Integer Factorization By Sieving The Delta

Vishal Mudgal *

1 Abstract

Let $n = p \times q$ ($p < q$) and $\Delta = |p - q|$, where p, q are odd integers, then, it is hypothesized that factorizing this composite n will take O(1) time once the steady state value is reached for any Δ in $zone_0$ of some observation deck (od) with specific dial settings. We also introduce a new factorization approach by looking for Δ in different Δ sieve zones. Once Δ is found and n is already given, one can easily find the factors of this composite n from any one of the following quadratic equations: $p^2 + p\Delta - n = 0$ or $q^2 - q\Delta - n = 0$. The new factorization approach does not rely on congruence of squares or any special properties of n, p or q and is only based on sieving the Δ. In addition, some other new factorization approaches are also discussed. Finally, a new trapdoor function is presented which is leveraged to encrypt and decrypt a message with different keys.

Contents

*17 Simei Street 4, Double Bay Residences, Singapore-529881. Email: vishal.mudgal@deltasieve.org

2 Introduction

If $n = p \times q$ where p, q are some large primes, then no non-quantum algorithm exists today that can either find p or q in polynomial time when only n is given. This problem of factorizing the product of two large primes has kept great minds busy for quite some time, especially since 1977, when Rivest-Shamir-Adleman [1] leveraged this problem in building a public-key cryptosystem, famously known as RSA, that is widely used for secure data transmission. However, in 1994, Peter Shor [2] published an algorithm that can solve the integer factorization problem in polynomial time by using a universal quantum computer. When in future, a large ideal universal quantum computer with enough qubits is able to operate efficiently, then RSA scheme will no longer remain secure. Two key ideas have remained centerstage when attempting to solve the factorization problem. Variety of different methods and approaches have been developed around these two central ideas.

1. **Congruence of squares method**
In the 17th century, Pierre de Fermat [3] applied the difference-of-squares method to factorization. The idea is to represent an odd integer as the difference of two squares, i.e. $n = a^2 - b^2$. If neither factor equals one, then n can be factored as $(a + b)(a - b)$. This method works well when the two factors are close to each other but in worst case, this method can be far worse than trial division. However, this idea was further expanded by Maurice B. Kraitchik in the 1920s, who reasoned that instead of finding two integers a and b, such that, $n = a^2 - b^2$, it is sufficient to find two integers a and b with $a^2 - b^2$ equal to multiple of n, i.e. $a^2 \equiv b^2 \pmod{n}$ and $a \not\equiv \pm b \pmod{n}$. The idea of factorization by congruence of squares was born. Most general-purpose factorization algorithms are based on this idea.

Continued fraction factorization (CFRAC) by Derrick H. Lehmer and Ralph E. Powers [4] and implemented as a computer algorithm by Michael A. Morrison and John Brillhart [5], Square forms factorization by Daniel Shanks [6]. Linear sieve by Richard C. Schroeppel [7]. Random squares method by John D. Dixon [8]. Quadratic sieve by Carl B. Pomerance [9]. The multiple polynomial quadratic sieve by Robert D. Silverman [10]. The special number field sieve by John M. Pollard, and even though this is a special purpose factorization method, it laid the foundations for the general number field sieve (GNFS), making GNFS the fastest non-quantum algorithm. The details of how Pollard's original idea, which was suited for numbers of special form was extended to be applied to any number in general, is described in the book titled "The development of the number field sieve" [11]. Finally, some Lattice based factorization methods have also been explored by many researchers to solve the factorization problem.

The aforementioned factorization methods may use many other different ideas and concepts from analytical number theory, analytical algebraic theory or other areas of mathematics, however, achieving congruence of squares remains a key underlying goal to find the nontrivial factors of the semiprime n.

2. **Special properties of semiprime or any one of its unknown factors**
Numbers come in different size and form and sometimes this size and form have special properties, which is leveraged for factorization. Pollard's rho algorithm by John M. Pollard [12] is useful when number to be factored has small factors and Pollard's $p-1$ algorithm, again by John M. Pollard [13] is used when the number preceding one of the factors, p-1, is powersmooth. Williams's $p+1$ algorithm by Hugh C. Williams [14] is used in scenarios when the number to be factored contains one or more prime factors p such that $p+1$ is smooth, i.e. $p+1$ only contains small factors and Elliptic-curve factorization method (ECM) by Hendrik W. Lenstra Jr. [15] is most suitable for finding small factors not exceeding 50 to 60 digits.

There are many other different and creative ideas that have been applied to factorization, but the above two approaches have remained the front-runners for many years. A lot of research has already been carried out around these two key ideas and while a lot more is still left to be discovered, we thought to experiment with a different underlying approach. After a lot of failed experiments and toying with new structures, the inspiration came from nature and especially from the principle of flow of energy. For energy to flow between any two points, a difference of some sorts is required between these points - potential difference, gravitational difference, pressure difference etc. Applying this newly found inspiration to factorization, where, $n = p \times q$ and p, q are some large primes, the only reasonable potential/gravitational/pressure difference equivalent was observed in:

$$\Delta = |p - q| \tag{1}$$

And we embarked on a long but beautiful journey to comprehend this esoteric "Δ". With only n given as an input, it is quite fascinating to observe this property of numbers where one can make the Δ appear by only performing fundamental arithmetic operations. Along the way, this also led us to launch a systemic study of:

$$\sum = p + q \tag{2}$$

Leading us to find the beautiful equilibrium between the two and laid the foundations for a new trapdoor function that can be used in encryption and decryption of data and also opened up another factorization avenue at the same time.

$$\Delta \rightleftharpoons \sum \tag{3}$$

We could not find any literature in the public domain where the ideas and observations presented in this paper have been applied to factorization or for encryption/decryption of data, as we also found a new trapdoor function. We spent a lot of time in finding any prior work having similarities with our research and findings, but to the best of our efforts, we couldn't find anything.

We present our findings focussed on this $\Delta_{|p-q|}$, $\sum_{p+q}$ and $\Delta_{|p-q|} \rightleftharpoons \sum_{p+q}$, and some other insights that we think we have been blessed with during the coarse of this journey.

3 Notation and setup

$\Delta = |p - q|$: difference between any two integers and it's resultant absolute value
$p = 2k + 1$ or $p = 2k$ for $k \in \mathbb{N}$
$q = p + \Delta$
$n = p \times q$
$\lfloor\sqrt{n}\rfloor$: the floor function of n
$\Delta_{|p-q|}$: delta series (all combinations of p and q with respective $|p - q|$ value)
$\sum_{p+q}$: sum series (all combinations of p and q with respective $p + q$ value)
$\Delta_{|p-q|} \rightleftharpoons \sum_{p+q}$: equilibrium state between delta and sum series
$dial_1$: relative distance from $\lfloor\sqrt{n}\rfloor$:

$$dial_1 = \begin{cases} a_1 \in \mathbb{Z}_0 & \text{for } \lfloor\sqrt{n}\rfloor = 2k,\ k \in \mathbb{N} & \text{(4a)} \\ a_2 \in \mathbb{Z}_0 & \text{for } \lfloor\sqrt{n}\rfloor = 2k+1,\ k \in \mathbb{N} & \text{(4b)} \end{cases}$$

$dial_2$: relative distance from $\lfloor\sqrt{n}\rfloor + dial_1$ (or d_1):

$$dial_2 = \begin{cases} v_1 \in \mathbb{Z} & \text{for } \lfloor\sqrt{n}\rfloor + dial_1 = 2k,\ k \in \mathbb{N} & \text{(5a)} \\ v_2 \in \mathbb{Z} & \text{for } \lfloor\sqrt{n}\rfloor + dial_1 = 2k+1,\ k \in \mathbb{N} & \text{(5b)} \end{cases}$$

$dial_P$: dial pair and represented as $\{dial_1, dial_2\}$

$dial\ settings$: can be represented in any of the below formats:

1. As a dial pair. i.e. $dial_P = \{dial_1, dial_2\} = \{a_1, a_2, v_1, v_2\}$
2. As a matrix:

a_1	a_2
v_1	v_2

$d_1 = \lfloor\sqrt{n}\rfloor + dial_1$
$d_2 = d_1 + dial_2$
od: observation deck. Different observation decks will be referred with a numerical subscript value

$od_1 = d_1^2 - n$

$od_2 = d_2^2 - n$

$od_3 = od_2 - od_1$
$od_4 = od_1 + od_2$
$od_5 = od_1 + od_2 + od_3 + od_4$
$od_6 = \sqrt{(n \times v_1^2) + (od_1 \times od_2)}$ for $v_1 = v_2 = 2$

df_x: difference between consecutive od values. Difference between different observation decks will be referred with a numerical subscript value. For e.g. df_6 represents difference between consecutive od_6 values

id: sequence number starting from 1

$Steady\ State\ Value$: the value which can be expressed as a function of Δ and some constant k and doesn't change for a particular observation deck with a specific dial setting, for any Δ

$\Delta\ sieve\ zone$: this is the zone where Δ can be sieved. It is hypothesized that there are infinite Δ sieve zones

$\Delta\ sieve\ coverage$: sum total of numbers that can be sieved in a particular Δ sieve zone with specific dial settings

$Switchover\ zone$: the first row of a zone when the steady state value is first observed is defined as the switchover zone (soz) for that observation deck

$Reflection\ over\ \{X,Y\}\ or\ ro\{X,Y\}$: when value of an observation deck repeats over an interval from some convergence points/values, it is referred as $ro\{X,Y\}$

4 Steady State Value

For some fixed dials and known Δ, we aim to find nontrivial observation decks, such that:

$$\sum_{i=x}^{k} a_i df_i = 0 \text{ for } x,k \in \mathbb{N},\ a \in \mathbb{Z}_0\text{; and}$$
$$\sum_{i=x}^{k} a_i od_i \neq 0 \text{ for } x,k \in \mathbb{N},\ a \in \mathbb{Z}_0 \tag{6}$$

When this is achieved, it is hypothesized, that a steady state value will be yielded in a specific Δ sieve zone of an observation deck and this steady state will remain constant for **any** Δ in the same observation deck. There can be many different steady states in different (or same) observation decks and the steady state value as a function of Δ and constants is expressed as:

$$c_1\Delta^2 + c_2\Delta + k \tag{7}$$

Note: $c_1, c_2 \in \mathbb{Q}$, $k \in \mathbb{Z}$ and c_1, c_2, k are constants for a given observation deck with specific dial settings.

Now, finding $\sum_{i=x}^{k} a_i df_i = 0$ is a subset sum problem (SSP), where target sum T = 0 is required. However, in some edge cases, equation (6) may yield a trivial solution. The verification process is simple, as any steady state value that is yielded for known Δ in any observation deck can be verified with "known $\Delta + 4$". Now, if steady state value obtained for known Δ doesn't hold for "known $\Delta + 4$", then the solution of equation (6) was trivial, otherwise, this steady state will remain constant for any Δ in the same observation deck as found for known Δ.

This steady state property is quite interesting, it's like tuning a Δ sieve zone for a particular observation deck with known Δ and sieving any Δ through it (as long as the observation deck yields the corresponding Δ sieve zone). The zone where steady state is observed is referred as a Δ sieve zone for that observation deck. There can be many Δ sieve zones ($zone_0, zone_1, ..., zone_x$), with different steady states in the same observation deck.

Below equations will help in finding the steady state value with specific dial settings in $zone_0$ of od_4 and od_2. When a steady state value is yielded in $zone_0$ of an observation deck, then it is hypothesized that this steady state will continue until ∞. Let's see this for od_4 first, when:

$dial_P = \{0,-1,2,2\}$; $\Delta = 4k, p = 2j+1,\ k,j \in \mathbb{N}$; or
$dial_P = \{0,-1,2,2\}$; $\Delta = 4k+2, p = 2j,\ k,j \in \mathbb{N}$; or
$dial_P = \{-1,0,2,2\}$; $\Delta = 4k+2, p = 2j+1,\ k,j \in \mathbb{N}$; or
$dial_P = \{-1,0,2,2\}$; $\Delta = 4k, p = 2j,\ k,j \in \mathbb{N}$

$$SteadyStateValue_{od_4} = \frac{\Delta^2}{2} + 2 \tag{8}$$

Likewise, for od_2, when:

$dial_P = \{0,-1,2,2\}$; $\Delta = 4k+2, p = 2j+1,\ k,j \in \mathbb{N}$; or
$dial_P = \{0,-1,2,2\}$; $\Delta = 4k, p = 2j,\ k,j \in \mathbb{N}$; or
$dial_P = \{-1,0,2,2\}$; $\Delta = 4k, p = 2j+1,\ k,j \in \mathbb{N}$; or
$dial_P = \{-1,0,2,2\}$; $\Delta = 4k+2, p = 2j,\ k,j \in \mathbb{N}$

$$SteadyStateValue_{od_2} = \left(\frac{\Delta}{2}\right)^2 \tag{9}$$

Also, when $p < q$, then the value of p on first occurrence of steady state value in $zone_0$ (either od_2 or od_4) and when $dial_P = \{0,-1,2,2\}$ is given as:

$$p = \begin{cases} \left(2 \times \left(\frac{\Delta-4}{4}\right)\left(\frac{\Delta-4}{4}+1\right)\right)+1 & \text{for } \Delta = 4k,\ k \in \mathbb{N};\ p = 2j+1,\ j \in \mathbb{N} \quad (10a) \\ \left(\frac{\Delta-6}{4}+1\right)^2 - \left(\frac{\Delta-6}{4}\right) & \text{for } \Delta = 4k+2,\ k \in \mathbb{N};\ p = 2j+1,\ j \in \mathbb{N} \quad (10b) \\ \left(\frac{\Delta-4}{4}\right)^2 & \text{for } \Delta = 4k, k = 2m+1,\ k,m \in \mathbb{N}; p = 2j,\ j \in \mathbb{N} \quad (10c) \\ \left(\frac{\Delta-4}{4}\right)\left(\frac{\Delta-4}{4}+1\right) - \left(\frac{\Delta-4}{4}-1\right) & \text{for } \Delta = 4k, k = 2m,\ k,m \in \mathbb{N}; p = 2j,\ j \in \mathbb{N} \quad (10d) \\ \left(2 \times \left(\left(\frac{\Delta-6}{4}+1\right)^2 - 1\right)\right)+2 & \text{for } \Delta = 4k+2,\ k \in \mathbb{N};\ p = 2j,\ j \in \mathbb{N} \quad (10e) \end{cases}$$

Likewise, when $dial_P = \{-1,0,2,2\}$ and when $p < q$, then the value of p on first occurrence of steady state value in $zone_0$ (either od_2 or od_4) is given as:

$$p = \begin{cases} \left(\frac{\Delta-4}{4}\right)^2 & \text{for } \Delta = 4k, k = 2m,\ k,m \in \mathbb{N}; p = 2j+1,\ j \in \mathbb{N} \quad (11a) \\ \left(\frac{\Delta-4}{4}\right)\left(\frac{\Delta-4}{4}+1\right) - \left(\frac{\Delta-4}{4}-1\right) & \text{for } \Delta = 4k, k = 2m+1,\ k,m \in \mathbb{N}; p = 2j+1,\ j \in \mathbb{N} \quad (11b) \\ \left(2 \times \left(\left(\frac{\Delta-6}{4}+1\right)^2 - 1\right)\right)+3 & \text{for } \Delta = 4k+2,\ k \in \mathbb{N};\ p = 2j+1,\ j \in \mathbb{N} \quad (11c) \\ \left(2 \times \left(\frac{\Delta-4}{4}\right)\left(\frac{\Delta-4}{4}+1\right)\right)+2 & \text{for } \Delta = 4k,\ k \in \mathbb{N};\ p = 2j,\ j \in \mathbb{N} \quad (11d) \\ \left(\frac{\Delta-6}{4}\right)\left(\frac{\Delta-6}{4}+1\right)+2 & \text{for } \Delta = 4k+2,\ k \in \mathbb{N};\ p = 2j,\ j \in \mathbb{N} \quad (11e) \end{cases}$$

A new system and method is presented to factorize any composite n, which is a product of two large primes p and q, by searching for Δ, which is the difference between the two primes, i.e. $\Delta = |p-q|$.

Furthermore, we have been able to generalize the steady state value in different observation decks. In this paper we will cover these generalizations for od_4 and od_5 in any $zone$ and with respective dial settings.

Steady state from od_4 (for any Δ) when $dial_1 = \{0, -1\}$ or $dial_1 = \{-1, 0\}$ and $v_1 = v_2$

$$SteadyStateValue_{od_4} = \frac{(\Delta)^2}{2} + \frac{(v_1)^2}{2} \text{ for } v_1 = 2k \text{ where } k = 2j+1 \text{ for } j \in \mathbb{N}_0 \tag{12}$$

Steady state from od_5 (for any Δ) when $dial_1 = \{-2, -1\}$ or $dial_1 = \{-1, -2\}$ and $v_1 = v_2$

$$SteadyStateValue_{od_5} = \Delta^2 + \frac{3}{4}(v_1)^2 \text{ for } v_1 = 4k \text{ where } k = 2j+1 \text{ for } j \in \mathbb{N}_0 \tag{13}$$

It is also hypothesized that with the same dial settings, the steady state value will appear in the same Δ sieve zone of a specific observation deck for any Δ. However, the number of rows in these Δ sieve zones will be different for different Δ and will be referred as "Δ sieve coverage".

We believe this is a new territory and from our research we couldn't find any prior art where Δ has been the primary focus for factorization purposes. As a result, we had to introduce some new notations and terminologies. There are 47 Tables and 10 Figures in this paper which will explain these ideas and concepts with clear examples. We now present the examples below making references to the respective tables and figures.

Kindly note, the values of Δ are selected in a manner to accommodate $\Delta = 4k$, $\Delta = 4k+2$ forms when Δ is even and $\Delta = 4k+1$, $\Delta = 4k+3$ forms when Δ is odd. The concepts will remain valid for any large value of Δ.

