Nonlinearity In Similar Structures: On $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$, And $g^u=f^v$.

Michael C. Nwogugu
Enugu 400007, Enugu State, Nigeria
Phone: 234-909-606-8162
Emails: mcn2225@gmail.com; mcn2225@aol.com

Abstract.

Liptai, Németh, et. al. (2020) conjectured (and supposedly proved) that in the diophantine equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$ in positive integers a≤b, and c≤d, the only solution to the title equation is (a,b,c,d)=(1,2,1,1). This article proves that the Liptai, Németh, et. al. (2020) conjecture and results are wrong, and that there is more than one solution for the equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$. This article introduces "*Existence Conditions*" and new theories of "*Rational Equivalence*", and a new theorem pertaining to the equation $g^u=f^v$.

Keywords: Number Theory; Exponential Diophantine Equations; Prime Numbers; Nonlinearity; Linear Recurrence; Dynamical Systems; Mathematical Cryptography; Ill-posed Problems.

1. Introduction.

The equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$ is among a class of diophantine equations that have applications in many fields including Computer Science, Applied Math, Physics and Econometrics/Economics. The nonlinear equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ is an ill-posed problem because it and both sides of the equation can vary and behave differently over the interval 0<a,b,c,d<+∞.

The main problems/deficiencies in the Liptai, Németh, et. al. (2020) analysis are as follows:

- **i)** Liptai, Németh, et. al. (2020) uses so many un-verified "assumptions" that its "proofs" are really just conjectures.
- **ii)** Liptai, Németh, et. al. (2020) didn't prove that (a+b)>(c+d) or that a,b ≥ c,d, or that (a+b)/(c+d) ≥ 1.5; all of which are critical elements of the analysis.
- **iii)** Liptai, Németh, et. al. (2020) didn't sufficiently discuss the effect(s) of the "structural" similarities of both sides of the equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$.
- **iv)** Liptai, Németh, et. al. (2020) didn't derive valid "existence" conditions for the system (the equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$ is an ill-posed problem).
- **v)** Liptai, Németh, et. al. (2020) didn't prove the lower-bound of the equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$.

2. Existing Literature.

On various approaches to solutions of diophantine equations and exponentials with different-bases, see: Bertok, Hajdu, et. al. (2017), Matveev (2000), Stewart (1980), Ibarra & Dang (2006). and Schlickewei & Schmidt (1993).

On Homomorphisms, see: Wang & Chin (2012). On Linear Recurrences, see Kuhapatanakul & Laohakosol (2019) and Morgari, Steila & Elia (2000); but the formal definitions of *Linear Recurrences* and "*Recurrence Relations*" are somewhat different from the definitions used in Liptai, Németh, et. al. (2020).

Chu (2008) and Lu & Wu (2016) studied dynamical systems pertaining to Diophantine equations (and each of the *equations* $(X^a-1)(X^b-1)=a$, $(Y^c-1)(Y^d-1)=b$, and $(X^a-1)(X^b-1)=(Y^c-1)(Y^d-1)$ can approximate Dynamical Systems). Luca, Moree & Weger (2011) discussed *Group Theory* as it relates to Diophantine Equations. Zadeh (2019) notes that Diophantine equations have been used in analytic functions. Stewart (1980), Jones, Sato, et. al. (1976) and Matijasevič (1981) noted that primes can also be represented as Diophantine equations or as polynomials (ie. each of the equations $[(X^a-1)(X^b-1)]+[(Y^c-1)(Y^d-1)]$, and $[(X^a-1)(X^b-1)]-[(Y^c-1)(Y^d-1)]$ can represent a prime). On uses of *Diophantine Equations* and *Mersenne Composite Numbers* in Cryptography, see: Ding, Kudo, et. al. (2018), Okumura (2015), Nemron (2008) and Ogura (2012) (ie. each of the equations $(X^a-1)(X^b-1)=a$; $(Y^c-1)(Y^d-1)=b$; and $[(X^a-1)(X^b-1)]-[(Y^c-1)(Y^d-1)]=c$; and $(X^a-1)(X^b-1)= (Y^c-1)(Y^d-1)$ can be used in cryptoanalysis and in the creation of public-keys).

