

A bit of modification on the forms of the weird numbers with an application on cryptosystem

Saja A. Abdulkarim *

Department of Mathematics

College of Education for Pure Sciences

University of Babylon

Babylon

Iraq

Faez A. Al-Maamori [†]

Department of Mathematics

Faculty of Information Technology

University of Babylon

Babylon

Iraq

Abstract

This research aims to generate primitive weird numbers using mathematical and programming methods. The n function was used to create these numbers within a specific range where p and q are primes, $b > a > 2$ also $K \geq 1$. Programming was implemented in Python to generate these numbers. A function $G(x)$ for generating prime numbers was also used, modified to create weird numbers, and implemented programmatically. The findings of this research have been verified through previous research, and finally, tables and graphs of the resulting numbers were plotted.

Furthermore, Number theory is regarded as the core of cryptosystem science, where there are several distributions of various types in the sequence of the natural numbers. This work concentrated on finding a bit of enhancement of the general form of the wired numbers in order to use them in cryptosystem work.

Subject Classification: Primary 11A25, Secondary 94A60.

Keywords: Weird numbers, Primitive weird numbers, RSA cryptosystem.

* E-mail: pure218.sja.ali@student.uobabylon.edu.iq (Corresponding Author)

[†] E-mail: faez@itnet.uobabylon.edu.iq

1. Introduction

The field of number theory possesses a rich and extensive historical background within the realm of mathematics. In fact, its various challenges and theoretical constructs have significantly influenced numerous domains of mathematical inquiry. Even in contemporary times, it remains a dynamic and integral segment of modern mathematical discourse. Number theory deals with the field of numbers and their characteristics, including the study of numbers and the relationships between them and other mathematical operations like abundant, deficient and weird numbers WN [1].

Prime numbers played a crucial role in the encryption process, where a prime number is known as a number that is biggest than one which is not divisible only by 1 and itself [1-2].

Let $n \in N^+$ where N^+ is the set of Natural numbers, and let $\sigma(n) = \sum_{d|n} d$ be the sum of total divisors of n , and we defined its abundance, which is symbolized by $\Delta(n) = A(n) = A\sigma$ so that $\Delta(n) = \sigma(n) - 2n$, then n is called perfect if $\Delta(n) = 0$ abundant if $\Delta(n) > 0$ and deficient if $\Delta(n) < 0$. We further define n to be semiperfect if n represents the unique summation of certain proper divisors of n . A positive n is defined as a primitive abundant number PAN if it satisfies two conditions. First, it must be abundant A ; second, it must be primitive in that all its proper divisors must be deficient numbers [3-5].

A WN n is an AN , but not semiperfect number, and also can be expressed as a number which is multiplied by a prime number PN such that $P > \sigma(n)$ while a primitive weird number PWN is one that is not a multiple of a smaller WN [7].

Based on that, this research will also discuss the use of WN as part of the encryption process within the RSA algorithm. The algorithm relies on generating PN to produce public and private encryption keys. WN contributes to the computational complexity of the process, such that the WN w is used as a base in the encryption process [8].

This work aims to introduce a bit of enhancement of the general form of the PWN that is, to show for any n that is a PWN , hence, there exists a and $b \in N$ for which $b > a > 2$ then $n = 2^k(2^k + a)(2^k + b)$, then to prove it and generate a PWN from it. Also, to generate the WN by $G(x)$ function, and compare them by using curves. Also, to use a WN w as a part of the encryption process.

2. Main results

Lemma 2.0.1: $\Delta(n)$ cannot be represented as a summation of the divisors of n if and only if n is classified as an abundant number, this consequently implies that n is categorized as a weird number [6].

The following proposition is an enhancing of theorems [9].

Proposition 2.1: Let $K \geq 1$, where $k \in Z^+$ and let a and b be both positive odd integers such that $(2^k + a)$ and $(2^k + b)$ are primes. If $b > a > 2$ and $p < q$ then $n = 2^k(2^k + a)(2^k + b)$ is a PWN .