"Place Table 1 here." Below observations can then be made:

- Steady State Value = 74 as per equation (8) or as per equation (12)
- $dial_2$ $(v_1 = v_2) = 2$
- $p = 13$ as per equation (10a)
- $zone_0$ for od_4 is defined from $id = 7 \to \infty$

"Place Table 2 here." Below observations can then be made:

- Steady State Value = 121 as per equation (9)
- $p = 21$ as per equation (10b)
- $zone_0$ for od_2 is defined from $id = 11 \to \infty$

"Place Table 3 here." Below observations can then be made:

- Steady State Value = 36 as per equation (9)
- $p = 4$ as per equation (10c)
- $zone_0$ for od_2 is defined from $id = 2 \to \infty$

"Place Table 4 here." Below observations can then be made:

- Steady State Value = 64 as per equation (9)
- $p = 10$ as per equation (10d)
- $zone_0$ for od_2 is defined from $id = 5 \rightarrow \infty$

"Place Table 5 here." Below observations can then be made:

- Steady State Value = 244 as per equation (8) or as per equation (12)
- $dial_2\,(v_1 = v_2) = 2$
- $p = 50$ as per equation (10e)
- $zone_0$ for od_4 is defined from $id = 25 \rightarrow \infty$

"Place Table 6 here." Below observations can then be made:

- Steady State Value = 144 as per equation (9)
- $p = 25$ as per equation (11a)
- $zone_0$ for od_2 is defined from $id = 13 \rightarrow \infty$

"Place Table 7 here." Below observations can then be made:

- Steady State Value = 36 as per equation (9)
- $p = 5$ as per equation (11b)
- $zone_0$ for od_2 is defined from $id = 3 \rightarrow \infty$

"Place Table 8 here." Below observations can then be made:

- Steady State Value = 244 as per equation (8) or as per equation (12)
- $dial_2\,(v_1 = v_2) = 2$
- $p = 51$ as per equation (11c)
- $zone_0$ for od_4 is defined from $id = 26 \rightarrow \infty$

"Place Table 9 here." Below observations can then be made:

- Steady State Value = 74 as per equation (8) or as per equation (12)
- $dial_2\,(v_1 = v_2) = 2$
- $p = 14$ as per equation (11d)
- $zone_0$ for od_4 is defined from $id = 7 \rightarrow \infty$

"Place Table 10 here." Below observations can then be made:

- Steady State Value = 121 as per equation (9)
- $p = 22$ as per equation (11e)
- $zone_0$ for od_2 is defined from $id = 11 \rightarrow \infty$

In addition, we will relook at Table 1, Table 5, Table 8 and Table 9, with focus turned to the difference between the consecutive observation deck values, represented as df_x, where x is the reference number that identifies the respective observation deck. The hypothesis that a Δ sieve zone will be yielded when the sum total of these df_x is 0 and mathematically represented as $\sum_{i=x}^{k} a_i df_i = 0$ for $x, k \in \mathbb{N}$, $a \in \mathbb{Z}$ will also become clear. When this is achieved, the steady state value will be yielded in the respective Δ sieve zone and its value will be expressed as $\sum_{i=x}^{k} a_i od_i$ for $x, k \in \mathbb{N}$, $a \in \mathbb{Z}$. One exception to this rule occurs at *switchover zones*, where Δ sieve zone is yielded but $\sum_{i=x}^{k} a_i df_i \neq 0$

"Place Table 11 here." Below observations can then be made:

- Δ sieve zone is yielded in od_4 when $df_1 + df_2 = 0$
- There is an exception to the above rule, at the switchover zones (id=7), where Δ sieve zone is yielded but $df_1 + df_2 \neq 0$

"Place Table 12 here." Below observations can then be made:

- Δ sieve zone is yielded in od_4 when $df_1 + df_2 = 0$
- There is an exception to the above rule, at the switchover zones (id=25), where Δ sieve zone is yielded but $df_1 + df_2 \neq 0$

"Place Table 13 here." Below observations can then be made:

- Δ sieve zone is yielded in od_4 when $df_1 + df_2 = 0$
- There is an exception to the above rule, at the switchover zones (id=26), where Δ sieve zone is yielded but $df_1 + df_2 \neq 0$

"Place Table 14 here." Below observations can then be made:

- Δ sieve zone is yielded in od_4 when $df_1 + df_2 = 0$
- There is an exception to the above rule, at the switchover zones (id=7), where Δ sieve zone is yielded but $df_1 + df_2 \neq 0$

We will continue to expand on this idea to yield Δ sieve zones in different observation decks. We will see this with few more examples for od_5 "Place Table 15 here." Below observations can then be made:

- For od_5, Δ sieve zone will be yielded when $df_1 + df_2 + df_3 + df_4 = 0$
- There is an exception to the above rule, at the switchover zones (id=56), where Δ sieve zone is yielded but $df_1 + df_2 + df_3 + df_4 \neq 0$
- $dial_2\,(v_1 = v_2) = 4$
- $zone_0$ is defined from id = 56 to ∞
- $SteadyStateValue_{od_5} = 2128$ as per equation (13)

"Place Table 16 here." Below observations can then be made:

- For od_5, Δ sieve zone will be yielded when $df_1 + df_2 + df_3 + df_4 = 0$
- There is an exception to the above rule, at the switchover zones (id=61), where Δ sieve zone is yielded but $df_1 + df_2 + df_3 + df_4 \neq 0$
- $dial_2\,(v_1 = v_2) = 4$
- $zone_0$ is defined from id = 61 to ∞

- $SteadyStateValue_{od_5} = 2316$ as per equation (13)

It is hypothesized that once the steady state is achieved in $zone_0$ of od_2, od_4 or od_5 for any Δ, this steady state will continue until ∞

A quick note with regards to the primary purpose of covering the natural numbers of the form $p,q = 2j$, for $j \in \mathbb{N}$ (the even numbers) as given in Table 3, Table 4, Table 5, Table 9 and Table 10 is to highlight the applicability of relationship with Δ in different observation decks (od), which is especially useful when we try to factorize the composite n by taking its multiple, like $4kn$, for $k \in \mathbb{N}$, as this multiple (k) will change the Δ

In fact, relationship with Δ exists for any kn, for $k \in \mathbb{N}$. We will cover the "$odd\ \Delta$" use case, i.e. $\Delta = 4k+1\ and\ \Delta = 4k+3$ for $k \in \mathbb{N}_0$ towards the end of this paper.

4.1 $dial_P$

A dial pair, represented as "$dial_P = \{dial_1, dial_2\} = \{a_1, a_2, v_1, v_2\}$" (or like a matrix as given under the "Notation and setup" section) plays a critical role in understanding how to sieve the Δ. We have briefly explained how the dial pairs are chosen as per equations: (4a), (4b), (5a) and (5b), but we will take a quick moment to explain it a bit more in this subsection.

$dial_1$: Relative distance from $\lfloor\sqrt{n}\rfloor$

1. We start with the composite n we want to factorize and it's $\sqrt{n}$. We take the floor value of $\sqrt{n}$ ($\lfloor\sqrt{n}\rfloor$). So, we have n and $\lfloor\sqrt{n}\rfloor$
2. Now, $\lfloor\sqrt{n}\rfloor$ can either be even ($\lfloor\sqrt{n}\rfloor = 2j$ for $j \in \mathbb{N}$) or odd ($\lfloor\sqrt{n}\rfloor = 2j+1$ for $j \in \mathbb{N}$)
3. If $\lfloor\sqrt{n}\rfloor = 2j$ for $j \in \mathbb{N}$, we select a value a_1, likewise, if $\lfloor\sqrt{n}\rfloor = 2j+1$ for $j \in \mathbb{N}$, we select a value a_2. Both $a_1, a_2 \in \mathbb{Z}_0$ and together a_1, a_2 are referred as $dial_1$ and represented as $dial_1 = \{a_1, a_2\}$
4. Let's use $dial_1 = \{-1, 1\}$ in below examples:
   (a) If $n_1 = 137$, $\lfloor\sqrt{n}\rfloor = 11$, then $a_2 = 1$ and $dial_1 = 1$
   (b) Likewise, if $n_2 = 147$, $\lfloor\sqrt{n}\rfloor = 12$, then $a_1 = -1$ and $dial_1 = -1$

Before we go to $dial_2$, we should see how $dial_1$ is put to use when calculating d_1:

1. $d_1 = \lfloor\sqrt{n}\rfloor + dial_1$
2. From example in point 4(a) above, $d_1 = 11 + 1 = 12$
3. From example in point 4(b) above, $d_1 = 12 + (-1) = 11$

$dial_2$: Relative distance from d_1

1. If $d_1 = 2j$ for $j \in \mathbb{N}$, we select a value v_1, likewise, if $d_1 = 2j+1$ for $j \in \mathbb{N}$, we select a value v_2. Both $v_1, v_2 \in \mathbb{Z}$ and together v_1, v_2 are referred as $dial_2$ and represented as $dial_2 = \{v_1, v_2\}$

2. Let's use $dial_2 = \{2,4\}$ in below examples:

   (a) If $n_1 = 137$, $\lfloor\sqrt{n}\rfloor + dial_1 = 12$, then $v_1 = 2$ and $dial_2 = 2$
   (b) Likewise, if $n_2 = 147$, $\lfloor\sqrt{n}\rfloor + dial_1 = 11$, then $v_2 = 4$ and $dial_2 = 4$

d_2:

1. $d_2 = d_1 + dial_2$

2. From above examples, for $n_1 = 137$, $d_1 = 12$, $dial_2 = 2$, then, $d_2 = 12 + 2 = 14$

3. Likewise, for $n_2 = 147$, $d_1 = 11$, $dial_2 = 4$, then, $d_2 = 11 + 4 = 15$

There can be infinite dial pairs and changing their settings can change the Δ sieve zone within an observation deck. In some cases, $\{v_1, v_2\}$ of $dial_2$ plays a critical role (together with Δ) in calculating the steady state value.

Also, when there are two or more dial pairs, like, $dial_{P1} = \{0,-1,6,6\}$ and $dial_{P2} = \{-2,1,16,16\}$, they may be connected with some relationship(s) with each other, such that, systematic increment to $dial_{P1}$ will require respective changes to $dial_{P2}$ in order to maximize the Δ sieve coverage in different or same observation decks.

For e.g.:

- $v1_{dial_{P2}} = (2 \times v1_{dial_{P1}}) + 4$; or

- $v1_{dial_{P2}} = v1_{dial_{P1}} + 10$

Assuming $v_1 = v_2$ in both dial pairs, if we now increment $dial_{P1} = \{0,-1,10,10\}$, there can be two corresponding updates that can be made to v_1, v_2 of $dial_{P2}$ as per the above relationships:

- $dial_{P2} = \{-2,1,24,24\}$; or

- $dial_{P2} = \{-2,1,20,20\}$

In addition, intra dial relationship(s) between a_1, a_2, v_1 and v_2 will also exist and the increment applied to a_1, a_2, v_1 and v_2 to change the Δ sieve zone will be dependent on Δ, in terms of whether Δ is of $4k, 4k+1, 4k+2$ or $4k+3$ form, for $k \in \mathbb{N}$

4.2 Δ sieve zones ($zone_0, zone_1, ..., zone_x$)

This is the zone within an observation deck where Δ can be sieved. For fixed dial settings, the steady state value remains constant in these zones. As the dial settings change, the Δ sieve zone will shift and the steady state value will also change. However, this steady state value will continue to remain a function of Δ, dial settings and some constant k, as mentioned in equation (7)

The property for Δ sieve zone to shift (from $zone_0 --> zone_1 --> ... --> zone_x$) as dial settings change is also quite interesting. This is like tuning the $zone_0$ of Δ sieve zone for a particular observation deck first and then sieving the Δ in any other zones for any n in that Δ series by appropriately changing the involved dials.

Example data for equations (12) and (13) is given below in Table 17 and Table 18 respectively.

Note: Since the screen real estate can't accommodate all the Table columns, we will only keep the most relevant columns to clarify the concepts.

"Place Table 17 here." Following observations can then be made. The Δ sieve zone in od_4 shifts up and moves to $zone_1$ as we change $dial_2$ to 6

- Δ sieve zone is yielded when $df_1 + df_2 = 0$ with an exception at $id = 6$, referred as *switchover zone* (details in subsection 4.4 below)
- $zone_1$ for od_4 is defined from $6 <= id < 26$
- $dial_2$ $(v_1 = v_2) = 6$
- $SteadyStateValue_{od_4} = 260$ as per equation (12)

"Place Table 18 here." Following observations can then be made. The Δ sieve zone in od_5 shifts up and moves to $zone_1$ as we change $dial_2$ to 12

- Δ sieve zone is yielded when $df_1 + df_2 + df_3 + df_4 = 0$ with an exception at $id = 8$, referred as *switchover zone*
- $zone_1$ for od_5 is defined from $8 <= id < 12$
- $dial_2$ $(v_1 = v_2) = 12$
- $SteadyStateValue_{od_5} = 2224$ as per equation (13)

Likewise, one can make the Δ sieve zones shift into different zones by changing the dials for different observation decks.

4.3 Δ sieve coverage

Δ sieve coverage determines the sum total of numbers which are under the Δ sieve zone for a given set of dial pairs. As the dial settings change, the Δ sieve coverage will also change. In the below examples, one can sieve for Δ in od_1, od_2, od_4, od_5 for given dial pair.

- "Place Table 19 here." With $\Delta = 160$ and $\{a_1, a_2, v_1, v_2\}$ = {-2, 2, 12, 12}, we can sieve the Δ in respective observation decks

- "Place Table 20 here." With $\Delta = 480$ and $\{a_1, a_2, v_1, v_2\}$ = {-2, 2, 12, 12}, we can sieve the Δ in respective observation decks

Note the increase in Δ sieve coverage with increasing Δ in respective observation decks.

Numbers outside of Δ sieve coverage are referred as "$zoneless$". However, the same numbers may come under respective observation decks Δ sieve zones as dial settings change and will become "$zoners$".

With one dial pair, we are able to create six observation decks, but given od_3, od_4, od_5, od_6 are derived from od_1 and od_2, we can potentially have infinite such observatories from just one dial pair. It's also important to have non-overlapping Δ sieve zones distributed amongst these observation decks to increase the overall Δ sieve coverage.

Let's introduce another dial pair and visualize the increase in non-overlapping Δ sieve coverage with increasing Δ sieve zones.

$\Delta = 94$

$dial_{P1} = \{dial_1, dial_2\} = \{0, -1, 6, 6\}$

$dial_{P2} = \{dial_3, dial_4\} = \{-2, 1, 16, 16\}$

$d_3 = \lfloor\sqrt{n}\rfloor + dial_3$

$d_4 = d_3 + dial_4$

$od_7 = d_3^2 - n$

$od_8 = d_4^2 - n$

$od_9 = od_2 + od_8$

$od_{10} = od_4 + od_8$

$od_{11} = od_2 + (2 \times od_8) + od_4$

With $dial_{P1} = \{0, -1, 6, 6\}$ and $dial_{P2} = \{-2, 1, 16, 16\}$, the below steady state values can be observed from respective observation decks for **any** Δ

$$SteadyStateValue_{od_{9a}} = \frac{\Delta^2}{2} + 72 \tag{14}$$

$$SteadyStateValue_{od_{9b}} = \frac{\Delta^2}{2} + 32 \tag{15}$$

$$SteadyStateValue_{od_{10}} = \frac{\Delta^2}{2} + \left(\frac{\Delta}{2}\right)^2 + 168 \tag{16}$$

$$SteadyStateValue_{od_{11}} = \Delta^2 + \left(\frac{\Delta}{2}\right)^2 + 144 \tag{17}$$

“Place Table 21 here.” One can see how Δ is now being sieved in different observation decks. These Δ sieve zones will remain constant for any Δ in respective observation decks. We will now be able to see how the Δ sieve coverage increases with increase in Δ through Figure 1. “Place Figure 1 here.” Below observations can then be made.

Here, we have excluded od_8 and od_7 as they are the perfect square forms and factorization can be easily achieved with difference of squares method. While the relationship with Δ still exists, we wanted to get the statistics for non perfect square forms. The **only** purpose of this graph in Figure 1 is to confirm the hypothesis stated previously around tuning some Δ sieve zones in shape of fixed observation decks for any **one** Δ and sieving **any** other Δ through them. It is this property that makes it quite lucrative to approach the factorization problem via this method. In addition, this also confirmed that the Δ sieve coverage will also grow with increase in Δ.

However, one important point to note is, p will also grow at the same rate for its corresponding Δ, bringing p & q close to each other with reference to their respective Δ, making factorization simple through Fermat's method as well.

“Place Figure 2 here.”

1. p on x-axis represents the growth of p with increasing Δ sieve coverage (filled in red) for fixed $\Delta = 1002$
2. Area highlighted in red will come under Δ sieve coverage from od_4 and od_5 with base dial starting at $\{0, -1, 8, 8\}$ and $v_1 = v_2$ having an incremental rate of +8 with each iteration
3. Light red signifies the non-overlapping coverage zones between od_4 and od_5, while dark red means overlapping zones between these two observation decks

4.4 Switchover zone (soz)

The first row of a zone when the steady state value is first observed is defined as the switchover zone (soz) for that observation deck. Based on $dial_1$, $dial_2$, ... , $dial_x$, the steady state values can be different at these switchover zones. Also, while steady state value is yielded at the switchover zones, however, $\sum_{i=x}^{k} df_i \neq 0$ here.

“Place Table 22 here.” Below observations can then be made:

- The row in bold is soz_1 for od_4 with dial settings mentioned in Table 22

“Place Table 23 here.” Below observations can then be made:

- The row in bold is soz_0 for od_5 with dial settings mentioned in Table 23

4.5 Switchover point (sop)

Switchover points are observed from od_3 and are quite dense at the beginning for a given Δ starting with $p = 1$, but their frequency decreases as one progresses with the Δ series with increasing p. "Place Table 24 here." Below observations can then be made:

- The rows in bold are switchover points for od_3 with dial settings mentioned in the Table 24.
  1. $od_{3_{sop_2}} = 120$ $(id = 2, df_3 = -48)$
  2. $od_{3_{sop_3}} = 168$ $(id = 3, df_3 = -48)$
  3. $od_{3_{sop_6}} = 264$ $(id = 6, df_3 = -48)$

5 Intra Δ relationships (aΔ)

The purpose is to find the "previous composite n" or "next composite n" with the same Δ as that of the composite n we are trying to factorize. "previous composite n" will be represented as odd subscripts (n_1, n_3, n_5, etc) with higher odd subscripts away from the n we are trying to factorize. Likewise, "next composite n" will be represented as even subscripts (n_2, n_4, n_6, etc) with higher even subscripts away from the n we are trying to factorize.

5.1 od connect

Different observation decks (od) can be connected to each other through a nontrivial relationship that can help to yield the previous or next composite n. We will see this with following example. "Place Table 25 here." We need to factorize $n = 219781$

As a first step, observation deck values will be calculated for this n, i.e. od_1, od_2, od_3, od_4 (highlighted in bold in Table 25). Based on this available information, some relationship needs to be established with other observation decks so we can determine $n_{id=137}$ (value of n for $id = 137$). In this example we can see:

$$(od_{3_{id=136}}) - (od_{3_{id=137}}) = -8 \tag{18}$$

$$od_{4_{id=136}} - df_{4_{id=137}} = od_{4_{id=137}} \tag{19}$$

$$\left(\frac{od_{3_{id=136}}}{4} - df_{4_{id=137}}\right) \times 2 = od_{4_{id=137}} \tag{20}$$

In above equations (19) and (20), "$df_{4_{id=137}}$", represents the value of df_4 for $id = 137$.

The relationship in equation (20) is key in finding the next n . However, It's not known how many such nontrivial relationships are out there to make this method effective.

Let's find n_2 for $id = 137$. From (18), (19) and (20):

$$od_3 = 1884, od_4 = -214, df_4 = 576 \tag{21}$$

$$\begin{aligned} od_3 &= od_2 - od_1 \\ od_4 &= od_2 + od_1 \end{aligned} \tag{22}$$

From (21) and (22) and assuming we are not going to hit the *switchover point* (*sop*), $d1_{id=137} = d1_{id=136} + 2$, so $d1_{id=137} = 470$

$$\begin{aligned} od_1 &= -1049, od_2 = 835 \\ od_1 &= d_1^2 - n \\ -1049 &= 470^2 - n \\ n_2 &= 221949 \end{aligned} \tag{23}$$

Once n_2 is known, determining its factors should be simple, assuming n_2 is not a difficult semiprime. Once the factors of n_2 are determined, it will be easy to find out the nontrivial factors of the composite n we are trying to factorize.

5.2 Range of previous/next n

The aim is to first find the range within which the previous or next composite n values will fall, such that they have the same Δ as that of the composite n we are trying to factorize. Once the range is known, the second goal is to find some nontrivial relationship between min/max value of this range and od_x, df_x, Δ, so the previous or next composite n can be found efficiently. Kindly note, we are not covering this second goal in this paper. “Place Table 26 here.”

