lemma 1, the set of solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ is parametrized by a parameter $t\in\mathbb{Z}$ and the solutions have the form

$$\begin{aligned} x &= b-\frac{b}{d}\cdot t,\\ y &= \frac{a}{d}\cdot t, \end{aligned}$$

where $d=\gcd(a,b)$. As only the non-negative solutions count, t must fulfill

$$b\geq\frac{b}{d}\cdot t \quad\text{and}\quad t\geq 0.$$

So $0\leq t\leq d=\gcd(a,b)$, hence there are $\gcd(a,b)+1$ solutions in $\mathbb{N}\times\mathbb{N}$. □

We also need the following uniform bound.

Lemma 5. *If $a,b\geq 1$ are natural numbers and at least one of them is greater than 1, then for all $n\in\mathbb{N}$ one has*

$$s_{a,b}(n)\leq s_{1,1}(n)=n+1.$$

One has $s_{a,b}(n)=s_{1,1}(n)$ only if $n=0$.

Proof. We first observe that

$$f_{1,1}(z)=\frac{1}{(z-1)^2}=\sum_{n\geq 0}(n+1)z^n,$$

so for all $n\in\mathbb{N}$, $s_{1,1}(n)=n+1$.

Since $f_{a,b}(z)=f_{b,a}(z)$, we may assume without loss of generality that $a>1$. In order to prove the inequality, we observe that $s_{1,1}(n)$ is the number of pairs $(X,Y)\in\mathbb{N}\times\mathbb{N}$ such that

$$X+Y=n,$$

while $s_{a,b}(n)$ is the number of pairs $(x, y) \in \mathbb{N} \times \mathbb{N}$ such that

$$ax + by = n.$$

But $(x, y) \mapsto (X, Y) = (ax, by)$ is a one-to-one mapping from the set of solutions of the second equation to the set of solutions of the first one. If $n > 0$, this mapping cannot be onto, as its images always have multiples of a on the first component, while for some $0 \leq k \leq n$ the pair $(X, Y) = (k, n - k)$ has first component not divisible by a and satisfies the first equation. □

4. Main Results

We now prove the main result.

Theorem 1. *Let $a, b \geq 1$ be two natural numbers. Then*

$$\gcd(a, b) = \left(\left\lfloor \frac{5^{ab(ab+a+b)}}{(5^{a^2b} - 1)(5^{ab^2} - 1)} \right\rfloor \bmod 5^{ab} \right) - 1.$$

Proof. We specialize Lemma 2 to the generating function $f_{a,b}$ and then choose a base c that works uniformly for all $a, b \geq 1$. The sequences $s_{a,b}(n)$ have arithmetic-term representations given by

$$\left\lfloor c^{n^2} f_{a,b}(c^{-n}) \right\rfloor \bmod c^n = \left\lfloor \frac{c^{n^2+an+bn}}{(c^{an} - 1)(c^{bn} - 1)} \right\rfloor \bmod c^n,$$

where a priori the constant c depends on the pair (a, b). We will show that one can find constants $c \in \mathbb{N}$ that successfully represent all sequences $s_{a,b}(n)$ for $n \geq m$, where the rank m depends only on c.

Let $R_{a,b}$ be the convergence radius at $z = 0$ for the meromorphic function $f_{a,b}(z)$. The set of poles $\mathcal{P}(f_{a,b})$ consists of roots of 1 only,

$$\mathcal{P}(f_{a,b}) = \mathcal{U}(a) \cup \mathcal{U}(b),$$

where $\mathcal{U}(m) = \{z \in \mathbb{C} \mid z^m = 1\}$. As all these poles $u \in \mathbb{C}$ have $|u| = 1$, we deduce that uniformly $R_{a,b} = 1$ for all $a, b \geq 1$. Hence the condition $c^{-1} < R_{a,b}$ is uniformly satisfied for all $c \in \mathbb{N}$, $c \geq 2$.

The condition $s_{a,b}(n) < c^{n-2}$ for all $n \geq m$ and some $m \in \mathbb{N}$ can be uniformly satisfied for all $a, b \geq 1$. Indeed, Lemma 5 gives $s_{a,b}(n) < n + 1$ for $n > 0$ and $(a, b) \neq (1, 1)$, while $s_{1,1}(n) = n + 1$. Thus for all $a, b \geq 1$ and $n > 0$ one has

$$s_{a,b}(n) \leq n + 1.$$

So we observe that already for $c = 2$,

$$s_{a,b}(n) < n + 1 < 2^{n-2}$$

for all $n \geq 5$ and $(a, b) \neq (1, 1)$. This shows that one may uniformly take $c = 2$, and the representation then works for $n \geq 5$ for all $(a, b) \neq (1, 1)$. We still have to make the substitution $n = ab$ and get that