Proof: Let $n = 2^k pq$ where $(2^k + a)$ and $(2^k + b)$ be two primes with a and b being a positive odd integer such that $b > a > 2$. Let $n = 2^k(2^k + a)(2^k + b)$, we will prove that n is *PWN* in three stages, in the first stage, we will prove that n is *A*, then in the second stage, prove that n is *PAN*, and in the last step, we rely on Lemma to ensure reliability, we rely on it when proving. First, proof that it is abundant. We have

$$\begin{aligned}\Delta(n) &= \sigma(n) - 2n = \sigma(2^k pq) - 2(2^k pq) = \sigma(2^k)\Delta(p)\Delta(q) - 2^{k+1}pq \\ &= (2^{k+1} - 1)(p + 1)(q + 1) - 2^{k+1}pq \\ &= 2^{2k+2} + 2^{k+1}(a + b) + 2^{k+1} - 2^{2k} - 2^k(a + b) - 2^{k+1} \\ &\quad - (ab + a + b + 1) \\ &= 2^{2k+2} - 2^{2k} + 2^{k+1}(a + b) - 2^k(a + b) \\ &\quad - (ab + a + b + 1) = 3 \cdot 2^{2k} + 2^k(a + b) - (a + 1)(b + 1)\end{aligned}$$

since $K \geq 1$ and a and b are both positive integers, then the term $3 \cdot 2^{2k} + 2^k(a + b)$ is a large term, while $(a + 1)(b + 1)$ is a relatively small negative term, then that implies that $\Delta(n) > 0$ will be an *AN*. Second, we have to show that n is a *PAN*. We have to prove that $\max\left\{\Delta\left(\frac{n}{p}\right), \Delta\left(\frac{n}{q}\right), \Delta\left(\frac{n}{2}\right)\right\} < 0$

we have

$$\begin{aligned}\Delta\left(\frac{n}{p}\right) &= \Delta\left(\frac{2^k pq}{p}\right) = \Delta(2^k q) = 2^k - b - 1 < 0 \\ \Delta\left(\frac{n}{q}\right) &= \Delta\left(\frac{2^k pq}{q}\right) = \Delta(2^k p) = 2^k - a - 1 < 0 \\ \Delta\left(\frac{n}{2}\right) &= \Delta\left(\frac{2^k pq}{2}\right) = \Delta(2^{k-1}pq) = 2^{2k} - 2^k - (a + b + ab + 1) < 0\end{aligned}$$

Since n is an *A* and each it non-trivial divisors are deficient, consequently n is *PAN*, now to complete that n is *W* it must achieved that n is not semiperfect. The ascending arrangement of proper factors of n commences with $1, 2, 2^2, 2^3, \dots, 2^k \cdot p, 2p, \dots, 2^k p, q, 2q, \dots, 2^k q, pq, 2pq, \dots, 2^{k-1}pq$.

We may signified this set by $A_n = \{d|n: 0 < d < n\}$ is the proper divisors of n , which are the positive divisors of n that is less than n . From the condition of abundance, we have $\Delta(n) = \sigma(2^k)\sigma(p)\sigma(q) - 2^{k+1}pq$ then $\sigma(2^k) = 2^{k+1} - 1$ we will use it and give the symbol B for it hence $= 2^{k+1} - 1$, and we have $\Delta(n) = A(n) = A$, so that $A = B(p + 1)(q + 1) - (B + 1) = B + Bp + Bq - pq$ since n is abundant, we have $A + pq = B + Bp + Bq$ this is equal to $(p - B)(q - B) = B(B + 1) - A(1)$

we complete the proof with show that $A > B$ and $B < p < 2B$

Now, if $\leq B$, we would have $A = \sum_{j \in J} 2^j$ for some $J \subset \{0, 1, \dots, k\}$, whence $A \in \sum A_n$. Similarly if $p \leq B$ The state explains that if $p \leq B$ this would make the number n semiperfect which contradicts the basic hypothesis that n is weird Therefore, p must be $> B$ and $p = \sum_{j \in J} 2^j$ for some $J \subset \{0, \dots, k\}$,

$$n = 2^k pq = (2^k - 1)pq + pq = \sum_{j=0}^{k-1} 2^j pq + pq = \sum_{j=0}^{k-1} 2^{2j} q + \sum_{j \in J} 2^j q$$