If $n = 1643$, $od_1 = -122$, then:
$n_3 = 1323$, $d1_{n_3} = 35$, $n_1 = 1479$, $d1_{n_1} = 37$
$n_2 = 1815$, $d1_{n_2} = 41$, $n_4 = 1995$, $d1_{n_4} = 43$

Assuming the previous and next n values are not going to cross the switchover points, which means d_1 will be linear and we can find the respective ranges for n_1, n_2, ... ,n_x

$n_1range = (d_{1_{n_3}}^2 - od_1)$ to $(d_{1_{n_1}}^2 - od_1) = (35^2 + 122)$ to $(37^2 + 122) = 1347$ to 1491
$n_1range_{min} = 1347$ and $n_1range_{max} = 1491$

$n_2range = (d_{1_{n_2}}^2 - od_1)$ to $(d_{1_{n_4}}^2 - od_1) = (41^2 + 122)$ to $(43^2 + 122) = 1803$ to 1971
$n_2range_{min} = 1803$ and $n_2range_{max} = 1971$

Summary of the ranges we obtained above:

- n_1 range: 1347 - 1491
- n_2 range: 1803 - 1971

5.3 Reflection over {X,Y}

As we are looking for Δ indirectly in this observation deck by finding the previous or next composite integer having the same Δ as that of the composite n we are trying to factorize, this goal is achieved by looking for reflected od_6 values here.

“Place Table 27 here.” $od_6 = \sqrt{4n + (od_1 \times od_2)}$ for $\{v_1, v_2\} = \{2,2\}$. Reflection over **4,4** is observed. Since $|X - Y| = 0$, values will be same over the reflection points for some interval. Here {X,Y} = {4,4} and is represented as: $ro\{4,4\}_0$

“Place Table 28 here.” Reflection over **3,5** is observed. Since $|X - Y| = 2$, reflected values will differ by 2 over the reflection points. Here {X,Y} = {3,5} and is represented as: $ro\{3,5\}_2$

Note:

1. Reflection can be some distance d apart from the point(s) of convergence (X, Y)
2. When searching for od_6, it's not known at the start whether to search up or down and hence one may need to go in both directions simultaneously

od_6 search is carried out based on certain assumptions around how the reflection will occur so as to find a nontrivial n_1 or n_2, such that the Δ between the factors of n_1 or n_2 is same as that of the composite n we are trying to factorize. Below equation is used for this search:

$$\begin{aligned}
&(od_6)^2 = d_1^4 + 4(d_1)^3 + n_2^2 + 4(d_1)^2 - 2n_2(d_1)^2 - 4n_2 d_1 \\
&\quad OR \\
&(od_6)^2 = d_1^4 + 4(d_1)^3 + n_1^2 + 4(d_1)^2 - 2n_1(d_1)^2 - 4n_1 d_1
\end{aligned} \tag{24}$$

Key points with regards to equation (24):

1. $n_2 > n > n_1$
2. d_1 is dependent on the corresponding n (n_1, n_2, etc) and on fixed dial settings
3. There can be many trivial n_1 or n_2 satisfying the above equation
4. There is also a possibility for some of the Δs of these trivial n_1 or n_2 to be in close vicinity of the nontrivial Δ of composite n we are trying to factorize
5. Reflection is not a mandatory condition for carrying out od_6 search
6. The below graphs visualizes all od_6 values for different Δs until steady state is achieved

“Place Figure 3 here.” and “Place Figure 4 here.” Key points with regards to Figure 3 and Figure 4 below:

1. The graphs are dependent on $dial_2$, i.e. $v_1 = v_2 = 2$, i.e. graphs will change if v_1 or v_2 changes

2. The graphs looks like letter "A", increasing (or decreasing) in its size as it attains the steady state. For this reason, this will be referred as "A_+" or "A_-" graph.

3. We observed the same A_+ pattern for large Δs (for both $\Delta = 4k$ and $\Delta = 4k + 2$ form, for $k \in \mathbb{N}$) and hence we hypothesized that reflections in od_6 are imminent

4. Note: n is on log scale on x-axis

“Place Figure 5 here.” and “Place Figure 6 here.” A quick look at some other graphs with different $v_1 = v_2$ values.

1. Figure 5: $v_1 = v_2 = 14$
2. Figure 6: $v_1 = v_2 = 37$

6 Inter Δ relationships (rΔ)

$$known\ \Delta = delta\_val_{id=id\_val}\{dial_{P1}, ...dial_{Pn}\} \simeq unknown\ \{\Delta_1, \Delta_2, \Delta_3\} \simeq \{n1, n2, n3\} \tag{25}$$

This section is about finding relationships with “known Δ” and “unknown Δs”. Any od_x, df_x, $zone_x$ where we are searching for Δ can have nontrivial relationships with any other od_x, df_x, $zone_x$ of any one or more known Δs

Also, with a given known Δ, known dial pairs (one or more) and some fixed id (one or more), many other unknown Δs can be selected $(\Delta_1, \Delta_2, \Delta_3)$ such that for these fixed dial pairs, known Δ yields a Δ sieve zone at selected id value(s) in any one of the observation decks, and the same number of dial pairs will yield Δ sieve zones for the respective unknown Δs. Conversely, for many unknown Δs, a known Δ can be found with some fixed id (one or more), such that the same number of dial pairs will yield Δ sieve zones for both known Δ and unknown Δs.

Let’s see equation (25) with below example:

$$known\ \Delta = 122_{id=93}\{0, -1, 8, 8\} \simeq \{162, 178, 202\} \simeq \{785539, 936863, 441383\} \tag{26}$$

Details of notation used in equations (25) and (26):

- "known $\Delta = 122_{id=93}\{0, -1, 8, 8\}$": A Δ sieve zone is observed (in od_2) at $id = 93$ for $\Delta = 122$ with $dial_P = \{0, -1, 8, 8\}$
- "≃": Similar/equal symbol is used for now. Having a Δ sieve congruence symbol will be useful
- "{162, 178, 202}": Set of unknown Δs
- "{785539,936863,441383}": A Δ sieve zone will be observed for these n for $dial_P = \{0, -1, 8, 8\}$ in one of the observation decks.

“Place Table 29 here.” $n1 = 785539$, $n2 = 936863$, $n3 = 441383$
Here, known $\Delta\{122\}$ is linked with unknown $\Delta\{162, 178, 202\}$ with a fixed reference of $dial_P = \{0, -1, 8, 8\}$

Note: $dial_P$ of unknown Δs doesn’t necessarily have to be fixed and can change as long as there is some relationship between $dial_P$ of unknown Δs with $dial_P$ of known Δ for factorization purposes.

7 The sum series ($\sum = p + q$)

Very similar to Δ series, instead of studying all p, q linked with the same Δ, we study all p, q linked with the same $\sum$, such that, $\Delta_{|p-q|} = \sum_{p+q}$

"Place Table 30 here." and "Place Table 31 here." Below observations can then be made.

The N on $\sum$ series, as described in Table 30 and Table 31 is connected with od_6 on the Δ series. It is this relationship between N and od_6 that not only lays the foundation for a new factorization method but also a new trapdoor function supporting two different keys for encryption and decryption respectively. This is explained clearly with more examples in the next sections.

8 The equilibrium of $\Delta_{|p-q|}$ and $\sum_{p+q}$

The equilibrium between N on $\sum_{p+q}$ and od_6 on $\Delta_{|p-q|}$ series is reached when:

$$N_{\Delta \rightleftharpoons \Sigma} = \begin{cases} od6_{\Delta_{|p-q|}} & \text{for } \Delta = 4k, p = 2j+1,\ k, j \in \mathbb{N};\ \Delta = 4k+2, p = 2j,\ k, j \in \mathbb{N} \quad (27a) \\ od6_{\Delta_{|p-q|}} + 1 & \text{for } \Delta = 4k+2, p = 2j+1,\ k, j \in \mathbb{N};\ \Delta = 4k, p = 2j,\ k, j \in \mathbb{N} \quad (27b) \end{cases}$$

"Place Table 32 here." and "Place Table 33 here." The equilibrium is reached when $N_{\Delta \rightleftharpoons \Sigma} = od6_{\Delta_{|p-q|}} = 99$ as per equation (27a)

"Place Table 34 here." In this Table:

- $N_{\Sigma_{p+q}}$ is from Table 33, starting from $N = 99$, for $od_6 = 0$ ($id = 6$) and moving down
- $od6_{\Delta_{|p-q|}}$ is from Table 32, starting from $od_6 = 99$ ($id = 21$) and moving up
- $N_{\Sigma_{p+q}}$ - $od6_{\Delta_{|p-q|}}$ = $\Delta \rightleftharpoons \sum$
- $df_{\Delta\Sigma}$: Difference between consecutive $\Delta \rightleftharpoons \sum$ values

"Place Table 35 here." From Table 34 and Table 35, we define below points:

1. od_6 on Δ series is said to be in "full equilibrium" with N on the $\sum$ series, iff :
   - "od_6 + (any) $\Delta \rightleftharpoons \sum$" can get od_6 to jump to (any) N on it's $\sum$ series, such that, sum of the factors of N equals difference between the factors of n on the Δ series
2. od_6 on Δ series is said to be in "close equilibrium" with n on the $\sum$ series, iff :
   - "od_6 + (any) $\Delta \rightleftharpoons \sum + k,\ k \in \mathbb{N}$" can get od_6 to jump to (any) n on it's $\sum$ series, such that, sum of the factors of N equals difference between the factors of n on the Δ series

When we can make the composite n on Δ series jump to another composite N on $\sum$ series, and assuming the corresponding N on $\sum$ series is not a difficult semiprime, and once the factors of N are found, one can add these factors to get the Δ. Once the Δ is known, the factors of the composite n we are trying to factorize can be easily determined.

$\Delta \rightleftharpoons \sum$ in Table 34 and Table 35 contain the constants, which od_6 on any Δ series can use to jump to N on the $\sum$ series. These constants will be referred as the "global equilibrium constants (gec)". When studying gec with consecutive Δs ($4k$ and $4k+2$ forms separately), we can observe gec grows with increasing Δ, however, the non-constant elements (nce), connecting Δ and $\sum$ series also grow at the same rate. Below two equations can summarize the relationship between gec and nce.

$$Total\ number\ of\ elements\ on\ \Delta\ series = Number\ of\ gec + Number\ of\ nce \tag{28}$$

$$Total\ number\ of\ elements\ on\ \Delta\ series = (2 \times Number\ of\ gec) + residue \tag{29}$$

Number of gec and nce are calculated based on continuous comparison between consecutive Δ and $\Delta + 4$ (for $\Delta = 4k, k \in \mathbb{N}$). "Place Figure 7 here." In reference to this figure:

1. Start with $\Delta = 20$ and get all the elements on Δ series (from p=1 until steady state)
2. Get all the elements on $\sum = 20$ series, such that number of elements between Δ and $\sum$ series is same
3. Calculate $\Delta \rightleftharpoons \sum$ and increment Δ by 4
4. Repeat steps 1 to 3 for this incremented Δ and $\sum$
5. Check how many elements are common (gec) and not common (nce) between $\Delta \rightleftharpoons \sum = 20$ and $\Delta \rightleftharpoons \sum = 24$
6. Continuously increment Δ by 4 and keep comparing the gec and nce with the previous Δ until a preset threshold is reached

"Place Table 36 here." and "Place Table 37 here." Below observations can then be made.

From Table 36 and Table 37, the equilibrium is reached when $N_{\Delta \rightleftharpoons \sum} = od6_{\Delta_{|p-q|}} + 1 = 121$ as per equation (27b)

"Place Table 38 here." In this Table:

- $N_{\sum_{p+q}}$ is from Table 37, starting from $N = 121$, for $od_1 = 0$ ($id = 6$) and moving down
- $od6_{\Delta_{|p-q|}}$ is from Table 36, starting from $od_6 = 120$ ($id = 26$) and moving up
- $N_{\sum_{p+q}}$ - $od6_{\Delta_{|p-q|}} = \Delta \rightleftharpoons \sum$
- $df_{\Delta\sum}$: Difference between consecutive $\Delta \rightleftharpoons \sum$ values

"Place Table 39 here." From Table 38 and Table 39, we define below points:

1. $\Delta \rightleftharpoons \sum$ in Table 38 and Table 39 contain the global equilibrium constants (gec), which od_6 on any Δ series can use to jump to N on the $\sum$ series. The points mentioned earlier for $\Delta = 4k$ form will remain same for $\Delta = 4k + 2$ form as well

"Place Figure 8 here." Both Figure 7 and Figure 8 are almost similar in terms of the growth of gec and nce. However, there is a difference in growth of $residue$ between $\Delta = 4k$ and $\Delta = 4k+2$ for $k \in \mathbb{N}$ form. "Place Figure 9 here." and "Place Figure 10 here." These two figures highlight the difference between the residue graphs.

For completeness, below two examples will cover the use cases when $p = 2k$ for $k \in \mathbb{N}$ form, i.e. p is an even number. "Place Table 40 here." and "Place Table 41 here." We can observe From Table 40 and Table 41, the equilibrium is reached when $N_{\Delta \rightleftharpoons \Sigma} = od6_{\Delta_{|p-q|}} + 1 = 100$ as per equation (27b)

"Place Table 42 here." and "Place Table 43 here." We can observe From Table 42 and Table 43, the equilibrium is reached when $N_{\Delta \rightleftharpoons \Sigma} = od6_{\Delta_{|p-q|}} = 120$ as per equation (27a)

9 The Trapdoor

Computing od_6 from a given n is easy, however, it's not easy to go back to n from od_6 even though Δ is known. Also, we have seen above how $\Delta \rightleftharpoons \sum$ equilibrium connects od_6 on Δ series with N on $\sum$ series and this allows us to find n from od_6 easily when this relationship and Δ are given.

When Δ is known publicly

1. Algorithm
   (a) Message encryption and generating the private key:
      i. Select some large Δ (such that integer $p < p_{ssv}$)
      ii. Select below dial pairs:
         A. For $\Delta = 4k$ for $k \in \mathbb{N}$, $\Delta_{dial_{P1}} = \{0, -1, 2, 2\}$, $\sum_{dial_{P2}} = \{-1, 0, 2, 2\}$
         B. For $\Delta = 4k+2$ for $k \in \mathbb{N}$, $\Delta_{dial_{P1}} = \{-1, 0, 2, 2\}$, $\sum_{dial_{P2}} = \{-1, 0, 2, 2\}$
      iii. Compute steady state value (ssv) from equation (12)
      iv. Compute p_{ssv} at this steady state value from equation (10a). As dials are fixed, equation (10a) can be used for both $\Delta = 4k$ and $\Delta = 4k+2$ for $k \in \mathbb{N}$
      v. Compute $od6_{ssv}$ at this steady state value
      vi. Convert message M into an integer p
      vii. Compute $p_{dist} = p_{ssv} - p$
      viii. Compute $q = p + \Delta$
      ix. Compute $n = p \times q$
      x. Compute od_1 and od_2
      xi. Compute $od_6 = \sqrt{(4n) + (od_1 \times od_2)}$
      xii. od_6 is the ciphertext
      xiii. Compute N_{Σ} :
         A. From equation (27a), $N_{\Delta \rightleftharpoons \Sigma} = od6_{ssv}$
         B. From equation (27b), $N_{\Delta \rightleftharpoons \Sigma} = od6_{ssv} + 1$

xiv. From $N_{\Delta\rightleftharpoons\Sigma}$ and Δ, compute $p_{\Delta\rightleftharpoons\Sigma}, q_{\Delta\rightleftharpoons\Sigma}$ on the sum series, such that $p_{\Delta\rightleftharpoons\Sigma} \times q_{\Delta\rightleftharpoons\Sigma} = N_{\Delta\rightleftharpoons\Sigma}$ and $p_{\Delta\rightleftharpoons\Sigma} < q_{\Delta\rightleftharpoons\Sigma}$ (Note: $\Delta = (p-q)_{\Delta series} = (p+q)_{\Sigma series}$)

xv. Compute $p_{sum\_series} = p_{\Delta\rightleftharpoons\Sigma} - p_{dist}$

xvi. Compute $q_{sum\_series} = \Delta - p_{sum\_series}$

xvii. Compute $N_{sum\_series} = p_{sum\_series} \times q_{sum\_series}$

xviii. Compute $(\Delta \rightleftharpoons \Sigma)_{private} = N_{sum\_series} - od_6$

xix. $(\Delta \rightleftharpoons \Sigma)_{private}$ is the private key

(b) Decryption when cipher text: od_6, private key: $(\Delta \rightleftharpoons \Sigma)_{private}$ and Δ are given:

i. Compute $N_{sum\_series} = od_6 + (\Delta \rightleftharpoons \Sigma)_{private}$

ii. Compute 2 factors of N_{sum_series}: p_{sum_series} and q_{sum_series}, such that $\Delta = p_{sum\_series} + q_{sum\_series}$ and $p_{sum\_series} < q_{sum\_series}$

iii. Compute steady state value (ssv) from equation (12)

iv. Compute $od_{6_{ssv}}$ at this steady state value

v. Compute p_{ssv} at this steady state value from equation (10a). As dials are fixed, equation (10a) can be used for both $\Delta = 4k$ and $\Delta = 4k+2$ for $k \in \mathbb{N}$

vi. Compute $N_{\Delta\rightleftharpoons\Sigma}$:

A. From equation (27a), $N_{\Delta\rightleftharpoons\Sigma} = od_{6_{ssv}}$

B. From equation (27b), $N_{\Delta\rightleftharpoons\Sigma} = od_{6_{ssv}} + 1$

vii. From $N_{\Delta\rightleftharpoons\Sigma}$ and Δ, compute $p_{\Delta\rightleftharpoons\Sigma}, q_{\Delta\rightleftharpoons\Sigma}$ on the sum series, such that $p_{\Delta\rightleftharpoons\Sigma} \times q_{\Delta\rightleftharpoons\Sigma} = N_{\Delta\rightleftharpoons\Sigma}$ and $p_{\Delta\rightleftharpoons\Sigma} < q_{\Delta\rightleftharpoons\Sigma}$

viii. Compute $q_{dist} = q_{sum\_series} - q_{\Delta\rightleftharpoons\Sigma}$

ix. $p = p_{ssv} - q_{dist}$

x. This p is the integer we encrypted earlier and can be converted into original message M

In the below example, we will see the steps involved to encrypt the message (without using any padding scheme) by selecting a Δ, generate the private key and decrypt the encrypted message when Δ and private key are provided.