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

for $ab \geq 5$ and $c = 2$. However, as we want a formula that is true for all $a, b \geq 1$, we have to look for larger values of c. The condition that one gets a good result for $a = b = 1$ reads

$$2 = \left\lfloor \frac{c^3}{(c-1)^2} \right\rfloor \bmod c.$$

For $c = 2, 3, 4$ the right-hand side evaluates to $0, 0, 3$ respectively. The first value of c to satisfy this condition is $c = 5$. For $c = 5$, the inequality

$$n + 1 < 5^{n-2}$$

is fulfilled by all $n \geq 3$. Hence the coefficient-extraction formula works uniformly with $c = 5$ for all $a, b \geq 1$ and $ab \geq 3$. The remaining cases with $ab < 3$ are $(a, b) \in \{(1, 1), (1, 2), (2, 1)\}$. For the critical case $(1, 1)$, one has

$$\left\lfloor \frac{5^3}{(5-1)^2} \right\rfloor \bmod 5 = \left\lfloor \frac{125}{16} \right\rfloor \bmod 5 = 7 \bmod 5 = 2 = \gcd(1, 1) + 1.$$

Direct computation for $(1, 2)$ and $(2, 1)$ likewise gives $\gcd(a, b) + 1 = 2$. □

The div–mod formula has the following mod–mod consequence.

Corollary 1. *Let $a, b \geq 1$ be two natural numbers. Then*

$$\gcd(a, b) = \left(\left(\left(-5^{ab(ab+a+b)} \right) \bmod \left((5^{a^2b} - 1)(5^{ab^2} - 1) \right) \right) \bmod 5^{ab} \right) - 2.$$

Proof. We introduce the following notation: $A := 5^{ab(ab+a+b)}$, $B := (5^{a^2b} - 1)(5^{ab^2} - 1)$ and $C := 5^{ab}$. In order to apply Lemma 3, we check its conditions. The conditions $A, B > 0$, $C \geq 2$, $C \mid A$, $B \nmid A$, $B \bmod C = 1$ are evidently fulfilled. It remains to show that

$$\lfloor A/B \rfloor \bmod C \neq C - 1.$$

But we know that $\lfloor A/B \rfloor \bmod C = \gcd(a, b) + 1$ and $C = 5^{ab}$, so we have to show that $\gcd(a, b) + 1 \neq 5^{ab} - 1$. Since $\gcd(a, b) + 1 = s_{a,b}(ab) \leq ab + 1$, it is enough to show that

$$ab + 1 < 5^{ab} - 1$$

for all $a, b \geq 1$. Denote $ab = k \geq 1$. We observe that the inequality

$$k + 2 < 5^k$$

holds for all $k \geq 1$. □

By proving inequalities and verifying the remaining cases

$$(1,2), (2,1), (1,3), (3,1), (1,4), (4,1), \quad \text{and} \quad (2,2),$$

as in the proofs of Theorem 1 and Corollary 1, one obtains the following result.

Corollary 2. *For all natural numbers $a, b \geq 1$ with $(a,b) \neq (1,1)$ the following identities hold true:*

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

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

If one replaces the exponentiation base $c = 2$ with the base $c = 3$ or $c = 4$, the identities hold true for all $a, b \geq 1$, with the unique exception $(a,b) = (1,1)$ again. For these bases, the remaining cases to verify are $(1,2), (2,1), (1,3)$ and $(3,1)$.

Remark 1. The mod–mod representations given in Corollaries 1 and 2 are not arithmetic terms in the sense of [3] and [2]. Indeed, the subterm $-c^{ab(ab+a+b)}$ contains an essential negative sign. However, the mod–mod representations have computational advantages over the div–mod representations, because the subterm

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

can be computed much faster than the analogous

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

by using the Algorithm for Fast Exponentiation in modular arithmetic. □

References

[1] D. Burton, *Elementary Number Theory*, Allyn and Bacon, revised printing, Boston, 1980.

[2] S. S. Marchenkov, Superpositions of elementary arithmetic functions, *J. Appl. Ind. Math.* **1** (3) (2007), 351–360.

[3] S. Mazzanti, Plain bases for classes of primitive recursive functions, *Math. Log. Q.* **48** (1) (2002), 93–104.

[4] M. Petkovšek and H. Zakrajšek, Solving linear recurrence equations with polynomial coefficients, in *Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions*, Texts and Monographs in Symbolic Computation, Springer, Vienna, 2013, 259–284.

[5] M. Prunescu and L. Sauras-Altuzarra, Computational considerations on the representation of number-theoretic functions by arithmetic terms, *J. Log. Comput.* **35** (3) (2025), exaf012, 37 pp.

[6] M. Prunescu and L. Sauras-Altuzarra, On the representation of C-recursive integer sequences by arithmetic terms, *J. Difference Equ. Appl.* **31** (9) (2025), 1263–1285.

[7] J. M. Shunia, Elementary formulas for greatest common divisors and semiprime factors, preprint, `arXiv:2407.03357v3`, 2024.

[8] J. M. Shunia and L. Sauras Altuzarra, Arithmetic terms for sums of multinomial coefficients, *Ramanujan J.* **68** (3) (2025), Paper No. 93, 12 pp.

[9] R. P. Stanley, *Enumerative Combinatorics*, Volume 1, Cambridge University Press, Cambridge, second edition, 2011.