If $p \leq B$, then n can be represented as the sum of two separate sets of its integer factors. This means that n is a semiperfect, and This conclusion (that n is semiperfect) contradicts with hypothesis that n is W , therefore not semiperfect. Since we assume first that $p < q$ then

$$p < q \rightarrow p - B < q - B \rightarrow (p - B)(p - B) < (q - B)(p - B) \rightarrow (p - B)^2 < B(B + 1) - A \text{ From 1 we get}$$

$$(p - B) < \sqrt{B(B + 1) - A} \quad (2)$$

and $A > B \rightarrow -A < -B \rightarrow B(B + 1) - A < B(B + 1) - B \rightarrow$ we get

$$\sqrt{B(B + 1) - A} < B \quad (3)$$

then, by combining (2) and (3) we get $p - B < \sqrt{B(B + 1) - A} < B$. Then $p - B < B$ Whence $p < 2B$ by $(p - B)(q - B) = B(B + 1) - A$ and $A > B$ we have $4 \mid A$ and $B < A < B(B + 1)$, since n is weird and $pq \neq s + rp + tq$ for all positive integers s, r and $t \leq B$ then it follows that $A \notin \sum A_n$, hence n is weird.

3. Practical Application

3.1 Practical Application of $n = 2^k pq$

The curve and table illustrate the progression of PWN , highlighting the unpredictable increase in their values. PWN increase in an irregular manner. The *horizontal axis* represents the order of the number, while the *vertical axis* is the value of the number.

To clarify the results shown in Figure 1, as shown in Table 1.

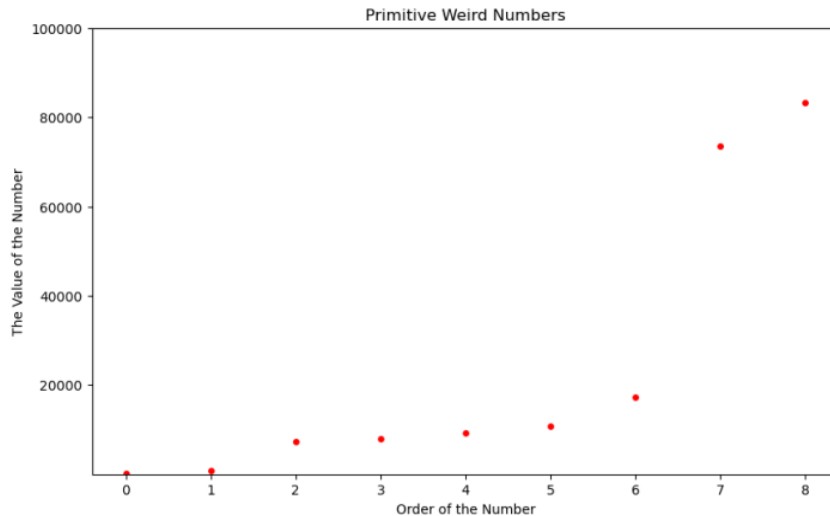


Figure 1
Primitive weird number less than 100000

Table 1
Primitive weird number less than 100000

k	p	q	n	k	p	q	n	k	p	q	n
1	5	7	70	3	23	43	7912	3	17	127	17272
2	11	19	836	3	19	61	9272	4	43	107	73616
3	29	31	7192	3	19	71	10792	4	41	127	83312

The results for the function were in complete agreement with what is published in the relevant scientific literature [9-10].

3.2 *Weird numbers by $G(x)$*

In this subsection, we present the theoretical framework for generating WN from $G(x)$. We developed it to generate WN by using real numbers. It also aims to expand the mathematical understanding of weird numbers by providing a new method for generating them, thus enhancing their potential applications in number theory. In this section, from another angle, we present a numerical example to illustrate how the function works and how these numbers are generated. A WN is defined as an abundant but not semiperfect. We will generate these numbers in Figure 2. First, we need to define the Mobius function $\mu(n)$.