1. Example-1

(a) Message encryption and generating the private key:

i. $\Delta = 137136$

ii. $\Delta_{dial_{P1}} = \{0, -1, 2, 2\}$, $\sum_{dial_{P2}} = \{-1, 0, 2, 2\}$
iii. Steady State Value = 9403141250
iv. $p_{ssv} = 2350716745$
v. $od6_{ssv}$ = 4701570623
vi. Convert message "AUM" (using ASCII code) into an integer p = **658577**
vii. p_{dist} = 2350058168
viii. q = 795713
ix. n = 524038280401
x. od_1 = -1279185 and od_2 = 1616435
xi. od_6 = **168623**
xii. od_6 is the ciphertext
xiii. $N_{\Delta \rightleftharpoons \Sigma}$ = 4701570623
xiv. $p_{\Delta \rightleftharpoons \Sigma}$ = 68567 and $q_{\Delta \rightleftharpoons \Sigma}$ = 68569
xv. p_{sum_series} = -2349989601
xvi. q_{sum_series} = 2350126737
xvii. N_{sum_series} = -5522773392982061937
xviii. $(\Delta \rightleftharpoons \sum)_{private}$ = **-5522773392982230560**
xix. $(\Delta \rightleftharpoons \sum)_{private}$ is the private key

(b) Decryption when cipher text: od_6, private key: $(\Delta \rightleftharpoons \sum)_{private}$ and Δ are given:
i. N_{sum_series} = -5522773392982061937
ii. p_{sum_series} = -2349989601 and q_{sum_series} = 2350126737
iii. Steady state value = 9403141250
iv. $od6_{ssv}$ = 4701570623
v. p_{ssv} = 2350716745
vi. $N_{\Delta \rightleftharpoons \Sigma}$ = 4701570623
vii. $p_{\Delta \rightleftharpoons \Sigma}$ = 68567 and $q_{\Delta \rightleftharpoons \Sigma}$ = 68569
viii. q_{dist} = 2350058168
ix. p = **658577**
x. This p is the integer we encrypted earlier. With available ASCII mapping, this can be converted back to the original message "AUM"

10 Odd Δ

$$SteadyStateValue_{od_5} = \begin{cases} \Delta^2 + 3 & \text{for } \Delta = 4k+3, p = 2j+1,\ k, j \in \mathbb{N}; dial_{P1} = \{-1, 0, 2, 2\} \quad (30a) \\ \Delta^2 + 3 & \text{for } \Delta = 4k+1, p = 2j+1,\ k, j \in \mathbb{N}; dial_{P1} = \{0, -1, 2, 2\} \quad (30b) \\ \Delta^2 + 3 & \text{for } \Delta = 4k+1, p = 2j,\ k, j \in \mathbb{N}; dial_{P1} = \{-1, 0, 2, 2\} \quad (30c) \\ \Delta^2 + 3 & \text{for } \Delta = 4k+3, p = 2j,\ k, j \in \mathbb{N}; dial_{P1} = \{0, -1, 2, 2\} \quad (30d) \end{cases}$$

The principle of tuning the Δ sieve zone remains the same for odd Δ as well, i.e. we are looking for $\sum df_x = 0$, where x corresponds to those observation decks whose respective df when summed gives 0. One observation deck can be used multiple times to achieve this zero sum state.

As we are observing the steady state from od_5, we are looking for zone(s) where $df_1 + df_2 + df_3 + df_4 = 0$, i.e. $\sum_{x=1}^{4} df_x = 0$. Steady State is yielded at the switchover zone as well, however, $\sum_{x=1}^{4} df_x \neq 0$ here.

“Place Table 44 here.” Below observations can then be made:

- $SteadyStateValue_{od_5} = 532$ as per equation (30a)
- $df_1 + df_2 + df_3 + df_4 = 0$ is achieved at $id = 19$

“Place Table 45 here.” Below observations can then be made:

- $SteadyStateValue_{od_5} = 628$ as per equation (30b)
- $df_1 + df_2 + df_3 + df_4 = 0$ is achieved at $id = 22$

“Place Table 46 here.” Below observations can then be made:

- $SteadyStateValue_{od_5} = 628$ as per equation (30c)
- $df_1 + df_2 + df_3 + df_4 = 0$ is achieved at $id = 22$

“Place Table 47 here.” Below observations can then be made:

- $SteadyStateValue_{od_5} = 532$ as per equation (30d)
- $df_1 + df_2 + df_3 + df_4 = 0$ is achieved at $id = 18$

11 Final Remarks

This is our first number theory paper and even though we have consulted numerous online and offline resources and have reviewed this paper and re-reviewed the review countless times, we still might have had missed some important guidelines and we seek your forgiveness if a spelling or grammar or structure or some obvious rules of the paper writing terrain were not followed correctly and worst, if we still left that typo dangling out there. Our primary focus was to clearly bring out the dimension of $\Delta_{|p-q|}$, $\sum_{p+q}$ and the relationship between the two, i.e. $\Delta_{|p-q|} \rightleftharpoons \sum_{p+q}$. We believe, we have covered a lot of ground here but we are also cognizant that this might just be the beginning of a more beautiful journey some of you will be willing to embark upon and find more esoteric connections and hopefully one day, with some hard work and a lot of grace, we may find that factorization was always in O(1), Uff!

The property of Δ sieve zones being yielded when $\sum_{i=x}^{k} a_i df_i = 0$ for $x, k \in \mathbb{N}$, $a \in \mathbb{Z}$ and the respective Δ sieve values getting expressed as: $c_1\Delta^2 + c_2\Delta + k$, where c_1, c_2, k are constants for $c_1, c_2 \in \mathbb{Q}$, $k \in \mathbb{Z}$ for **any** Δ, changed our world. It meant, we could reuse the effort spent in factorizing a composite n to factorize other composite numbers. In addition, the property of these Δ sieve zones to switch into different zones with changing

$dial_2$ gave us another powerful instrument in the toolchain. We now have two tools with wonderful ability and flexibility to be executed in parallel and using only fundamental arithmetic operations to sieve the Δ

In our almost decade long search, the first ray of hope came in the form of observing one $a\Delta$ relationship, but it was $ro\{X,Y\}$ which gave us the required motivation to continue with the pursuit, as we took the pulsating "As" as some form of sign from the nature.

There is tremendous life philosophy in Δ sieve zones, if one looked at them with that lens. We could see how nature is trying to communicate with us through numbers and saying, once we know and acknowledge the difference(s), either with others or with ourselves, the chaos ends and we attain the steady state.

Finally, it was the equilibrium of $\Delta_{|p-q|} \rightleftharpoons \sum_{p+q}$ which took us back in time, some 13.8 billion years ago, right at that "moment", and gave us some insights and ideas on what might have had happened and helped us in providing an explanation of where all the antimatter disappeared. This research started by taking inspiration from Physics and it was the payback time. We had to make an assumption, a mighty one, but not an absurd one, an assumption which some of us may be able to relate to. What iff, there was a multiplicative force and under its influence, two antimatter particles ended up creating the matter, like when we multiply two negative numbers and we get a positive number? So, while we are searching for antimatter all around us and not able to find much, Sherlock says, we are not able to find it because the matter we see today was made from antimatter. The actual matter is somewhere else, the real one, the one which doesn't obey the laws of observable "antimatter" universe ... now this is getting absurd!

11.1 Applications

1. **Integer Factorization**

   (a) With appropriate selection of dials and observation decks leading to sufficient number of Δ sieve zones, one can factorize the composite n, as described in section 4 - "Steady State Value" and is a general purpose factorization method

   (b) ro{X,Y} is also a general purpose factorization method and will lead to nontrivial factorization of the composite n, as described in subsection 5.3 - "Reflection over {X,Y}"

   (c) $a\Delta$ relationships are special purpose and in certain instances will lead to nontrivial factorization of the composite n, as described in subsection 5.1 - "od connect" and subsection 5.2 - "Range of previous/next n"

   (d) $r\Delta$ relationships are also special purpose and in certain instances will lead to nontrivial factorization of the composite n, as described in section 6 - "Inter Δ relationships (rΔ)"

(e) When some $\Delta \rightleftharpoons \sum$ constant is added to od_6 on the Δ series and if it yields N on the corresponding $\sum$ series, then this will lead to nontrivial factorization of the composite n, as described in section 8 - "The equilibrium of $\Delta_{|p-q|}$ and $\sum_{p+q}$"

2. **RSA Strengthening**
When the composite n is obtained from two random primes, we may need to make sure this random n is RSA-safe by passing it through the factorization methods discussed in this paper to eliminate the possibility of nontrivial factorization, thereby leading to strengthening of RSA

3. **RSA - Master Key** ($known\ \Delta \simeq unknown\{\Delta_1, \Delta_2, \Delta_3, ..., \Delta_x\}$)
$r\Delta$ (with known Δ and unknown Δs) allows for creation of an RSA-master key in form of known Δ, as described in section 6 - "Inter Δ relationships (rΔ)". Information about dials and observation deck sieve formulae will be part of the private key.

   (a) The RSA master key is likely to have a smaller private key footprint when a message is cyclically encrypted many times over with different public keys

   (b) Different public keys can be used to encrypt the message which can be decrypted with the same private key as long as they are linked with the same known Δ

4. **The New Trapdoor**
Section 9 - "The Trapdoor", introduces a new trapdoor function. The $\Delta \rightleftharpoons \sum$ equilibrium provides the foundational framework to build message encryption/decryption schemes, digital signatures and authentication schemes.

11.2 Further Research

There are some questions at this point that requires further research.

1. By having as many fixed dials and observation decks as required, which can yield the required number of Δ sieve zones and <u>without</u> changing $dial_2$, will we able to sieve any Δ in polynomial time?

2. By having as many fixed dials and observation decks as required, which can yield the required number of Δ sieve zones and <u>with</u> changing $dial_2$, will we able to sieve any Δ in polynomial time?

3. Will the composite n, calculated from two large random primes p and q, used in RSA be required to calculate a safety index to confirm whether it is safe from factorization by different factorization methods presented in this paper?

4. When different semiprimes are calculated by multiplying two large random primes p and q in RSA, what Δ sieve zones do these semiprimes are found for their respective Δs? Is there a pattern to randomness, whereby the probability for certain kind of Δ sieve zones to appear is higher than the others?

5. Can there be an equivalent quantum algorithm for methods described in this paper? If yes, will it require less or more qubits in comparison to Shor's algorithm [2] for integer factorization?

6. Will there always be some dial settings that will yield $zone_0$ in any observation deck? Note: $zone_0$ is the zone where Δ can be sieved and will continue until ∞

7. What is the angle of reflection on rising or falling edge of intra-A or inter-A to observe a nontrivial reflection? Does it fall within any range? and whether knowing this angle of reflection provide any advantage in the nontrivial factorization of the composite n?

8. What are the different counting functions looking like?

   (a) Number of $zones$ for any Δ?

   (b) Number of $zoners$ and $zoneless$ for any Δ and for all possible $dial$ combinations?

   (c) How many different $dial_1$ combinations exists such that the Δ sieve coverage zones doesn't change with changing $dial_2$ for any Δ?

9. Can we find similar patterns emerge when we apply the ideas in this paper to discrete logarithms?

10. Can lattices be used in anyway to further speed-up the search of Δ sieve zones?

Acknowledgements

To Phadnis sir, our beloved maths teacher and his never ending passion and excitement for the subject.

To Papa Dinesh, our anchor, our life force, the only one we know who never stopped learning, never stopped dreaming and never stopped believing in the force of life. To Mumma Jyotsna, our solace in solar flare, our comforter in chilling winter, our life coach from many lifetimes. To Didi Shveta, the courageous torchbearer of the family and our partner and co-conspirator on many theories about observable universe and beyond.

To Divya, my heat shield, my springboard, the one who has been the witness of all and the breeze of calm amidst chaos. To Arjun, whose arrival resulted in the manifestation of a dream from a very long time or may be from time immemorial!

To Krishnadasji's soul invigorating voice that kept us going.

A Tables

Table 1: $\Delta_{|p-q|} = 12;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p + \Delta;\ dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	13	13	3	2	4	4	16	-9	3	12	-6	5
2	3	15	45	6	6	8	36	64	-9	19	28	10	3
3	5	17	85	9	8	10	64	100	-21	15	36	-6	5
4	7	19	133	11	10	12	100	144	-33	11	44	-22	13
5	9	21	189	13	12	14	144	196	-45	7	52	-38	21
6	11	23	253	15	14	16	196	256	-57	3	60	-54	29
7	**13**	25	325	18	18	20	324	400	-1	75	76	**74**	**35**
8	15	27	405	20	20	22	400	484	-5	79	84	**74**	**35**
...	...	...	...	...	...	...	...	...	...	...	...	**74**	**35**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**74**	**35**

Table 2: $\Delta_{|p-q|} = 22;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p + \Delta;\ dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	23	23	4	4	6	16	36	-7	13	20	6	1
...	...	...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...
8	15	37	555	23	22	24	484	576	-71	21	92	-50	27
9	17	39	663	25	24	26	576	676	-87	13	100	-74	39
10	19	41	779	27	26	28	676	784	-103	5	108	-98	51
11	**21**	43	903	30	30	32	900	1024	-3	**121**	124	118	57
12	23	45	1035	32	32	34	1024	1156	-11	**121**	132	110	53
...	...	...	...	...	...	...	...	...	...	**121**	...	...	...
∞	∞	∞	∞	...	...	...	...	...	...	**121**	...	...	...

Table 3: $\Delta_{|p-q|} = 12;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	14	28	5	4	6	16	36	-12	8	20	-4	4
2	**4**	16	64	8	8	10	64	100	0	**36**	36	36	16
3	6	18	108	10	10	12	100	144	-8	**36**	44	28	12
...	...	...	...	...	...	...	...	...	...	**36**	...	...	...
∞	∞	∞	∞	...	...	...	...	...	...	**36**	...	...	...

Table 4: $\Delta_{|p-q|} = 16;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	18	36	6	6	8	36	64	0	28	28	28	12
2	4	20	80	8	8	10	64	100	-16	20	36	4	0
3	6	22	132	11	10	12	100	144	-32	12	44	-20	12
4	8	24	192	13	12	14	144	196	-48	4	52	-44	24
5	**10**	26	260	16	16	18	256	324	-4	**64**	68	60	28
6	12	28	336	18	18	20	324	400	-12	**64**	76	52	24
...	...	...	...	...	...	...	...	...	...	**64**	...	...	...
∞	∞	∞	∞	...	...	...	...	...	...	**64**	...	...	...

Table 5: $\Delta_{|p-q|} = 22;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	24	48	6	6	8	36	64	-12	16	28	4	0
2	4	26	104	10	10	12	100	144	-4	40	44	36	16
3	6	28	168	12	12	14	144	196	-24	28	52	4	0
4	8	30	240	15	14	16	196	256	-44	16	60	-28	16
5	10	32	320	17	16	18	256	324	-64	4	68	-60	32
6	12	34	408	20	20	22	400	484	-8	76	84	68	32
7	14	36	504	22	22	24	484	576	-20	72	92	52	24
8	16	38	608	24	24	26	576	676	-32	68	100	36	16
9	18	40	720	26	26	28	676	784	-44	64	108	20	8
10	20	42	840	28	28	30	784	900	-56	60	116	4	0
11	22	44	968	31	30	32	900	1024	-68	56	124	-12	8
12	24	46	1104	33	32	34	1024	1156	-80	52	132	-28	16
13	26	48	1248	35	34	36	1156	1296	-92	48	140	-44	24
14	28	50	1400	37	36	38	1296	1444	-104	44	148	-60	32
15	30	52	1560	39	38	40	1444	1600	-116	40	156	-76	40
16	32	54	1728	41	40	42	1600	1764	-128	36	164	-92	48
17	34	56	1904	43	42	44	1764	1936	-140	32	172	-108	56
18	36	58	2088	45	44	46	1936	2116	-152	28	180	-124	64
19	38	60	2280	47	46	48	2116	2304	-164	24	188	-140	72
20	40	62	2480	49	48	50	2304	2500	-176	20	196	-156	80
21	42	64	2688	51	50	52	2500	2704	-188	16	204	-172	88
22	44	66	2904	53	52	54	2704	2916	-200	12	212	-188	96
23	46	68	3128	55	54	56	2916	3136	-212	8	220	-204	104
24	48	70	3360	57	56	58	3136	3364	-224	4	228	-220	112
25	**50**	72	3600	60	60	62	3600	3844	0	244	244	**244**	**120**
26	52	74	3848	62	62	64	3844	4096	-4	248	252	**244**	**120**
...	...	...	...	...	...	...	...	...	...	...	...	**244**	**120**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**244**	**120**

Table 6: $\Delta_{|p-q|} = 24;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p+\Delta;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	25	25	5	5	7	25	49	0	24	24	24	10
2	3	27	81	9	9	11	81	121	0	40	40	40	18
3	5	29	145	12	11	13	121	169	-24	24	48	0	2
4	7	31	217	14	13	15	169	225	-48	8	56	-40	22
5	9	33	297	17	17	19	289	361	-8	64	72	56	26
6	11	35	385	19	19	21	361	441	-24	56	80	32	14
7	13	37	481	21	21	23	441	529	-40	48	88	8	2
8	15	39	585	24	23	25	529	625	-56	40	96	-16	10
9	17	41	697	26	25	27	625	729	-72	32	104	-40	22
10	19	43	817	28	27	29	729	841	-88	24	112	-64	34
11	21	45	945	30	29	31	841	961	-104	16	120	-88	46
12	23	47	1081	32	31	33	961	1089	-120	8	128	-112	58
13	**25**	49	1225	35	35	37	1225	1369	0	**144**	144	144	70
14	27	51	1377	37	37	39	1369	1521	-8	**144**	152	136	66
...	...	...	...	...	...	...	...	...	...	**144**	...	...	...
∞	∞	∞	∞	...	...	...	...	...	...	**144**	...	...	...

Table 7: $\Delta_{|p-q|} = 12;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p+\Delta;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	13	13	3	3	5	9	25	-4	12	16	8	2
2	3	15	45	6	5	7	25	49	-20	4	24	-16	10
3	**5**	17	85	9	9	11	81	121	-4	**36**	40	32	14
4	7	19	133	11	11	13	121	169	-12	**36**	48	24	10
...	...	...	...	...	...	...	...	...	...	**36**	...	...	...
∞	∞	∞	∞	...	...	...	...	...	...	**36**	...	...	...

Table 8: $\Delta_{|p-q|} = 22;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p + \Delta;\ dial_P = \{-1, 0, 2, 2\}$

-1	0
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	23	23	4	3	5	9	25	-14	2	16	-12	8
2	3	25	75	8	7	9	49	81	-26	6	32	-20	12
3	5	27	135	11	11	13	121	169	-14	34	48	20	8
4	7	29	203	14	13	15	169	225	-34	22	56	-12	8
5	9	31	279	16	15	17	225	289	-54	10	64	-44	24
6	11	33	363	19	19	21	361	441	-2	78	80	76	36
7	13	35	455	21	21	23	441	529	-14	74	88	60	28
8	15	37	555	23	23	25	529	625	-26	70	96	44	20
9	17	39	663	25	25	27	625	729	-38	66	104	28	12
10	19	41	779	27	27	29	729	841	-50	62	112	12	4
11	21	43	903	30	29	31	841	961	-62	58	120	-4	4
12	23	45	1035	32	31	33	961	1089	-74	54	128	-20	12
13	25	47	1175	34	33	35	1089	1225	-86	50	136	-36	20
14	27	49	1323	36	35	37	1225	1369	-98	46	144	-52	28
15	29	51	1479	38	37	39	1369	1521	-110	42	152	-68	36
16	31	53	1643	40	39	41	1521	1681	-122	38	160	-84	44
17	33	55	1815	42	41	43	1681	1849	-134	34	168	-100	52
18	35	57	1995	44	43	45	1849	2025	-146	30	176	-116	60
19	37	59	2183	46	45	47	2025	2209	-158	26	184	-132	68
20	39	61	2379	48	47	49	2209	2401	-170	22	192	-148	76
21	41	63	2583	50	49	51	2401	2601	-182	18	200	-164	84
22	43	65	2795	52	51	53	2601	2809	-194	14	208	-180	92
23	45	67	3015	54	53	55	2809	3025	-206	10	216	-196	100
24	47	69	3243	56	55	57	3025	3249	-218	6	224	-212	108
25	49	71	3479	58	57	59	3249	3481	-230	2	232	-228	116
26	**51**	73	3723	61	61	63	3721	3969	-2	246	248	**244**	**120**
27	53	75	3975	63	63	65	3969	4225	-6	250	256	**244**	**120**
...	...	...	...	...	...	...	...	...	...	...	...	**244**	**120**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**244**	**120**

Table 9: $\Delta_{|p-q|} = 12;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	14	28	5	5	7	25	49	-3	21	24	18	7
2	4	16	64	8	7	9	49	81	-15	17	32	2	1
3	6	18	108	10	9	11	81	121	-27	13	40	-14	9
4	8	20	160	12	11	13	121	169	-39	9	48	-30	17
5	10	22	220	14	13	15	169	225	-51	5	56	-46	25
6	12	24	288	16	15	17	225	289	-63	1	64	-62	33
7	**14**	26	364	19	19	21	361	441	-3	77	80	**74**	**35**
8	16	28	448	21	21	23	441	529	-7	81	88	**74**	**35**
...	...	...	...	...	...	...	...	...	...	...	...	**74**	**35**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**74**	**35**

Table 10: $\Delta_{|p-q|} = 22;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	24	48	6	5	7	25	49	-23	1	24	-22	13
2	4	26	104	10	9	11	81	121	-23	17	40	-6	5
3	6	28	168	12	11	13	121	169	-47	1	48	-46	25
4	8	30	240	15	15	17	225	289	-15	49	64	34	15
5	10	32	320	17	17	19	289	361	-31	41	72	10	3
6	12	34	408	20	19	21	361	441	-47	33	80	-14	9
7	14	36	504	22	21	23	441	529	-63	25	88	-38	21
8	16	38	608	24	23	25	529	625	-79	17	96	-62	33
9	18	40	720	26	25	27	625	729	-95	9	104	-86	45
10	20	42	840	28	27	29	729	841	-111	1	112	-110	57
11	**22**	44	968	31	31	33	961	1089	-7	**121**	128	114	55
12	24	46	1104	33	33	35	1089	1225	-15	**121**	136	106	51
...	...	...	...	...	...	...	...	...	...	**121**	...	...	...
∞	∞	∞	∞	...	...	...	...	...	...	**121**	...	...	...