3. The Theorems.

Theorem-1: For Any Two Exponentials $g^u = f^v$ (Whose Bases And Exponents Are Real Numbers), Regardless Of The Numerical Magnitude Of Their Exponents, The Larger The Numerical Difference Between Their "Bases" (eg. $-\infty<g, f<+\infty$) Then Smaller The Probability That There Can Be More Than One Combination Of u And v That Makes $g^u = f^v$ Valid.

Proof:

This theorem is henceforth referred to as the *Exponential Equivalence Theory*.

If $g^u = f^v$, then:

As $|g\text{-}f| \to+\infty$, then $v\oplus u \to+\infty$;

As $|g\text{-}f| \to+\infty$; then $|v\text{-}u| \to+\infty$;

As $|g\text{-}f| \to+\infty$; then $[\,|+\infty\text{-}v|\to 0] \oplus [\,|+\infty\text{-}u|\to 0]$.

Thus as $|g\text{-}f|$ increases in magnitude, there are increasingly fewer "qualifying" or "feasible" integers in the intervals $(v,+\infty)$ and or $(u,+\infty)$, and the probability that there can be more than one "feasible" combination of *u* and *v* decreases. ■

Theorem-2: For Positive Integers, *Horizontal Equivalence* And *Vertical Equivalence* Can Exist Where Terms On Both Sides Of An Equation Have Similar Mathematical "Structures".

Proof:

Assume that as a condition for $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$, it's possible that:

2.1) $(3^a-1)=(5^c-1)$, and $(3^b-1)=(5^d-1)$; or

2.2) $(3^a-1)=(5^d-1)$, and $(3^b-1)=(5^c-1)$.

The foregoing are some of the possible combinations of (3^a-1), (5^c-1), (3^b-1) and (5^d-1).

If $(3^a-1)=(5^c-1)$, and $(3^b-1)=(5^d-1)$; then by "*horizontal equivalence*":

2.3) $(3^a-1)=(5^c-1)$, and $3^a=5^c$

2.4) $(3^b-1)=(5^d-1)$, and $3^b=5^d$;

That is because (3^a-1) and (5^c-1) have similar or the same mathematical "structure" – namely, an exponential (whose base and exponent are both positive integers) from which one is subtracted. Similarly, (3^b-1) and (5^d-1), have similar or the same "structure" which is an exponential (whose base and exponent are both positive integers) from which one is subtracted. Also $(3^a-1)(3^b-1)$ and $(5^c-1)(5^d-1)$ have similar or the same mathematical "structure" – namely, the multiplicative product of exponentials (whose base and exponent are positive integers) from which one is subtracted. However, in the Equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$, $(3^a-1)(3^b-1)$ and $(5^c-1)(5^d-1)$ can behave differently over the interval $0<a,b,c,d<+\infty$ because of the differences in the magnitude of the bases and exponents.

Note that Eq.-2.3 and Eq.-2.4 apply only to a sub-set of solutions for the equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ in positive integers $a\leq b$, and $c\leq d$.

It follows that by "*Vertical Equivalence*" and in order for Equations 2.3 & 2.4 to be valid, then:

2.5) a=b; and c=d;

That is because the equations $(3^a-1)=(5^c-1)$, and $(3^b-1)=(5^d-1)$, have the same mathematical "structure", and are part of or were derived from the same equation which is $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$. ■

Theorem-3: Given The Differences In The Magnitudes Of The Bases Of Exponents On Both Sides Of The Equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ (ie. 3 versus 5), For The Equation To Be Valid, Then: a,b ≥ c,d; Which Implies That There Is More Than One Solution For The Equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$.

Proof:

3.1) $Ln[(3^a-1)(3^b-1)] = Ln[(5^c-1)(5^d-1)]$;

3.2) $Ln(3^a-1)+Ln(3^b-1) = Ln(5^c-1) + Ln(5^d-1)$;

As a,b,c,d →+∞ (and for relatively medium and large values of a,b,c and d):

$(3^a-1) \rightarrow 3^a$

$(3^b-1) \rightarrow 3^b$

$(5^c-1) \rightarrow 5^c$

$(5^d-1) \rightarrow 5^d$

3.3) So that: $[(3^a)(3^b)] = [(5^c)(5^d)]$;

3.4) $Ln[(3^a)(3^b)] = Ln[(5^c)(5^d)]$;

$Ln(3^a)+Ln(3^b) = Ln(5^c)+Ln(5^d)$

$aLn(3)+bLn(3) = cLn(5)+dLn(5)$

$(Ln3)(a+b) = (Ln5)(c+d)$

3.5) $(a+b)/(c+d) = Ln5/Ln3 = 1.47 \approx 1.5$

$(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ can be expressed as $(X^a-1)(X^b-1) = (Y^c-1)(Y^d-1)$

By Horizontal Equivalence above, and since X<Y, in positive integers, then a≤b, and c≤d, then:

3.6) $X^a=Y^c$, and thus a≥c.