3.2.1 Mobius function $\mu(n)$ [1], [6]

The function $\mu(n)$ is defined as follows

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n \text{ has a square factor for some prime } p \\ -1^k, & \text{if } n \text{ can be expressed as a product of } k \text{ distinct primes.} \end{cases}$$

3.2.2 Proposition [3]

Let $G(x) = \chi'(\theta)\theta$ therefore,

$$G(x) = \chi'(\theta) \left(\sum_{n=1}^{\infty} \mu(n) \left(\left[x^{\frac{1}{n}} \right] - 1 \right) \right), x \geq 1$$

$$\chi'(\theta) = \begin{cases} 1, & \text{if } \theta \text{ is prime} \\ 0, & \text{if } \theta \text{ is not prime} \end{cases}$$

We will develop $G(x)$ by substituting the real numbers in x . Therefore, it will give us the WN with a condition:

$$\chi'(\theta) = \begin{cases} 1, & \text{if } \theta \text{ is weird} \\ 0, & \text{if } \theta \text{ is not weird} \end{cases}$$

3.2.3 Numerical Example of $G(x)$ $G(x) = \chi'(\theta)\theta$

$$G(82.2) = \chi'(\theta) \left(\sum_{n=1}^{\infty} \mu(82.2) \left(\left[82.2^{\frac{1}{n}} \right] - 1 \right) \right)$$

$$\begin{aligned}
&= \chi'(\theta) \left(\left(\mu(1) \left[82.2^{\frac{1}{1}} \right] - 1 \right) + \left(\mu(2) \left[82.2^{\frac{1}{2}} \right] - 1 \right) + \left(\mu(3) \left[82.2^{\frac{1}{3}} \right] - 1 \right) \right. \\
&\quad + \left(\mu(4) \left[82.2^{\frac{1}{4}} \right] - 1 \right) + \left(\mu(5) \left[82.2^{\frac{1}{5}} \right] - 1 \right) \\
&\quad \left. + \left(\mu(6) \left[82.2^{\frac{1}{6}} \right] - 1 \right) + \left(\mu(7) \left[82.2^{\frac{1}{7}} \right] - 1 \right) + \dots \right) \\
&= \chi'(\theta)(70) = 70
\end{aligned}$$

Since 70 is weird the $\chi'(\theta) = 1$

3.3 Practical Application of $G(x)$

Below is a figure and table 100000 that was generated by the cap G open paren x close paren function, where x is a real number, the input number, and $G(x)$ is the output weird number. Furthermore, by applying this proposed function to the numbers, it was found that these numbers perfectly match the WN established in previous research, as shown in Table 2 [11].

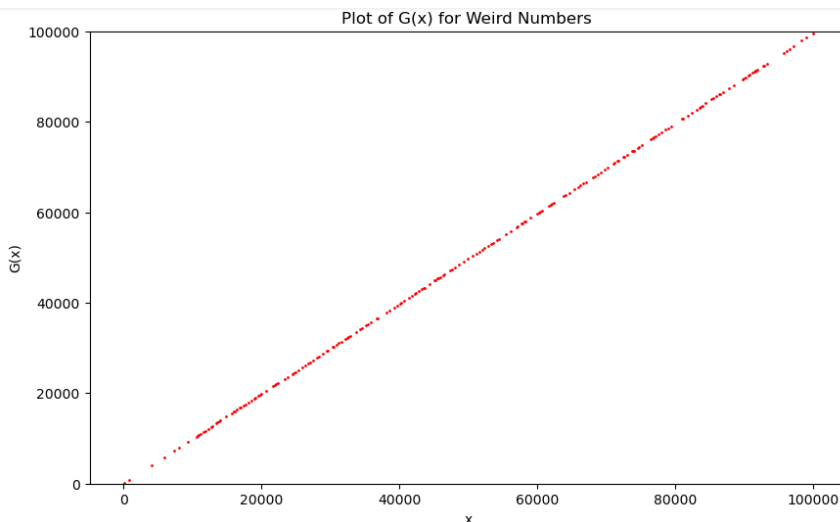


Figure 2

Weird number less than 100000

Table 2

Weird number less than 100000

x	$G(x)$	x	$G(x)$	x	$G(x)$	x	$G(x)$
82	70	27429	27230	49892	49630	73931	73616
874	836	27991	27790	50593	50330	74588	74270
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
26726	26530	48629	48370	73745	73430	99976	99610
27008	26810	49331	49070	73885	73570	100257	99890