Table 11: $\Delta_{|p-q|} = 12$; $p = 2j+1$, $j \in \mathbb{N}_0$; $q = p + \Delta$; $dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	1	13	13	-9	0	3	0	12	0	-6	0	...
2	3	15	45	-9	0	19	-16	28	-16	10	-16	...
3	5	17	85	-21	12	15	4	36	-8	-6	16	...
4	7	19	133	-33	12	11	4	44	-8	-22	16	...
5	9	21	189	-45	12	7	4	52	-8	-38	16	...
6	11	23	253	-57	12	3	4	60	-8	-54	16	...
7	13	25	325	-1	**-56**	75	**-72**	76	-16	**74**	**-128**	**0**
8	15	27	405	-5	**4**	79	**-4**	84	-8	**74**	**0**	**0**
9	17	29	493	-9	**4**	83	**-4**	92	-8	**74**	**0**	**0**
10	19	31	589	-13	**4**	87	**-4**	100	-8	**74**	**0**	**0**
11	21	33	693	-17	**4**	91	**-4**	108	-8	**74**	**0**	**0**
12	23	35	805	-21	**4**	95	**-4**	116	-8	**74**	**0**	**0**
13	25	37	925	-25	**4**	99	**-4**	124	-8	**74**	**0**	**0**
14	27	39	1053	-29	**4**	103	**-4**	132	-8	**74**	**0**	**0**
...	...	...	...	...	**4**	...	**-4**	...	...	**74**	**0**	**0**
∞	∞	∞	∞	...	**4**	...	**-4**	...	...	**74**	**0**	**0**

Table 12: $\Delta_{|p-q|} = 22;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{0, -1, 2, 2\}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	2	24	48	-12	0	16	0	28	0	4	0	...
2	4	26	104	-4	-8	40	-24	44	-16	36	-32	...
3	6	28	168	-24	20	28	12	52	-8	4	32	...
4	8	30	240	-44	20	16	12	60	-8	-28	32	...
5	10	32	320	-64	20	4	12	68	-8	-60	32	...
6	12	34	408	-8	-56	76	-72	84	-16	68	-128	...
7	14	36	504	-20	12	72	4	92	-8	52	16	...
8	16	38	608	-32	12	68	4	100	-8	36	16	...
9	18	40	720	-44	12	64	4	108	-8	20	16	...
...	...	...	...	...	...	...	...	...	...	...	...	...
23	46	68	3128	-212	12	8	4	220	-8	-204	16	...
24	48	70	3360	-224	12	4	4	228	-8	-220	16	...
25	50	72	3600	0	**-224**	244	**-240**	244	-16	**244**	**-464**	**0**
26	52	74	3848	-4	**4**	248	**-4**	252	-8	**244**	**0**	**0**
27	54	76	4104	-8	**4**	252	**-4**	260	-8	**244**	**0**	**0**
28	56	78	4368	-12	**4**	256	**-4**	268	-8	**244**	**0**	**0**
29	58	80	4640	-16	**4**	260	**-4**	276	-8	**244**	**0**	**0**
...	...	...	...	...	**4**	...	**-4**	...	...	**244**	**0**	**0**
∞	∞	∞	∞	...	**4**	...	**-4**	...	...	**244**	**0**	**0**

Table 13: $\Delta_{|p-q|} = 22;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p+\Delta;\ dial_P = \{-1,0,2,2\}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	1	23	23	-14	0	2	0	16	0	-12	0	...
2	3	25	75	-26	12	6	-4	32	-16	-20	8	...
3	5	27	135	-14	-12	34	-28	48	-16	20	-40	...
4	7	29	203	-34	20	22	12	56	-8	-12	32	...
5	9	31	279	-54	20	10	12	64	-8	-44	32	...
6	11	33	363	-2	-52	78	-68	80	-16	76	-120	...
7	13	35	455	-14	12	74	4	88	-8	60	16	...
8	15	37	555	-26	12	70	4	96	-8	44	16	...
9	17	39	663	-38	12	66	4	104	-8	28	16	...
...	...	...	...	...	...	...	...	...	...	...	...	...
17	33	55	1815	-134	12	34	4	168	-8	-100	16	...
18	35	57	1995	-146	12	30	4	176	-8	-116	16	...
19	37	59	2183	-158	12	26	4	184	-8	-132	16	...
20	39	61	2379	-170	12	22	4	192	-8	-148	16	...
21	41	63	2583	-182	12	18	4	200	-8	-164	16	...
22	43	65	2795	-194	12	14	4	208	-8	-180	16	...
23	45	67	3015	-206	12	10	4	216	-8	-196	16	...
24	47	69	3243	-218	12	6	4	224	-8	-212	16	...
25	49	71	3479	-230	12	2	4	232	-8	-228	16	...
26	51	73	3723	-2	**-228**	246	**-244**	248	-16	**244**	**-472**	**0**
27	53	75	3975	-6	**4**	250	**-4**	256	-8	**244**	**0**	**0**
28	55	77	4235	-10	**4**	254	**-4**	264	-8	**244**	**0**	**0**
29	57	79	4503	-14	**4**	258	**-4**	272	-8	**244**	**0**	**0**
30	59	81	4779	-18	**4**	262	**-4**	280	-8	**244**	**0**	**0**
...	...	...	...	...	**4**	...	**-4**	...	...	**244**	**0**	**0**
∞	∞	∞	∞	...	**4**	...	**-4**	...	...	**244**	**0**	**0**

Table 14: $\Delta_{|p-q|} = 12;\ p = 2j,\ j \in \mathbb{N};\ q = p + \Delta;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	2	14	28	-3	0	21	0	24	0	18	0	...
2	4	16	64	-15	12	17	4	32	-8	2	16	...
3	6	18	108	-27	12	13	4	40	-8	-14	16	...
4	8	20	160	-39	12	9	4	48	-8	-30	16	...
5	10	22	220	-51	12	5	4	56	-8	-46	16	...
6	12	24	288	-63	12	1	4	64	-8	-62	16	...
7	14	26	364	-3	**-60**	77	**-76**	80	-16	**74**	**-136**	**0**
8	16	28	448	-7	**4**	81	**-4**	88	-8	**74**	**0**	**0**
9	18	30	540	-11	**4**	85	**-4**	96	-8	**74**	**0**	**0**
10	20	32	640	-15	**4**	89	**-4**	104	-8	**74**	**0**	**0**
11	22	34	748	-19	**4**	93	**-4**	112	-8	**74**	**0**	**0**
...	...	...	...	...	**4**	...	**-4**	...	...	**74**	**0**	**0**
∞	∞	∞	∞	...	**4**	...	**-4**	...	...	**74**	**0**	**0**

Table 15: $\Delta_{|p-q|} = 46;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p + \Delta;\ dial_P = \{-1, -2, 4, 4\}$

-1	-2	*dial settings*
4	4	

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5
1	1	47	47	-22	0	34	0	56	0	12	0	80
2	3	49	147	-26	4	78	-44	104	-48	52	-40	208
3	5	51	255	-86	60	34	44	120	-16	-52	104	16
4	7	53	371	-82	-4	70	-36	152	-32	-12	-40	128
5	9	55	495	-54	-28	130	-60	184	-32	76	-88	336
6	11	57	627	-98	44	102	28	200	-16	4	72	208
7	13	59	767	-142	44	74	28	216	-16	-68	72	80
8	15	61	915	-74	-68	174	-100	248	-32	100	-168	448
9	17	63	1071	-110	36	154	20	264	-16	44	56	352
10	19	65	1235	-146	36	134	20	280	-16	-12	56	256
...	...	...	...	...	...	...	...	...	...	...	...	...
54	107	153	16371	-746	20	270	4	1016	-16	-476	24	64
55	109	155	16895	-766	20	266	4	1032	-16	-500	24	32
56	111	157	17427	-266	**-500**	798	**-532**	1064	**-32**	532	**-1032**	**2128**
57	113	159	17967	-278	**12**	802	**-4**	1080	**-16**	524	**8**	**2128**
58	115	161	18515	-290	**12**	806	**-4**	1096	**-16**	516	**8**	**2128**
59	117	163	19071	-302	**12**	810	**-4**	1112	**-16**	508	**8**	**2128**
60	119	165	19635	-314	**12**	814	**-4**	1128	**-16**	500	**8**	**2128**
...	...	...	...	...	...	...	...	...	...	...	...	**2128**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**2128**

Table 16: $\Delta_{|p-q|} = 48;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p+\Delta;\ dial_P = \{-2,-1,4,4\}$

-2	-1	
4	4	*dial settings*

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5
1	1	49	49	-13	0	51	0	64	0	38	0	140
2	3	51	153	-53	40	43	8	96	-32	-10	48	76
3	5	53	265	-69	16	59	-16	128	-32	-10	0	108
4	7	55	385	-61	-8	99	-40	160	-32	38	-48	236
5	9	57	513	-113	52	63	36	176	-16	-50	88	76
6	11	59	649	-73	-40	135	-72	208	-32	62	-112	332
7	13	61	793	-117	44	107	28	224	-16	-10	72	204
8	15	63	945	-161	44	79	28	240	-16	-82	72	76
9	17	65	1105	-81	-80	191	-112	272	-32	110	-192	492
10	19	67	1273	-117	36	171	20	288	-16	54	56	396
...	...	...	...	...	...	...	...	...	...	...	...	...
57	113	161	18193	-769	20	303	4	1072	-16	-466	24	140
58	115	163	18745	-789	20	299	4	1088	-16	-490	24	108
59	117	165	19305	-809	20	295	4	1104	-16	-514	24	76
60	119	167	19873	-829	20	291	4	1120	-16	-538	24	44
61	121	169	20449	-285	**-544**	867	**-576**	1152	**-32**	582	**-1120**	**2316**
62	123	171	21033	-297	**12**	871	**-4**	1168	**-16**	574	**8**	**2316**
63	125	173	21625	-309	**12**	875	**-4**	1184	**-16**	566	**8**	**2316**
64	127	175	22225	-321	**12**	879	**-4**	1200	**-16**	558	**8**	**2316**
65	129	177	22833	-333	**12**	883	**-4**	1216	**-16**	550	**8**	**2316**
...	...	...	...	...	...	...	...	...	...	...	...	**2316**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**2316**

Table 17: $\Delta_{|p-q|} = 22;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p+\Delta;\ dial_P = \{-1,0,6,6\}$

-1	0
6	6

dial settings

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	1	23	23	-14	0	58	0	72	0	44	0	...
2	3	25	75	-26	12	94	-36	120	-48	68	-24	...
3	5	27	135	-14	-12	154	-60	168	-48	140	-72	...
4	7	29	203	-34	20	158	-4	192	-24	124	16	...
5	9	31	279	-54	20	162	-4	216	-24	108	16	...
6	11	33	363	-2	-52	262	-100	264	-48	**260**	**-152**	**1**
7	13	35	455	-14	12	274	-12	288	-24	**260**	**0**	**1**
8	15	37	555	-26	12	286	-12	312	-24	**260**	**0**	**1**
9	17	39	663	-38	12	298	-12	336	-24	**260**	**0**	**1**
10	19	41	779	-50	12	310	-12	360	-24	**260**	**0**	**1**
11	21	43	903	-62	12	322	-12	384	-24	**260**	**0**	**1**
12	23	45	1035	-74	12	334	-12	408	-24	**260**	**0**	**1**
13	25	47	1175	-86	12	346	-12	432	-24	**260**	**0**	**1**
14	27	49	1323	-98	12	358	-12	456	-24	**260**	**0**	**1**
15	29	51	1479	-110	12	370	-12	480	-24	**260**	**0**	**1**
16	31	53	1643	-122	12	382	-12	504	-24	**260**	**0**	**1**
17	33	55	1815	-134	12	394	-12	528	-24	**260**	**0**	**1**
18	35	57	1995	-146	12	406	-12	552	-24	**260**	**0**	**1**
19	37	59	2183	-158	12	418	-12	576	-24	**260**	**0**	**1**
20	39	61	2379	-170	12	430	-12	600	-24	**260**	**0**	**1**
21	41	63	2583	-182	12	442	-12	624	-24	**260**	**0**	**1**
22	43	65	2795	-194	12	454	-12	648	-24	**260**	**0**	**1**
23	45	67	3015	-206	12	466	-12	672	-24	**260**	**0**	**1**
24	47	69	3243	-218	12	478	-12	696	-24	**260**	**0**	**1**
25	49	71	3479	-230	12	490	-12	720	-24	**260**	**0**	**1**
26	51	73	3723	-2	-228	766	-276	768	-48	764	-504	...
27	53	75	3975	-6	4	786	-20	792	-24	780	-16	...
...	...	...	...	...	...	...	...	...	...	...	...	...

Table 18: $\Delta_{|p-q|} = 46$; $p = 2j+1,\ j \in \mathbb{N}_0$; $q = p + \Delta$; $dial_P = \{-1, -2, 12, 12\}$

-1	-2	*dial settings*
12	12	

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5	$zone$
1	1	47	47	-22	0	242	0	264	0	220	0	704	...
2	3	49	147	-26	4	382	-140	408	-144	356	-136	1120	...
3	5	51	255	-86	60	370	12	456	-48	284	72	1024	...
4	7	53	371	-82	-4	470	-100	552	-96	388	-104	1328	...
5	9	55	495	-54	-28	594	-124	648	-96	540	-152	1728	...
6	11	57	627	-98	44	598	-4	696	-48	500	40	1696	...
7	13	59	767	-142	44	602	-4	744	-48	460	40	1664	...
8	15	61	915	-74	**-68**	766	**-164**	840	**-96**	692	**-232**	**2224**	**1**
9	17	63	1071	-110	**36**	778	**-12**	888	**-48**	668	**24**	**2224**	**1**
10	19	65	1235	-146	**36**	790	**-12**	936	**-48**	644	**24**	**2224**	**1**
11	21	67	1407	-182	**36**	802	**-12**	984	**-48**	620	**24**	**2224**	**1**
12	23	69	1587	-218	**36**	814	**-12**	1032	**-48**	596	**24**	**2224**	**1**
13	25	71	1775	-94	-124	1034	-220	1128	-96	940	-344	3008	...
14	27	73	1971	-122	28	1054	-20	1176	-48	932	8	3040	...
15	29	75	2175	-150	28	1074	-20	1224	-48	924	8	3072	...
16	31	77	2387	-178	28	1094	-20	1272	-48	916	8	3104	...
17	33	79	2607	-206	28	1114	-20	1320	-48	908	8	3136	...
18	35	81	2835	-234	28	1134	-20	1368	-48	900	8	3168	...
19	37	83	3071	-262	28	1154	-20	1416	-48	892	8	3200	...
20	39	85	3315	-290	28	1174	-20	1464	-48	884	8	3232	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...

Table 19: Δ sieve coverage e.g. with $\Delta = 160$

od_x	id start	id end	Δ sieve coverage	steady state value	equation reference
od_2	79	86	8	6400	(9)
od_4	163	190	28	12872	(12)
od_5	191	228	38	25708	(13)
od_1	761	1560	800	6400	(9)

Table 20: Δ sieve coverage e.g. with $\Delta = 480$

od_x	id start	id end	Δ sieve coverage	steady state value	equation reference
od_2	913	991	78	57600	(9)
od_4	1683	1939	256	115272	(12)
od_5	1940	2281	341	230508	(13)
od_1	7081	14280	7199	57600	(9)

Table 21: Δ sieve zones and coverage with two dials

od_x	id start	id end	Δ sieve coverage	steady state value	equation reference
od_8	14	15	2	2209	(9)
od_8	20	22	3	2209	(9)
od_{9a}	30	34	5	4490	(14)
od_{9b}	35	40	6	4450	(15)
od_{11}	49	57	9	11189	(17)
od_{10}	58	70	13	6795	(16)
od_7	530	∞	$530-\infty$	2209	(9)

Table 22: $\Delta_{\|p-q\|}=22;\ p=2j+1,\ j\in\mathbb{N}_0;\ q=p+\Delta;\ dial_P=\{-1,0,6,6\}$

-1	0
6	6

dial settings

id	p	q	$n=pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	1	23	23	-14	0	58	0	72	0	44	0	...
2	3	25	75	-26	12	94	-36	120	-48	68	-24	...
3	5	27	135	-14	-12	154	-60	168	-48	140	-72	...
4	7	29	203	-34	20	158	-4	192	-24	124	16	...
5	9	31	279	-54	20	162	-4	216	-24	108	16	...
6	**11**	**33**	**363**	**-2**	**-52**	**262**	**-100**	**264**	**-48**	**260**	**-152**	**1**
7	13	35	455	-14	12	274	-12	288	-24	260	0	1
8	15	37	555	-26	12	286	-12	312	-24	260	0	1
...	...	...	...	...	...	...	...	...	...	...		

Table 23: $\Delta_{\|p-q\|}=22;\ p=2j+1,\ j\in\mathbb{N}_0;\ q=p+\Delta;\ dial_P=\{-1,0,4,4\}$

-1	0
4	4

dial settings

id	p	q	$n=pq$	od_1	od_2	od_3	od_4	od_5	df_5	$zone$
1	1	23	23	-14	26	40	12	64	0	...
2	3	25	75	-26	46	72	20	112	-48	...
3	5	27	135	-14	90	104	76	256	-144	...
4	7	29	203	-34	86	120	52	224	32	...
5	9	31	279	-54	82	136	28	192	32	...
6	**11**	**33**	**363**	**-2**	**166**	**168**	**164**	**496**	**-304**	**0**
7	13	35	455	-14	170	184	156	496	0	0
...	...	...	...	...	...	...	...	...	...	...

Table 24: $\Delta_{|p-q|} = 22;\ p = 2j+1,\ j \in \mathbb{N}_0;\ q = p + \Delta;\ dial_P = \{-1, 0, 6, 6\}$

-1	0
6	6

dial settings

id	p	q	$n=pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	$zone$
1	1	23	23	-14	0	58	0	72	0	44	0	...
2	**3**	**25**	**75**	**-26**	**12**	**94**	**-36**	**120**	**-48**	**68**	**-24**	**...**
3	**5**	**27**	**135**	**-14**	**-12**	**154**	**-60**	**168**	**-48**	**140**	**-72**	**...**
4	7	29	203	-34	20	158	-4	192	-24	124	16	...
5	9	31	279	-54	20	162	-4	216	-24	108	16	...
6	**11**	**33**	**363**	**-2**	**-52**	**262**	**-100**	**264**	**-48**	**260**	**-152**	**1**
7	13	35	455	-14	12	274	-12	288	-24	260	0	1
8	15	37	555	-26	12	286	-12	312	-24	260	0	1
...	...	...	...	...	...	...	...	...	...	...		