3.7) $X^b=Y^d$; and thus b≥d.

Note that Eq.-3.6 and Eq.-3.7 apply to a sub-set of solutions for the equation $(X^a-1)(X^b-1) = (Y^c-1)(Y^d-1)$ in positive integers a≤b, and c≤d.

By "*Vertical Equivalence*", then:

3.8) a=b; and c=d; for most solutions to the equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$

Note that Eq.-3.8 applies only to a sub-set of solutions for the equations $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ and $(X^a-1)(X^b-1) = (Y^c-1)(Y^d-1)$ in positive integers a≤b, and c≤d.

Given that X<Y, and that in the equation $(X^a-1)(X^b-1) = (Y^c-1)(Y^d-1)$ in positive integers a≤b, and c≤d, both sides of the equation have the same or similar mathematical "structure", for the equation to be valid, it follows that:

3.9) a,b ≥ c,d.

The foregoing results, "conditions" and inequalities differ substantially from the Liptai, Németh, et. al. (2020) conjectures and result [(a,b,c,d) =(1,2,1,1)] which implies that there can be more than one solution for the equation $(3^a-1)(3^b-1)=(5^c-1)(5^d-1)$. ■

Theorem-4: The Liptai, Németh, et. al. (2020) Conjectures Are Wrong Because They Don't Satisfy The *Existence-1* Conditions; And There Are Infinitely Many Combinations Of "Qualifying" *a* And *c* (or *a,b,c* and *d*) Such That $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ Most Probably Has More Than One Solution.

Proof:

It's given that: a ≤ b, and c ≤ d. As explained herein and above, and by "*Horizontal Equivalence*":

4.1) $(3^a-1)=(5^c-1)$, and $3^a=5^c$

4.2) And simultaneously: $(3^b-1)=(5^d-1)$, and $3^b=5^d$

As explained above, and by "*Vertical Equivalence*", then:

4.3) a=b; and c=d;

As noted above, and given Theorem-3 above, and the differences between the bases (3 and 5 respectively) of the exponentials, for $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ to be valid:

4.4) a,b ≥ c,d

From *Equation-4.1*: $3^a=5^c$, and given that: $a \leq b$, and $c \leq d$, then if a,c = 0, then a,b,c,d = 0; and then: $(3^a-1)(3^a-1) = (5^c-1)(5^c-1)$; and thus, the Liptai, Németh, et. al. (2019) conjecture and result [ie. (a,b,c,d)=(1,2,1,1,)] don't apply to (a,b,c,d)=(0,0,0,0).

From Equation-4.1, $3^a=5^c$, and then:
4.5) $\text{Log}_3(5^c) = a = \text{Ln}(5^c)/\text{Ln}(3) = c\text{Ln}(5)/\text{Ln}(3) = c[\text{Ln}(5)/\text{Ln}(3)] = a = c1.465 \approx c1.5$
4.6) $\text{Log}_5(3^a) = c = \text{Ln}(3^a)/\text{Ln}(5) = a\text{Ln}(3)/\text{Ln}(5) = a[\text{Ln}(3)/\text{Ln}(5)] = c = a0.683 \approx a0.7$

From *Equation-4.1*, $3^a=5^c$, and it follows that the absolute number of possible (both "matching" and "incorrect") combinations of the positive integers $0< a,c <+\infty$ ($0< a, b, c, d < +\infty$) exceeds ten billion and may be as much as infinity. Because the numerical difference between 3 and 5 is not large (on a scale of zero to $+\infty$) then it follows that there is a high probability that there can be more than one combination of positive integers *a* and *c* ($0< a, b, c, d < +\infty$) that satisfy all the following conditions (the "*Existence-1 Conditions*") that make the equation and inequalities $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$, $a \leq b$ and $c \leq d$ valid:

4.7) a =b= c1.465 ($\approx$c1.5)
4.8) c =d $\approx$ a0.683 $\approx$ a0.7
4.9) $0< a,c < +\infty$; and $0< a,b,c,d < +\infty$ are integers
4.10) a=b; and c=d;
4.11) $a,b \geq c,d$;
4.12) $a \leq b$, and $c \leq d$;
4.13) $(3^a-1)(3^a-1) = (5^c-1)(5^c-1)$; and thus $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$.
4.14) $3^a=5^c$
4.15) $3^b=5^d$

Given the foregoing conditions, *a*, *b*, *c* and *d* can be calculated by iteration and or optimization.

It also follows that there are no upper bounds on *a*, *b*, *c* and *d*. Thus, the Liptai, Németh, et. al. (2020) proofs and conjecture are wrong and there is a high probability that there is more than one solution for the Diophantine equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$, where $a \leq b$, and $c \leq d$ are integers, because

i) the Liptai, Németh, et. al. (2020) result (a,b,c,d)=(1,2,1,1) doesn't satisfy all the "*Existence-1 Conditions*"; and
ii) the absolute number of possible (both "matching" and "incorrect") combinations of the two positive integers $0< a,c <+\infty$ ($0< a,b,c,d < +\infty$) exceeds ten billion and may be as much as infinity. ■

Theorem-5: The Liptai, Németh, et. al. (2020) Conjecture And Results Are Wrong And Don't Satisfy All The *Existence-2* Conditions; And There Are Infinitely Many Combinations Of "Qualifying" *a* And *c* (or *a,b,c* and *d*) Such That $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ Most Probably Has More Than One Solution; And For The Equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ To be Valid In Positive Integers $a\leq b$, and $c\leq d$ As Construed, Then:

i) **$(a+b)/(c+d) \geq 1$; And**
ii) **$a,b \geq c,d$;**
iii) **$b-a \geq d-c$;**

Proof:
$a \leq b$, and $c \leq d$
As explained herein and above, and by "*Horizontal Equivalence*":
$(3^a-1)(3^a-1) = (5^c-1)(5^c-1)$
If $(3^a-1) = (5^c-1)$, and $(3^b-1)=(5^d-1)$; then
5.1) $(3^a-1) = (5^c-1)$, and $3^a=5^c$
5.2) $(3^b-1) = (5^d-1)$, and $3^b=5^d$;

and by "*Vertical Equivalence*":
5.3) a=b; and c=d;
From **Theorem-3**:
5.4) $a,b \geq c,d$

Given "*Vertical Equivalence*" and the differences in the magnitudes of the integers on both sides of the equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ (ie. 3 versus 5):

5.6) $(3^a-1)(3^a-1) = (5^c-1)(5^c-1)$

Furthermore and as explained herein and above:
5.7) (a+b)/(c+d) = Ln5/Ln3 = 1.47≈ 1.5

If $(3^a-1)=(5^c-1)$, and $(3^b-1)=(5^d-1)$; then
$3^a=5^c$, and $3^b=5^d$; and thus by "vertical equivalence":
5.8) **b-a ≥ d-c;**
5.9) if b≥a, and d≥c; and a,b,c, and d are positive integers then b≥1 and d≥1.

Thus, the conditions for the validity of the equation and inequalities $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$, a ≤ b, and c ≤ d in positive integers (the "*Existence-2 Conditions*") are as follows:

5.10) (a+b)/(c+d) ≈ 1.5
5.11) $3^a=5^c$; and $3^b=5^d$;
5.12) $(3^a-1)(3^a-1) = (5^c-1)(5^c-1)$
5.13) 0< a,c < +∞; and 0< a,b,c,d < +∞ are positive integers
5.14) a=b; and c=d are positive integers
5.15) a,b ≥ c,d;
5.16) a ≤ b, and c ≤ d; are positive integers.
5.17) b-a ≥ d-c;
5.18) if b≥a, and d≥c; and a,b,c, and d are positive integers then b≥1 and d≥1.
5.19) That means that for each of *c* and *d* to be positive integers, they must be even numbers (and not odd numbers) which when multiplied by 1.5, produces another positive integer (there is no odd number which when multiplied by 1.5, produces a positive integer). The smallest such even number integer is 2.