4. The weird numbers in RSA Algorithms [1], [10-11]

In this research, the RSA encryption algorithm was modified by using WN as the basis for key generation. Real numbers were substituted into the WN generation function, resulting in an WN . Using the (F.T.A.) fundamental theorem of arithmetic which states that $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_k^{a_k}$ for $p_1, p_2, \dots, p_k$ are the k distinct prime factors of n and $a_i \geq 1$ also $n \geq 2$, therefore the WN was factored into its prime factors, specifically the two highest primes. These higher primes were then used to generate the next prime factor, $f(x)$, thus yielding p and q . The larger the WN , the larger the resulting primes, increasing the complexity and security of the algorithm. This allowed for the extraction of the value of n . A random factor, k , was also added to enhance the algorithm's security further. Then the methodology used in the traditional algorithm was then followed. The modification of the algorithm also altered the public and private keys, making the public key publicly available. This made decryption difficult for those who lacked the WN function and the methodology for finding the prime number. Finally, the encryption and decryption equations were modified to become

$$C = M^e \pmod{n} \times K \pmod{n}$$

$$M = (C \times k^{\{-1\}})^d \pmod{n}$$

4.1 The basic process of RSA algorithm

- Choose a real number and substitute it in $G(x)$ to result in a WN w .
- Then we factorize W into its prime numbers by using F.T.A. and choose the largest prime numbers.
- Use these numbers in the function $f(x) = \text{next prime}(W \times W_{p_i})$ to result p and another time to result q .
- Choose these two distinct prime numbers. p and q such that $p \neq q$ and $p, q \in P$.
- Calculate n which is required when we take module, where n is the product of the two selected prime number $n = pq$.
- Choose a haphazard k such that $\gcd(e, n) = 1$.
- Calculate the phi function $\Phi(n)$, which it $\Phi(n) = (p - 1)(q - 1)$.
- Choose the public key e which should holding $1 < e < \Phi(n)$ for which $\gcd(e, \Phi(n)) = 1$.
- Compute the private d from the following equation $d \equiv e^{-1} \pmod{\Phi(n)}$.
- Create the pair $(G(x), e, k)$ which is often called the public key which will be used for encryption and $(G(x), d, k^{-1})$ the private key for decryption.

Now we have described the encryption and decryption of the algorithm.

- Encryption phase of the RSA cryptosystem:
 - Input parameters: The public key $(G(x), e, k)$ and the plaintext message M .

- Output result: The cyphertext C .
- The message represented as an integer $M < n$.
- Compute $C = M^e \pmod{n} \times K \pmod{n}$.
- Gives C .
- Decryption phase of the RSA cryptosystem:
 - Input parameter: The private key $(G(x), d, k^{-1})$ and the cyphertext c .
 - Output result: The plaintext message M .
 - Compute $M = (C \times k^{-1})^d \pmod{n}$.
 - Return M .

The following Example shows the practical implementation of RSA algorithm where the Result illustrated in Table 3.

4.2 Numerical Example

$G(82.2) = w = 70$ From 4.2.3 or From Table 3

$$w = 2 * 5 * 7$$

$$p = f(w, p_i) = \text{Next prime}(w * p_i) = \text{Next prime}(70 * 5) \\ = \text{Next prime}(350) = 353$$

$$q = f(w, q_i) = \text{Next prime}(w * q_i) = \text{Next prime}(70 * 7) = 491$$

$$n = p * q = 353 * 491 = 173323 \text{ and } \Phi(n) = (353 - 1)(491 - 1) \\ = 172480$$

$$\text{Public encryption key} = \{G(X), e, K\} = \{G(82.2), 3, 5\}$$

$$\text{Private key} = \{G(x), d, K^{-1}\} = \{G(82.2), 114987, 103994\}$$

$$\text{Encryption } C = M^e \pmod{n} \times K \pmod{n} \\ = 100^3 \pmod{173323} \times 5 \pmod{173323} = 146956$$

$$\text{Decryption } M = (C \times k^{-1})^d \pmod{n} \\ = (146956 \times 5^{-1})^{114987} \pmod{173323} = 100$$