Table 25: $\Delta_{|p-q|} = 540$

0	-1
2	2

dial settings

id	p	q	$n=pq$	d_1	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4
1	1	541	541	22	-57	0	35	0	92	0	-22	0
...	...	...	...	...	...	...	...	...	...	...	...	...
136	271	811	**219781**	**468**	**-757**	292	**1119**	284	**1876**	-8	**362**	576
137	273	813	221949	470	-1049	292	835	284	1884	-8	-214	576
...	...	...	...	...	...	...	...	...	...	...	...	...

Table 26: $\Delta_{|p-q|} = 22$

-1	0
2	2

dial settings

id	p	q	$n=pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	23	23	4	3	5	9	25	-14	2	16	-12	8
...	...	...	...	...	...	...	...	...	...	...	...	...	...
13	25	47	1175	34	33	35	1089	1225	-86	50	136	-36	20
14	27	49	1323	36	**35**	37	1225	1369	-98	46	144	-52	28
15	29	51	1479	38	**37**	39	1369	1521	-110	42	152	-68	36
16	31	53	**1643**	40	**39**	41	1521	1681	**-122**	38	160	-84	44
17	33	55	1815	42	**41**	43	1681	1849	-134	34	168	-100	52
18	35	57	1995	44	**43**	45	1849	2025	-146	30	176	-116	60
19	37	59	2183	46	45	47	2025	2209	-158	26	184	-132	68
20	39	61	2379	48	47	49	2209	2401	-170	22	192	-148	76
∞	∞	∞	∞	...	...	...	...	...	...	...	...	244	120

Table 27: $\Delta_{|p-q|} = 22$

-1	0
2	2

dial settings

id	p	q	$n=pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	23	23	4	3	5	9	25	-14	2	16	-12	8
2	3	25	75	8	7	9	49	81	-26	6	32	-20	12
3	5	27	135	11	11	13	121	169	-14	34	48	20	8
4	7	29	203	14	13	15	169	225	-34	22	56	-12	8
5	9	31	279	16	15	17	225	289	-54	10	64	-44	24
6	11	33	363	19	19	21	361	441	-2	78	80	76	**36**
7	13	35	455	21	21	23	441	529	-14	74	88	60	**28**
8	15	37	555	23	23	25	529	625	-26	70	96	44	**20**
9	17	39	663	25	25	27	625	729	-38	66	104	28	**12**
10	19	41	779	27	27	29	729	841	-50	62	112	12	**4**
11	21	43	903	30	29	31	841	961	-62	58	120	-4	**4**
12	23	45	1035	32	31	33	961	1089	-74	54	128	-20	**12**
13	25	47	1175	34	33	35	1089	1225	-86	50	136	-36	**20**
14	27	49	1323	36	35	37	1225	1369	-98	46	144	-52	**28**
15	29	51	1479	38	37	39	1369	1521	-110	42	152	-68	**36**
16	31	53	1643	40	39	41	1521	1681	-122	38	160	-84	44
...	...	...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	244	120
∞	∞	∞	∞	...	...	...	...	...	...	...	...	244	120

Table 28: $\Delta_{|p-q|} = 20$

0	-1
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	21	21	4	4	6	16	36	-5	15	20	10	3
2	3	23	69	8	8	10	64	100	-5	31	36	26	11
3	5	25	125	11	10	12	100	144	-25	19	44	-6	5
4	7	27	189	13	12	14	144	196	-45	7	52	-38	21
5	9	29	261	16	16	18	256	324	-5	63	68	58	**27**
6	11	31	341	18	18	20	324	400	-17	59	76	42	**19**
7	13	33	429	20	20	22	400	484	-29	55	84	26	**11**
8	15	35	525	22	22	24	484	576	-41	51	92	10	**3**
9	17	37	629	25	24	26	576	676	-53	47	100	-6	**5**
10	19	39	741	27	26	28	676	784	-65	43	108	-22	**13**
11	21	41	861	29	28	30	784	900	-77	39	116	-38	**21**
12	23	43	989	31	30	32	900	1024	-89	35	124	-54	**29**
13	25	45	1125	33	32	34	1024	1156	-101	31	132	-70	37
...	...	...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	202	99
∞	∞	∞	∞	...	...	...	...	...	...	...	...	202	99

Table 29: $r\Delta$ example

known Δ	id	$dial_P$	Δ sieve value	od_x
122	93	{0, -1, 8, 8}	3721	od_2

Unknown Δ	n	$dial_P$	Δ sieve value	od_x
162	$n1$	{0, -1, 8, 8}	13154	od_4
178	$n2$	{0, -1, 8, 8}	31732	od_5
202	$n3$	{0, -1, 8, 8}	10201	od_2

Table 30: $\sum_{p+q} = 22;\ p = 2j+1$ for $j \in \mathbb{N}_0;\ q = \sum - p;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$N = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	21	21	4	3	5	9	25	-12	4	16	-8	6
2	3	19	57	7	7	9	49	81	-8	24	32	16	6
3	5	17	85	9	9	11	81	121	-4	36	40	32	14
4	7	15	105	10	9	11	81	121	-24	16	40	-8	6
5	9	13	117	10	9	11	81	121	-36	4	40	-32	18
6	11	11	121	11	11	13	121	169	0	48	48	48	22
7	13	9	117	10	9	11	81	121	-36	4	40	-32	18
8	15	7	105	10	9	11	81	121	-24	16	40	-8	6
9	17	5	85	9	9	11	81	121	-4	36	40	32	14
10	19	3	57	7	7	9	49	81	-8	24	32	16	6
11	21	1	21	4	3	5	9	25	-12	4	16	-8	6

Table 31: $\sum_{p+q} = 20;\ p = 2j+1$ for $j \in \mathbb{N}_0;\ q = \sum - p;\ dial_P = \{-1, 0, 2, 2\}$

-1	0	*dial settings*
2	2	

id	p	q	$N = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	19	19	4	3	5	9	25	-10	6	16	-4	4
2	3	17	51	7	7	9	49	81	-2	30	32	28	12
3	5	15	75	8	7	9	49	81	-26	6	32	-20	12
4	7	13	91	9	9	11	81	121	-10	30	40	20	8
5	9	11	99	9	9	11	81	121	-18	22	40	4	0
6	11	9	99	9	9	11	81	121	-18	22	40	4	0
7	13	7	91	9	9	11	81	121	-10	30	40	20	8
8	15	5	75	8	7	9	49	81	-26	6	32	-20	12
9	17	3	51	7	7	9	49	81	-2	30	32	28	12
10	19	1	19	4	3	5	9	25	-10	6	16	-4	4

Table 32: $\Delta_{|p-q|} = 20, p = 2j+1$ for $j \in \mathbb{N}$

0	-1	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	21	21	4	4	6	16	36	-5	15	20	10	3
...	...	...	...	...	...	...	...	...	...	...	...	...	...
17	33	53	1749	41	40	42	1600	1764	-149	15	164	-134	69
18	35	55	1925	43	42	44	1764	1936	-161	11	172	-150	77
19	37	57	2109	45	44	46	1936	2116	-173	7	180	-166	85
20	39	59	2301	47	46	48	2116	2304	-185	3	188	-182	93
21	41	61	2501	50	50	52	2500	2704	-1	203	204	202	**99**
22	43	63	2709	52	52	54	2704	2916	-5	207	212	202	**99**
...	...	...	...	...	...	...	...	...	...	...	...	202	**99**
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	202	**99**

Table 33: $\sum_{p+q} = 20, p = 2j+1$ for $j \in \mathbb{N}$

-1	0	*dial settings*
2	2	

id	p	q	$N = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	19	19	4	3	5	9	25	-10	6	16	-4	4
2	3	17	51	7	7	9	49	81	-2	30	32	28	12
3	5	15	75	8	7	9	49	81	-26	6	32	-20	12
4	7	13	91	9	9	11	81	121	-10	30	40	20	8
5	9	11	**99**	9	9	11	81	121	-18	22	40	4	**0**
6	11	9	**99**	9	9	11	81	121	-18	22	40	4	**0**
7	13	7	91	9	9	11	81	121	-10	30	40	20	8
8	15	5	75	8	7	9	49	81	-26	6	32	-20	12
9	17	3	51	7	7	9	49	81	-2	30	32	28	12
10	19	1	19	4	3	5	9	25	-10	6	16	-4	4
...	...	...	...	...	...	...	...	...	...	...	...	...	...

Δ	Σ	
{0,-1,2,2}	{-1,0,2,2}	*dial settings*

$N_{\Sigma_{p+q}}$	$od6_{\Delta_{\|p-q\|}}$	$\Delta \rightleftharpoons \Sigma$	$df_{\Delta\Sigma}$
99	99	0	
91	93	-2	2
75	85	-10	8
51	77	-26	16
19	69	-50	24
-21	61	-82	32
-69	53	-122	40
-125	45	-170	48
-189	37	-226	56
-261	29	-290	64

Table 34: $\Delta_{|p-q|} = \sum_{p+q} = 20$

Δ	Σ	
{0,-1,2,2}	{-1,0,2,2}	*dial settings*

$N_{\Sigma_{p+q}}$	$od6_{\Delta_{\|p-q\|}}$	$\Delta \rightleftharpoons \Sigma$	$df_{\Delta\Sigma}$
399	399	0	
391	393	-2	2
375	385	-10	8
351	377	-26	16
319	369	-50	24
279	361	-82	32
231	353	-122	40
175	345	-170	48
111	337	-226	56
39	329	-290	64

Table 35: $\Delta_{|p-q|} = \sum_{p+q} = 40$

Table 36: $\Delta_{|p=q|} = 22, p = 2j+1$ for $j \in \mathbb{N}$

-1	0	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	23	23	4	3	5	9	25	-14	2	16	-12	8
...	...	...	...	...	...	...	...	...	...	...	...	...	...
21	41	63	2583	50	49	51	2401	2601	-182	18	200	-164	84
22	43	65	2795	52	51	53	2601	2809	-194	14	208	-180	92
23	45	67	3015	54	53	55	2809	3025	-206	10	216	-196	100
24	47	69	3243	56	55	57	3025	3249	-218	6	224	-212	108
25	49	71	3479	58	57	59	3249	3481	-230	2	232	-228	116
26	51	73	3723	61	61	63	3721	3969	-2	246	248	244	**120**
27	53	75	3975	63	63	65	3969	4225	-6	250	256	244	**120**
...	...	...	...	...	...	...	...	...	...	...	...	244	**120**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	244	**120**

Table 37: $\sum_{p+q} = 22, p = 2j+1$ for $j \in \mathbb{N}$

-1	0	*dial settings*
2	2	

id	p	q	$N = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	1	21	21	4	3	5	9	25	-12	4	16	-8	6
2	3	19	57	7	7	9	49	81	-8	24	32	16	6
3	5	17	85	9	9	11	81	121	-4	36	40	32	14
4	7	15	105	10	9	11	81	121	-24	16	40	-8	6
5	9	13	117	10	9	11	81	121	-36	4	40	-32	18
6	11	11	**121**	11	11	13	121	169	**0**	48	48	48	22
7	13	9	117	10	9	11	81	121	-36	4	40	-32	18
8	15	7	105	10	9	11	81	121	-24	16	40	-8	6
9	17	5	85	9	9	11	81	121	-4	36	40	32	14
10	19	3	57	7	7	9	49	81	-8	24	32	16	6
11	21	1	21	4	3	5	9	25	-12	4	16	-8	6

Δ	Σ	
{-1,0,2,2}	{-1,0,2,2}	*dial settings*

$N_{\sum_{p+q}}$	$od6_{\Delta_{\lvert p-q \rvert}}$	$\Delta \rightleftharpoons \Sigma$	$df_{\Delta\Sigma}$
121	120	1	
117	116	1	0
105	108	-3	4
85	100	-15	12
57	92	-35	20
21	84	-63	28
-23	76	-99	36
-75	68	-143	44
-135	60	-195	52

Table 38: $\Delta_{\lvert p-q \rvert} = \sum_{p+q} = 22$

Δ	Σ	
{-1,0,2,2}	{-1,0,2,2}	*dial settings*

$N_{\sum_{p+q}}$	$od6_{\Delta_{\lvert p-q \rvert}}$	$\Delta \rightleftharpoons \Sigma$	$df_{\Delta\Sigma}$
441	440	1	
437	436	1	0
425	428	-3	4
405	420	-15	12
377	412	-35	20
341	404	-63	28
297	396	-99	36
245	388	-143	44
185	380	-195	52

Table 39: $\Delta_{\lvert p-q \rvert} = \sum_{p+q} = 42$

Table 40: $\Delta_{|p-q|} = 20, p = 2j$ for $j \in \mathbb{N}$

-1	0
2	2

dial settings

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	22	44	6	5	7	25	49	-19	5	24	-14	9
...	...	...	...	...	...	...	...	...	...	...	...	...	...
17	34	54	1836	42	41	43	1681	1849	-155	13	168	-142	73
18	36	56	2016	44	43	45	1849	2025	-167	9	176	-158	81
19	38	58	2204	46	45	47	2025	2209	-179	5	184	-174	89
20	40	60	2400	48	47	49	2209	2401	-191	1	192	-190	97
21	42	62	2604	51	51	53	2601	2809	-3	205	208	202	**99**
22	44	64	2816	53	53	55	2809	3025	-7	209	216	202	**99**
23	46	66	3036	55	55	57	3025	3249	-11	213	224	202	**99**
...	...	...	...	...	...	...	...	...	...	...	...	202	**99**
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	202	**99**

Table 41: $\sum_{p+q} = 20, p = 2j$ for $j \in \mathbb{N}$

-1	0
2	2

dial settings

id	p	q	$N = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	18	36	6	5	7	25	49	-11	13	24	2	1
2	4	16	64	8	7	9	49	81	-15	17	32	2	1
3	6	14	84	9	9	11	81	121	-3	37	40	34	15
4	8	12	96	9	9	11	81	121	-15	25	40	10	3
5	10	10	**100**	10	9	11	81	121	-19	21	40	2	1
6	12	8	96	9	9	11	81	121	-15	25	40	10	3
7	14	6	84	9	9	11	81	121	-3	37	40	34	15
8	16	4	64	8	7	9	49	81	-15	17	32	2	1
9	18	2	36	6	5	7	25	49	-11	13	24	2	1
10	20	0	0	0	-1	1	1	1	1	1	0	2	1
...	...	...	...	...	...	...	...	...	...	...	...	...	...

Table 42: $\Delta_{|p=q|} = 22, p = 2j$ for $j \in \mathbb{N}$

0	-1	*dial settings*
2	2	

id	p	q	$n = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	24	48	6	6	8	36	64	-12	16	28	4	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...
21	42	64	2688	51	50	52	2500	2704	-188	16	204	-172	88
22	44	66	2904	53	52	54	2704	2916	-200	12	212	-188	96
23	46	68	3128	55	54	56	2916	3136	-212	8	220	-204	104
24	48	70	3360	57	56	58	3136	3364	-224	4	228	-220	112
25	50	72	3600	60	60	62	3600	3844	0	244	244	244	**120**
26	52	74	3848	62	62	64	3844	4096	-4	248	252	244	**120**
27	54	76	4104	64	64	66	4096	4356	-8	252	260	244	**120**
...	...	...	...	...	...	...	...	...	...	...	...	244	**120**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	244	**120**

Table 43: $\sum_{p+q} = 22, p = 2j$ for $j \in \mathbb{N}$

-1	0	*dial settings*
2	2	

id	p	q	$N = pq$	$\lfloor\sqrt{n}\rfloor$	d_1	d_2	d_1^2	d_2^2	od_1	od_2	od_3	od_4	od_6
1	2	20	40	6	5	7	25	49	-15	9	24	-6	5
2	4	18	72	8	7	9	49	81	-23	9	32	-14	9
3	6	16	96	9	9	11	81	121	-15	25	40	10	3
4	8	14	112	10	9	11	81	121	-31	9	40	-22	13
5	10	12	**120**	10	9	11	81	121	-39	1	40	-38	21
6	12	10	**120**	10	9	11	81	121	-39	1	40	-38	21
7	14	8	112	10	9	11	81	121	-31	9	40	-22	13
8	16	6	96	9	9	11	81	121	-15	25	40	10	3
9	18	4	72	8	7	9	49	81	-23	9	32	-14	9
10	20	2	40	6	5	7	25	49	-15	9	24	-6	5
11	22	0	0	0	-1	1	1	1	1	1	0	2	1

Table 44: $\Delta_{|p-q|} = 23, p = 2j+1$ for $j \in \mathbb{N}$

-1	0
2	2

dial settings

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5
1	1	24	24	-15	0	1	0	16	0	-14	0	-12
2	3	26	78	-29	14	3	-2	32	-16	-26	12	-20
3	5	28	140	-19	-10	29	-26	48	-16	10	-36	68
4	7	30	210	-41	22	15	14	56	-8	-26	36	4
5	9	32	288	-63	22	1	14	64	-8	-62	36	-60
6	11	34	374	-13	-50	67	-66	80	-16	54	-116	188
7	13	36	468	-27	14	61	6	88	-8	34	20	156
8	15	38	570	-41	14	55	6	96	-8	14	20	124
9	17	40	680	-55	14	49	6	104	-8	-6	20	92
10	19	42	798	-69	14	43	6	112	-8	-26	20	60
11	21	44	924	-83	14	37	6	120	-8	-46	20	28
12	23	46	1058	-97	14	31	6	128	-8	-66	20	-4
13	25	48	1200	-111	14	25	6	136	-8	-86	20	-36
14	27	50	1350	-125	14	19	6	144	-8	-106	20	-68
15	29	52	1508	-139	14	13	6	152	-8	-126	20	-100
16	31	54	1674	-153	14	7	6	160	-8	-146	20	-132
17	33	56	1848	-167	14	1	6	168	-8	-166	20	-164
18	35	58	2030	-5	-162	179	-178	184	-16	174	-340	**532**
19	37	60	2220	-11	6	181	-2	192	-8	170	4	**532**
20	39	62	2418	-17	6	183	-2	200	-8	166	4	**532**
...	...	...	...	...	...	...	...	...	...	...	...	**532**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**532**

Table 45: $\Delta_{|p-q|} = 25, p = 2j+1 for j \in \mathbb{N}$

0	-1	*dial settings*
2	2	

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5
1	1	26	26	-10	0	10	0	20	0	0	0	20
2	3	28	84	-20	10	16	-6	36	-16	-4	4	28
3	5	30	150	-6	-14	46	-30	52	-16	40	-44	132
4	7	32	224	-28	22	32	14	60	-8	4	36	68
5	9	34	306	-50	22	18	14	68	-8	-32	36	4
6	11	36	396	-72	22	4	14	76	-8	-68	36	-60
7	13	38	494	-10	-62	82	-78	92	-16	72	-140	236
8	15	40	600	-24	14	76	6	100	-8	52	20	204
9	17	42	714	-38	14	70	6	108	-8	32	20	172
10	19	44	836	-52	14	64	6	116	-8	12	20	140
11	21	46	966	-66	14	58	6	124	-8	-8	20	108
12	23	48	1104	-80	14	52	6	132	-8	-28	20	76
13	25	50	1250	-94	14	46	6	140	-8	-48	20	44
14	27	52	1404	-108	14	40	6	148	-8	-68	20	12
15	29	54	1566	-122	14	34	6	156	-8	-88	20	-20
16	31	56	1736	-136	14	28	6	164	-8	-108	20	-52
17	33	58	1914	-150	14	22	6	172	-8	-128	20	-84
18	35	60	2100	-164	14	16	6	180	-8	-148	20	-116
19	37	62	2294	-178	14	10	6	188	-8	-168	20	-148
20	39	64	2496	-192	14	4	6	196	-8	-188	20	-180
21	41	66	2706	-2	-190	210	-206	212	-16	208	-396	**628**
22	43	68	2924	-8	6	212	-2	220	-8	204	4	**628**
23	45	70	3150	-14	6	214	-2	228	-8	200	4	**628**
...	...	...	...	...	...	...	...	...	...	...	...	**628**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**628**