It follows that the number of possible (both "matching" and "incorrect") combinations of positive integers 0<*a*,*c*<+∞ (0<*a*, b,*c*,*d*<+∞) that satisfy the equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ exceeds ten billion and may be as much as infinity. It also follows that there are no upper bounds on *a*, *b*, *c* and *d*. Because the Liptai, Németh, et. al. (2020) result (*a*,*b*,*c*,*d*)=(1,2,1,1) doesn't satisfy all the "*Existence-2 Conditions*", the Liptai, Németh, et. al. (2020) conjecture and proofs are wrong, and there is probably more than one solution for the Diophantine equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ where a ≤ b, and c ≤ d are positive integers. ■

Theorem-6: The Liptai, Németh, et. al. (2020) Conjecture And Result Satisfy All The *Existence-3* Conditions; But There Are Infinitely Many Combinations Of "Qualifying" *a* And *c* (or *a,b,c* and *d*) Such That $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ Most Probably Has More Than One Solution; And For The Equation $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$ To be Valid In Positive Integers a≤b, and c≤d As Construed, Then:

i) **(a+b)/(c+d) ≥1; And (a+b)/(c+d) =1.5**
ii) **c=d;**
iii) **a,b ≥ c,d;**
iv) **b-a ≥ d-c;**
v) $(3^a3^b)-3^a-3^b = (5^c5^d)-5^c-5^d$**;**
vi) **The Lower-Bound is (a,b,c,d)=(1,2,1,1).**

Proof:
6.1) $(3^a-1)(3^b-1) = (5^c-1)(5^d-1)$
6.2) $(3^a-1)(3^b-1) = (3^a3^b)-3^a-3^b+1$
6.3) $(5^c-1)(5^d-1) = (5^c5^d)-5^c-5^d+1$
6.4) Thus: $(3^a3^b)-3^a-3^b+1 = (5^c5^d)-5^c-5^d+1$
6.5) $(3^a3^b)-3^a-3^b = (5^c5^d)-5^c-5^d$
6.6) $3^{(a+b)}-3^a-3^b = 5^{(c+d)}-5^c-5^d$

6.7) $3^{(a+b)}$- $5^{(c+d)}$= 3^a+3^b- 5^c-5^d
Thus, (a+b)/(c+d)>1; and
a,b ≥ c,d
As noted above, c=d.

Since a,b,c and d are positive integers, in order for the inequalities b≥a and c≥d to be valid, then b≥1 and d≥1, a≥1 and c≥1 and since c=d, then: c,d ≥1.
If c,d = 1, then (a+b) = 3.
By trying a = 1 or 2 and b = 1 or 2, and substituting in the equation $(3^a−1)(3^b−1) = (5^c−1)(5^d−1)$, **the lower bound is (a,b,c,d) = (1,2,1,1).**

Alternatively (and without proving that c=d), if d=1 and c=1, and since (a+b) = (1.5c+1.5d), then (a+b) = 3. By trying a = 1 or 2 and b = 1 or 2, and substituting in the equation $(3^a−1)(3^b−1) = (5^c−1)(5^d−1)$, **the lower bound is (a,b,c,d) = (1,2,1,1).**

The *Existence-3* Conditions Are as follows:

i) (a+b)/(c+d) ≥1; And (a+b)/(c+d) =1.5
ii) c=d;
iii) a,b ≥ c,d;
iv) b-a ≥ d-c;
v) (3^a3^b)-3^a-3^b = (5^c5^d)-5^c-5^d

■

Theorem-7: There Is More Than Solution For The Equation $(3^a−1)(3^b−1) = (5^c−1)(5^d−1)$ In Positive Integers And In Positive Real Numbers.
Proof:
7.1) $(3^a−1)(3^b−1) = (5^c−1)(5^d−1)$ can be expressed as $(X^a−1)(X^b−1) = (Y^c−1)(Y^d−1)$, which is:
7.2) $[X^aX^b-X^b-X^a+1]=[Y^cY^d-Y^c-Y^d+1]$
7.3) $[X^{(a+b)}-X^b-X^a]=[Y^{(c+d)}-Y^c-Y^d]$
7.4) $[X^{(a+b)}-Y^{(c+d)}-X^b-X^a+Y^c+Y^d]=0$. If "similar" terms are matched in this Eq-7.4 (ie. matched with regards to opposite-signs, LHS/RHS of Eq.-7.1, and the structures of the variables), this equation supports the position that $X^a=Y^c$ and $X^b=Y^d$ and $X^{(a+b)}=Y^{(c+d)}$; which is a *necessary condition* for validity of Eq.-7.4. This Matching processes and equivalency is henceforth referred to as the "*Matching Reduction*" of an equation.