Table 3

Table to illustrate the results

$G(82.2)$	p	q	n	$\{G(X), e, K\}$	$\{G(x), d, K^{-1}\}$	C	M
70	353	491	172480	$\{G(82.2), 3, 5\}$	$\{G(82.2), 114987, 103994\}$	146956	100

5. Discussion and Conclusion

This research studied a function for generating PWN , it has been proven within the research, and another function was developed to generate WN . Both were then applied practically, and finally, the developed function of generating weird numbers were used in the RSA encryption algorithm as base for generating the keys. Furthermore, traditional RSA is a cryptographic system whose security relies on a clear mathematical assumption, the difficulty of factoring the number n into primes. This research proposed a modification that demonstrates the potential to enhance RSA security by hiding the n operator behind a secret function, $G(x)$, thus reducing the information available to an

attacker. However, introducing this layer increases the computational burden compared to traditional *RSA*. Nevertheless, the increased generation time contributes to greater system resistance to attacks, thereby strengthening security. In future work, the adoption of the proposal requires security proof within the framework of threat models used in cryptography.

References

- [1] S. Agarwal and A. S. Uniyal, "Number Theoretic Functions: Augmentation & Analytical Results," *International Journal of Mathematics Trends and Technology*, vol. 43, no. 3, pp. 232–233 (2017), doi: 10.14445/22315373/IJMTT-V43P527.
- [2] F. A. AL-Maamori, *Theory and Examples of Generalized Prime Systems*, Ph.D. thesis, Dept. of Mathematics and Statistics, University of Reading, Reading, UK, Mar., pp. 146 (2013).
- [3] G. Amato, M. F. Hasler, G. Melfi, and M. Parton, "Primitive abundant and weird numbers with many prime factors," *J. Number Theory*, vol. 201, pp. 436–459 (2019), doi: 10.1016/j.jnt.2019.02.027.
- [4] P. Athukorala, M. Chathurangi, and R. Ranasinghe, "A variant of *RSA* using continued fractions," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 1, pp. 127–134 (2022), doi: 10.1080/09720529.2021.1968574.
- [5] H. A. Hussein and F. A. Al-Maamori, "On using of weird number sequence in counting Beurling prime systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 5, pp. 1695–1704 (2024), doi: 10.47974/JDM-SC-2011.
- [6] G. Amato, M. F. Hasler, G. Melfi, and M. Parton, "Primitive weird numbers having more than three distinct prime factors," *Rivista di Matematica della Università di Parma*, vol. 7, no. 1, pp. 153–163 (2018).
- [7] S. J. Benkoski and P. Erdős, "On weird and pseudoperfect numbers," *Math. Comput.*, vol. 28, no. 126, pp. 617–623 (1974), doi: 10.1090/S0025-5718-1974-0347726-9.
- [8] A. Hassan, Z. I. Illo, A. U. Dakingari, N. J. Mallam, U. Aliyu, and A. Umar, "An insight to *RSA* algorithm," *HCDC International Journal of Multidisciplinary Research (HCDC-IJMR)*, vol. 1, no. 02, pp. 1–10 (2025).

- [9] G. Melfi, "On the conditional infiniteness of primitive weird numbers," *J. Number Theory*, vol. 147, pp. 508–514 (2014), doi: 10.1016/j.jnt.2014.07.024.
- [10] A. Nitaj, "The mathematical cryptography of the RSA cryptosystem," in *Cryptography: Protocols, Design and Applications*, K. Lek and N. Rajapakse, Eds., New York, USA: Nova Science Publishers, Inc, pp. 159–186 (2010).
- [11] N. J. A. Sloane, "Sequence A006037: Weird numbers: abundant but not pseudoperfect," *The On-Line Encyclopedia of Integer Sequences* (2026). [Online]. Available: OEIS A006037 (accessed May 22, 2026).

Received January, 2026