Table 46: $\Delta_{|p-q|} = 25, p = 2j$ for $j \in \mathbb{N}$

-1	0
2	2

dial settings

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5
1	2	27	54	-5	0	27	0	32	0	22	0	76
2	4	29	116	-35	30	5	22	40	-8	-30	52	-20
3	6	31	186	-17	-18	39	-34	56	-16	22	-52	100
4	8	33	264	-39	22	25	14	64	-8	-14	36	36
5	10	35	350	-61	22	11	14	72	-8	-50	36	-28
6	12	37	444	-3	-58	85	-74	88	-16	82	-132	252
7	14	39	546	-17	14	79	6	96	-8	62	20	220
8	16	41	656	-31	14	73	6	104	-8	42	20	188
9	18	43	774	-45	14	67	6	112	-8	22	20	156
10	20	45	900	-59	14	61	6	120	-8	2	20	124
11	22	47	1034	-73	14	55	6	128	-8	-18	20	92
12	24	49	1176	-87	14	49	6	136	-8	-38	20	60
13	26	51	1326	-101	14	43	6	144	-8	-58	20	28
14	28	53	1484	-115	14	37	6	152	-8	-78	20	-4
15	30	55	1650	-129	14	31	6	160	-8	-98	20	-36
16	32	57	1824	-143	14	25	6	168	-8	-118	20	-68
17	34	59	2006	-157	14	19	6	176	-8	-138	20	-100
18	36	61	2196	-171	14	13	6	184	-8	-158	20	-132
19	38	63	2394	-185	14	7	6	192	-8	-178	20	-164
20	40	65	2600	-199	14	1	6	200	-8	-198	20	-196
21	42	67	2814	-5	-194	211	-210	216	-16	206	-404	**628**
22	44	69	3036	-11	6	213	-2	224	-8	202	4	**628**
23	46	71	3266	-17	6	215	-2	232	-8	198	4	**628**
24	48	73	3504	-23	6	217	-2	240	-8	194	4	**628**
25	50	75	3750	-29	6	219	-2	248	-8	190	4	**628**
26	52	77	4004	-35	6	221	-2	256	-8	186	4	**628**
27	54	79	4266	-41	6	223	-2	264	-8	182	4	**628**
...	...	...	...	...	...	...	...	...	...	...	...	**628**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**628**

Table 47: $\Delta_{|p-q|} = 23, p = 2j$ for $j \in \mathbb{N}$

0	-1
2	2

dial settings

id	p	q	$n = pq$	od_1	df_1	od_2	df_2	od_3	df_3	od_4	df_4	od_5
1	2	25	50	-14	0	14	0	28	0	0	0	28
2	4	27	108	-8	-6	36	-22	44	-16	28	-28	100
3	6	29	174	-30	22	22	14	52	-8	-8	36	36
4	8	31	248	-52	22	8	14	60	-8	-44	36	-28
5	10	33	330	-6	-46	70	-62	76	-16	64	-108	204
6	12	35	420	-20	14	64	6	84	-8	44	20	172
7	14	37	518	-34	14	58	6	92	-8	24	20	140
8	16	39	624	-48	14	52	6	100	-8	4	20	108
9	18	41	738	-62	14	46	6	108	-8	-16	20	76
10	20	43	860	-76	14	40	6	116	-8	-36	20	44
11	22	45	990	-90	14	34	6	124	-8	-56	20	12
12	24	47	1128	-104	14	28	6	132	-8	-76	20	-20
13	26	49	1274	-118	14	22	6	140	-8	-96	20	-52
14	28	51	1428	-132	14	16	6	148	-8	-116	20	-84
15	30	53	1590	-146	14	10	6	156	-8	-136	20	-116
16	32	55	1760	-160	14	4	6	164	-8	-156	20	-148
17	34	57	1938	-2	-158	178	-174	180	-16	176	-332	**532**
18	36	59	2124	-8	6	180	-2	188	-8	172	4	**532**
19	38	61	2318	-14	6	182	-2	196	-8	168	4	**532**
20	40	63	2520	-20	6	184	-2	204	-8	164	4	**532**
21	42	65	2730	-26	6	186	-2	212	-8	160	4	**532**
22	44	67	2948	-32	6	188	-2	220	-8	156	4	**532**
23	46	69	3174	-38	6	190	-2	228	-8	152	4	**532**
24	48	71	3408	-44	6	192	-2	236	-8	148	4	**532**
25	50	73	3650	-50	6	194	-2	244	-8	144	4	**532**
26	52	75	3900	-56	6	196	-2	252	-8	140	4	**532**
27	54	77	4158	-62	6	198	-2	260	-8	136	4	**532**
...	...	...	...	...	...	...	...	...	...	...	...	**532**
∞	∞	∞	∞	...	...	...	...	...	...	...	...	**532**

B Figures

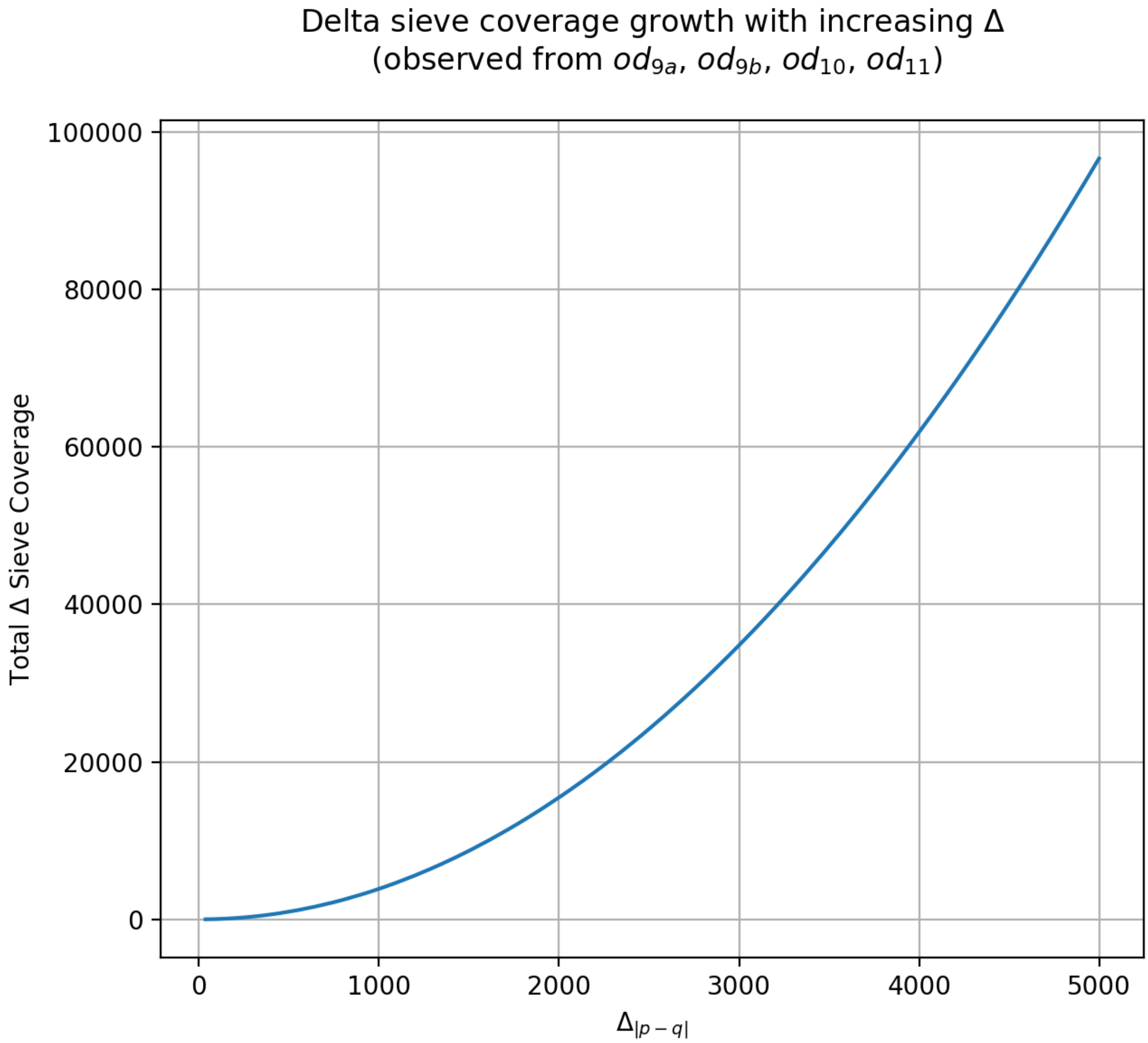

Figure 1: Δ Sieve Coverage Growth

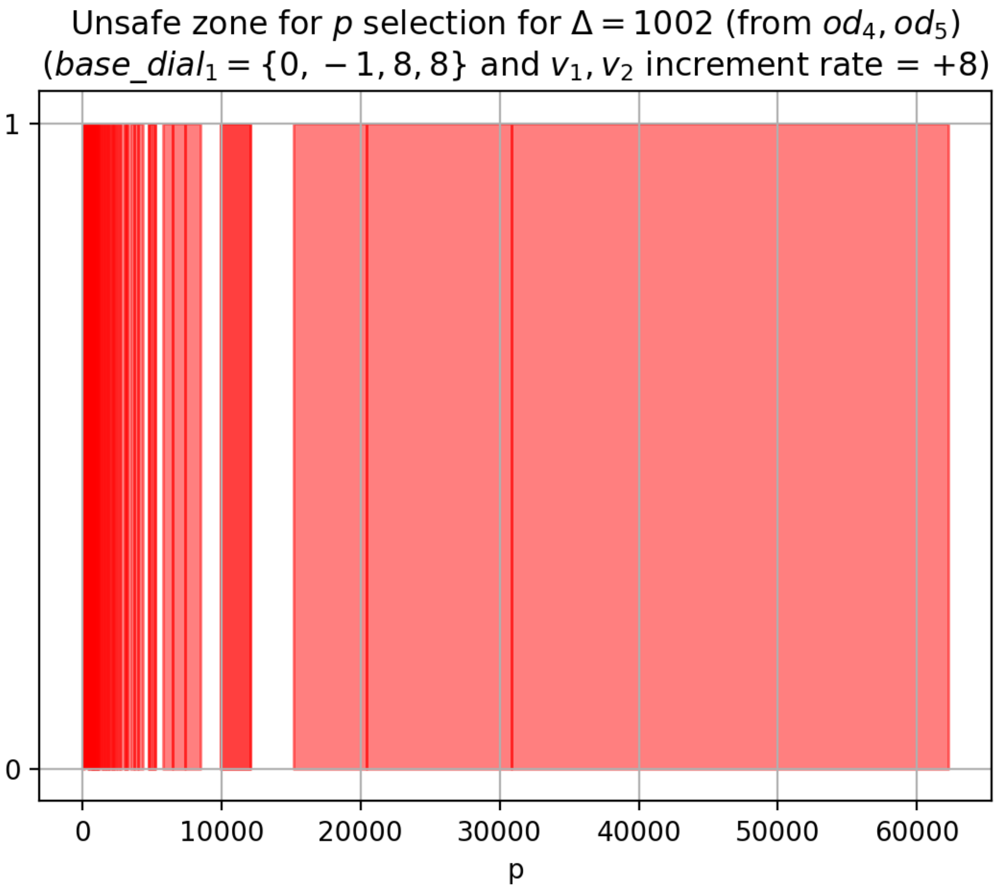

Figure 2: RSA unsafe zone for p selection from od_4, od_5

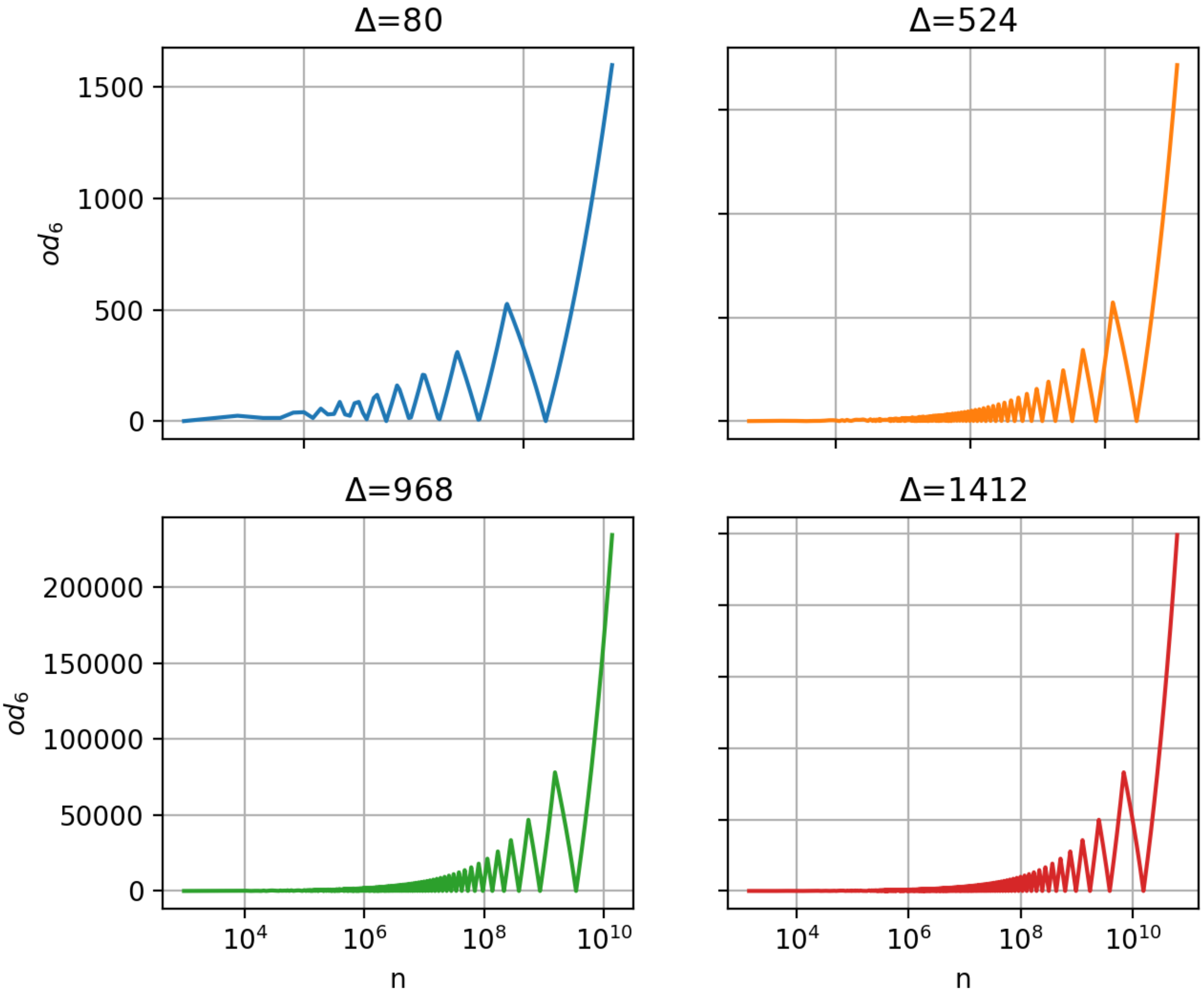

Figure 3: A_+ graph where $v_1 = v_2 = 2$ for $\Delta = 4k, k \in \mathbb{N}$ form

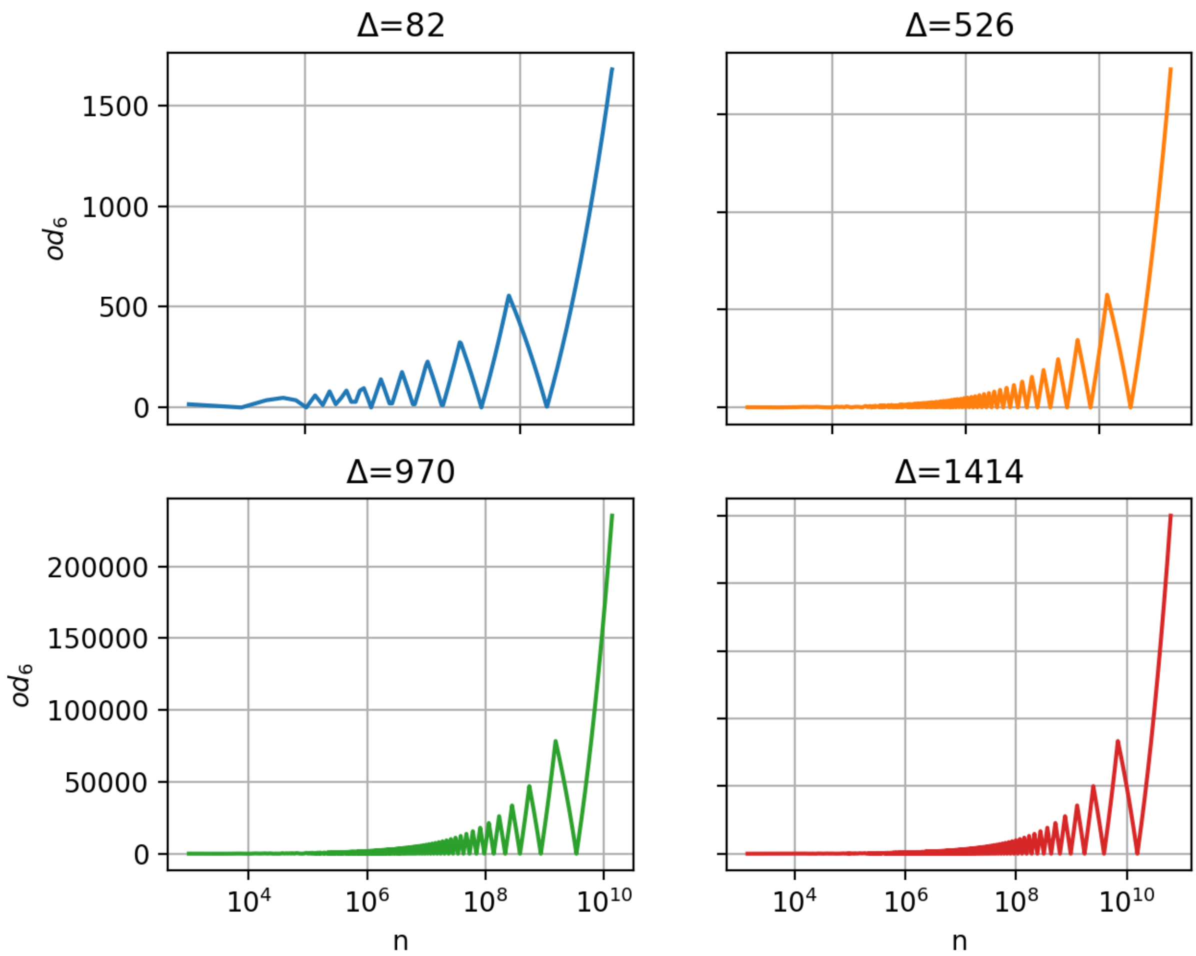

Figure 4: A_+ graph where $v_1 = v_2 = 2$ for $\Delta = 4k + 2, k \in \mathbb{N}$ form