If $X^a=Y^c$ and $X^b=Y^d$, and $X^{(a+b)}=Y^{(c+d)}$, then:
7.5) $[X^{(a+b)}-Y^{(c+d)}-X^b-X^a+Y^c+Y^d]=0$.

There are potentially and infinitely many combinations of $X^{(a+b)}$ and $Y^{(c+d)}$ in positive integers that make the equation $X^{(a+b)}-Y^{(c+d)}=0$ valid. There are potentially and infinitely many combinations of X, Y, *a*, *b*, *c* and *d* that make the equations $X^a=Y^c$ and $X^b=Y^d$ valid. Thus its highly probable that there is more than one solution for the equation $(3^a−1)(3^b−1) = (5^c−1)(5^d−1)$.

■

<u>Conclusion.</u>
Contrary to Liptai, Németh, et. al. (2020) the diophantine equation $(3^{x1}−1)(3^{x2}−1)=(5^{y1}−1)(5^{y2}−1)$ in positive integers $x1≤x2$, and $y1≤y2$, can have more than one solution where $x1$, $x2$, $y1$ and $y2$ are integers and $x1≤x2$, and $y1≤y2$.

Bibliography.

Bertok, L., Hajdu, F., et. al. (2017). On the number of non-zero digits of integers in multi-base representations. *Publicationes Math Debrecen*, 90, 181–194.

Chu, M. (2008). Linear algebra algorithms as dynamical systems. *Acta Numerica*, 17, 1-86.

Ding, J., Kudo, M., et. al. (2018). Cryptanalysis of a public key cryptosystem based on Diophantine equations via weighted LLL reduction. *Japan Journal of Industrial and Applied Mathematics*, 35, 1123–1152.

Ibarra, O. & Dang, Z. (2006). On the solvability of a class of diophantine equations and applications. *Theoretical Computer Science*, 352(1–3), 342-346.

Jones, J. P., Sato, D., et. al. (1976). Diophantine Representation of the Set of Prime Numbers. *American Mathematical Monthly*, 83, 449-464.

Liptai, K., Németh, L., Soydan, G. & Szalay, L. (2020). *Resolution of the equation* $(3^{x1}-1)(3^{x2}-1)=(5^{y1}-1)(5^{y2}-1)$. *Rocky Mountain Journal of Mathematics*, in press. https://arxiv.org/abs/2001.09717.

Luca, F., Moree, P., & Weger, de, B. M. M. (2011). Some Diophantine equations from finite group theory: $\Phi_m (x) = 2p^n -1$. *Publicationes Mathematicae* (Institutum Mathematicum Universitatis Debreceniensis), 78(2), 377-392.

Matijasevič, Y. (1981). Primes are nonnegative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, _________.

Matveev, E. (2000). An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64 (2000), 125–180. English translation in *Izvestia Mathematics*, 64, 1217–1269.

Nemron, I. (2008). An original abstract over the twin primes, the Goldbach conjecture, the friendly numbers, the perfect numbers, the Mersenne composite numbers, and the Sophie Germain primes. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(6), 715-726.

Ogura, N. (2012). *On Multivariate Public-key Cryptosystems*. PhD thesis, Tokyo Metropolitan University (2012).

Okumura, S. A (2015). Public key cryptosystem based on diophantine equations of degree increasing type. *Pacific Journal of Industrial Mathematics*, 7(4), 33–45.

Schlickewei, H. & Schmidt, W. (1993). Linear equations in members of recurrence sequences. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze*, 20, 219–246.

Stewart, C. (1980). On the representation of an integer in two different bases. *Journal fur die reine und angewandte Mathematik*, 319, 63–72.

Wang, L. & Chin, C. (2012). Some property-preserving homomorphisms. *Journal of Discrete Mathematical Sciences and Cryptography*, 15(2-3).

Zadeh, S. (2019). Diophantine equations for analytic functions. *Online Journal of Analytic Combinatorics*, 14, 1-7.