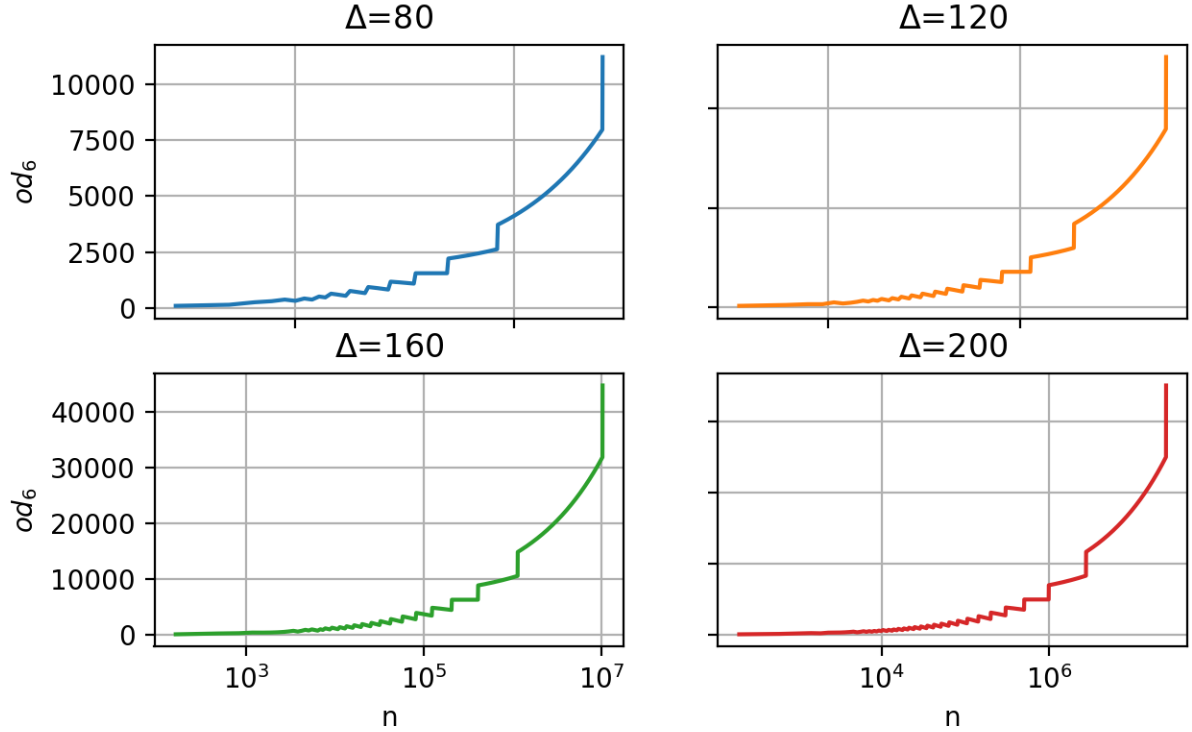

Figure 5: A_+ graph where $v_1 = v_2 = 14$ for $\Delta = 4k, k \in \mathbb{N}$ form

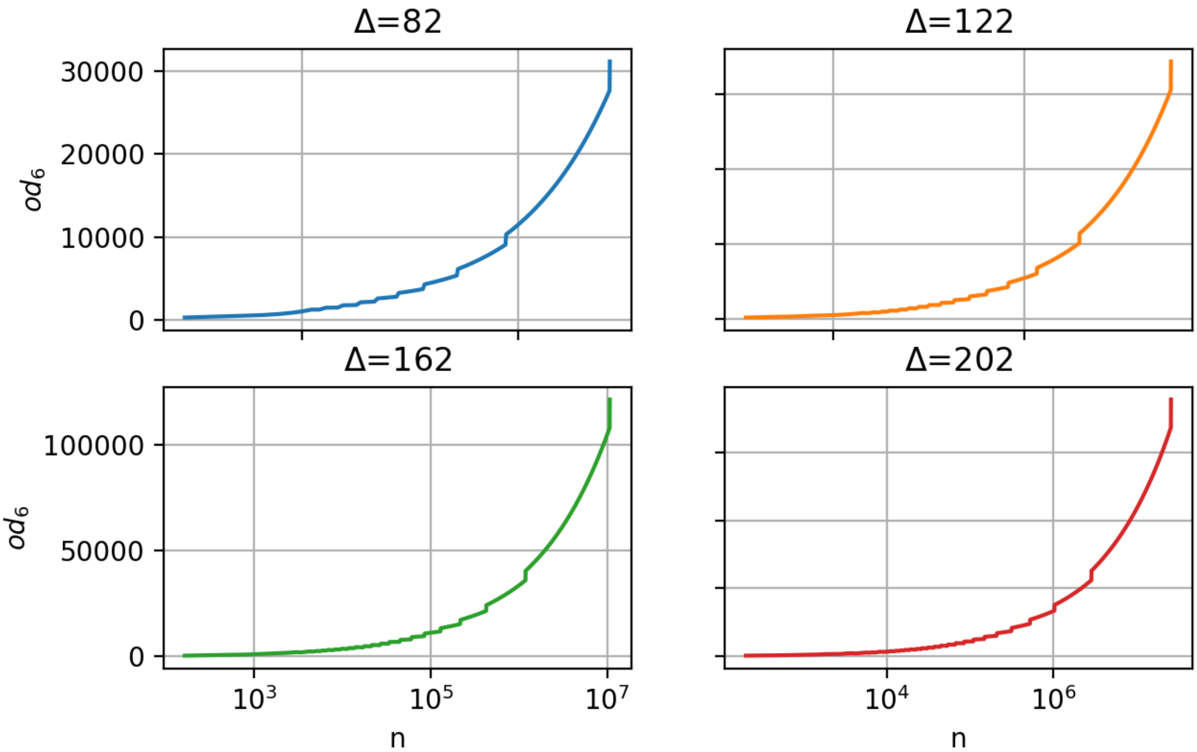

Figure 6: A_+ graph where $v_1 = v_2 = 37$ for $\Delta = 4k+2, k \in \mathbb{N}$ form

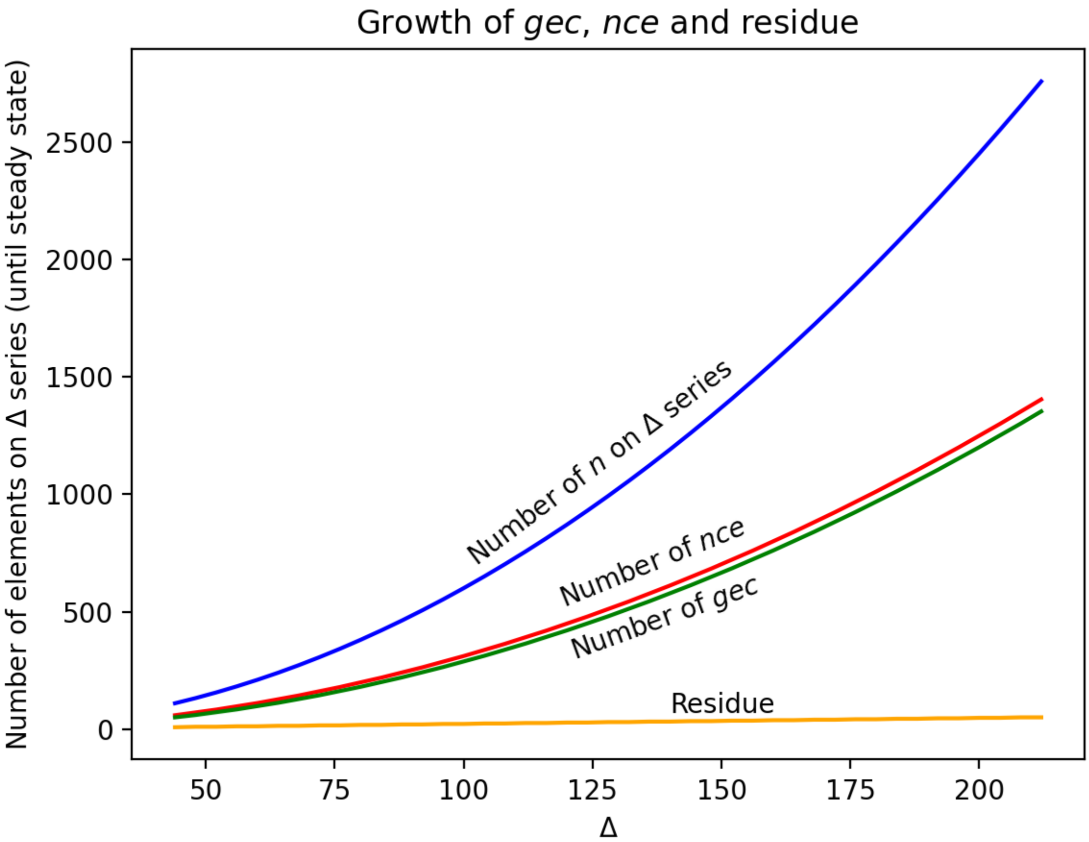

Figure 7: Growth of $gec, nce, residue$ when $\Delta = 4k, k \in \mathbb{N}$ form

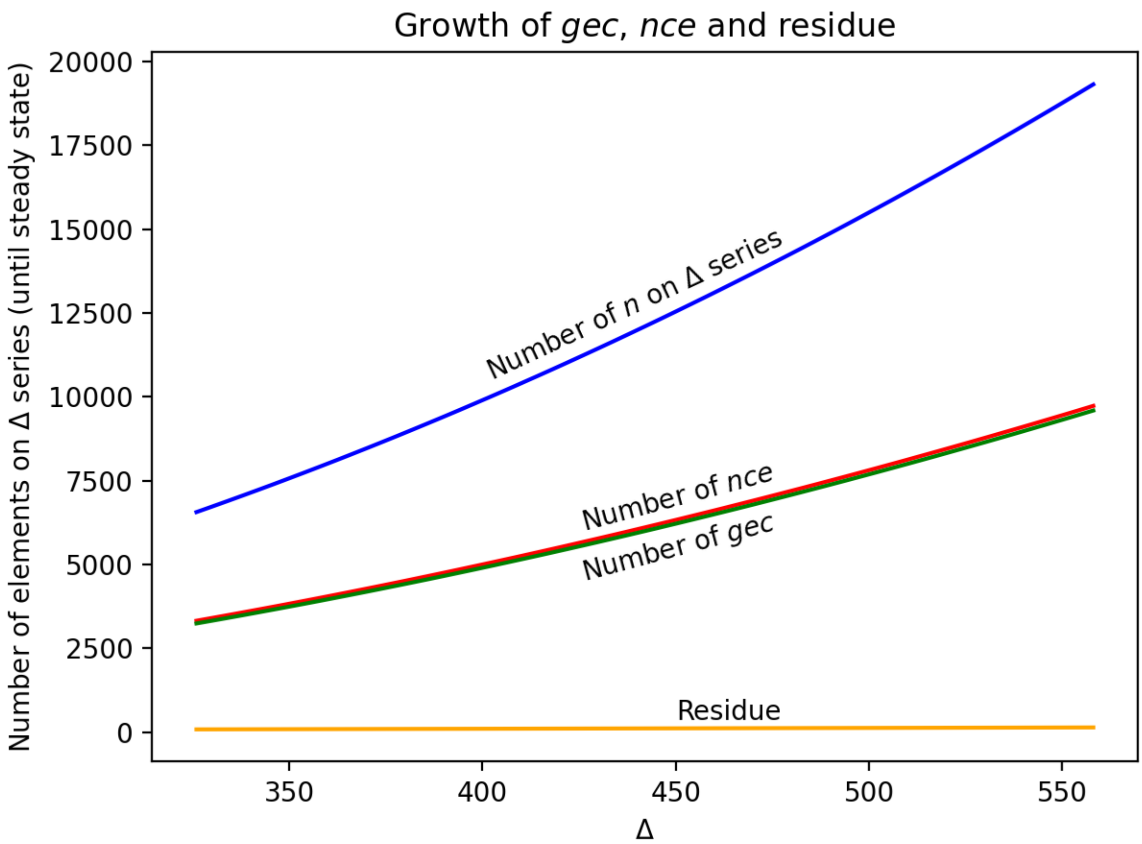

Figure 8: Growth of $gec, nce, residue$ when $\Delta = 4k+2, k \in \mathbb{N}$ form

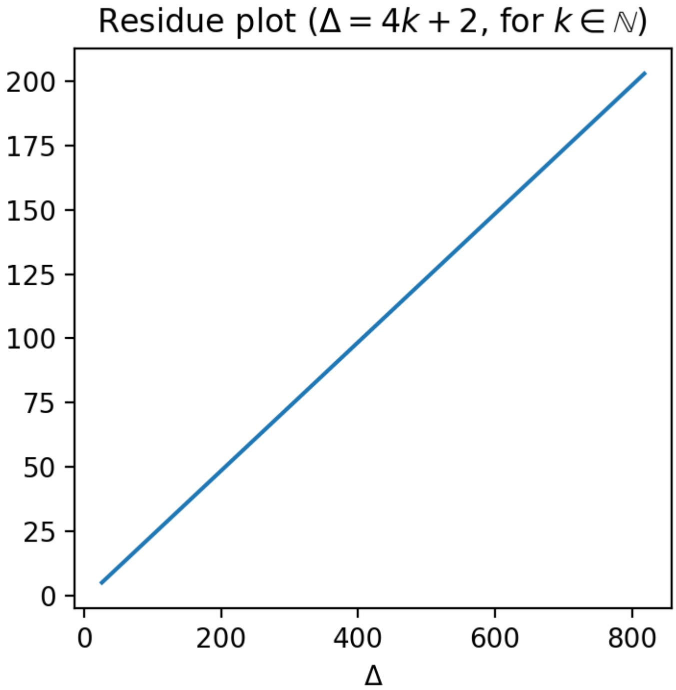

Figure 9: The linear residue

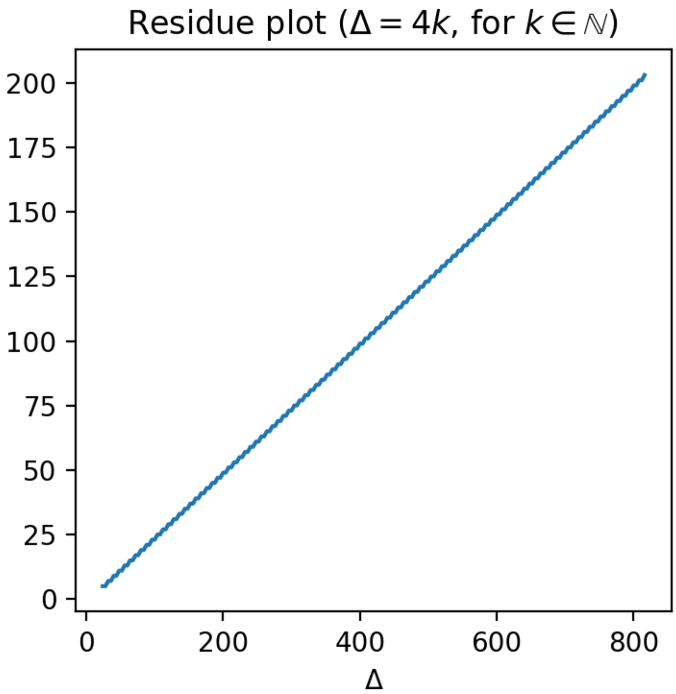

Figure 10: The wood saw residue

C Code to validate the hypotheses and observations

Github repo: https://github.com/vdeltasieve/arjun

1. **client_ssv_p_check.py**: The code confirms the hypotheses in the following equations: (8), (9), (10a), (10b), (10c), (10d), (10e), (11a), (11b), (11c), (11d), (11e)

2. **client_od_constant_check.py**: The code confirms the hypothesis that once a Δ sieve zone is tuned for some known Δ in a particular observation deck, this Δ sieve zone will remain constant for all Δs. This code specifically confirms the Δ sieve zone results as per equations: (14), (15), (16), (17)

3. **client_od4_dial_rotation_check.py**: The code confirms the hypothesis that Δ sieve zones will shift with changing v_1, v_2. This code specifically confirms this hypothesis for od_4

4. **client_od5_dial_rotation_check.py**: The code confirms the hypothesis that Δ sieve zones will shift with changing v_1, v_2. This code specifically confirms this hypothesis for od_5

5. **client_roxy.py**: The code confirms observations in subsection 5.3 - "Reflection over {X,Y}"

6. **client_delta_sum_equilibrium.py**: The code confirms the connection of od_6 on Δ series with N on $\sum$ series, as described in section 8 - "The equilibrium of $\Delta_{|p-q|}$ and $\sum_{p+q}$"

7. **client_dsc_trapdoor.py**: The code validates the algorithm and confirms the example given in section 9 - "The Trapdoor"

8. **client_odd_delta_ssv_check.py**: The code confirms the hypothesis in the following equations: (30a), (30b), (30c), (30d)

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, p. 120–126, Feb. 1978. https://doi.org/10.1145/359340.359342.

[2] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[3] P. de Fermat, "Fermat's factorization method," circa 1640. `https://en.wikipedia.org/wiki/Fermat's_factorization_method`.

[4] D. H. Lehmer and R. Powers, "On factoring large numbers," *Bulletin of the American Mathematical Society*, vol. 37, pp. 770–776, 1931.

[5] M. A. Morrison and J. Brillhart, "A method of factoring and the factorization of F_7," *Mathematics of Computation*, vol. 29, no. 129, pp. 183–205, 1975. http://www.jstor.org/stable/2005475.

[6] D. Shanks, "Squfof notes," *unpub*, circa 1975. Latexed by Stephen McMath March 2004.

[7] R. Schroeppel, "Linear sieve," *unpub*, late 1970s.

[8] J. Dixon, "Asymptotically fast factorization of integers," *Mathematics of Computation*, vol. 36, pp. 255–260, 1981.

[9] C. Pomerance, "The quadratic sieve factoring algorithm," in *Proc. of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, (Berlin, Heidelberg), p. 169–182, Springer-Verlag, 1985. https://dl.acm.org/doi/10.5555/20177.20194.

[10] R. D. Silverman, "The multiple polynomial quadratic sieve," *Mathematics of Computation*, vol. 48, no. 177, pp. 329–339, 1987. http://www.jstor.org/stable/2007894.

[11] A. K. Lenstra, H. W. Lenstra, M. S. Manasse, and J. M. Pollard, "The number field sieve," in *The development of the number field sieve* (A. K. Lenstra and H. W. Lenstra, eds.), (Berlin, Heidelberg), pp. 11–42, Springer Berlin Heidelberg, 1993. https://link.springer.com/chapter/10.1007/BFb0091537.

[12] J. M. Pollard, "A monte carlo method for factorization," *BIT Numerical Mathematics*, vol. 15, pp. 331–334, Sep 1975. https://doi.org/10.1007/BF01933667.

[13] J. M. Pollard, "Theorems on factorization and primality testing," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 76, no. 3, p. 521–528, 1974. https://doi.org/10.1017/S0305004100049252.

[14] H. C. Williams, "A $p+1$ method of factoring," *Mathematics of Computation*, vol. 39, pp. 225–234, 2021/08/09/ 1982. https://doi.org/10.2307/2007633.

[15] H. W. Lenstra, "Factoring integers with elliptic curves," *Annals of Mathematics*, vol. 126, pp. 649–673, 2021/08/09/ 1987. https://doi.org/10.2307/1971363.