doi:10.20944/preprints202009.0742.v1

Introducing two New Sieves for Factorization Natural Odd Numbers

Ramazanali Maleki Chorei

Department of Mathematics, Roudbar Branch, Islamic Azad University, Roudbar, Iran

Corresponding author: Dr.Maleki@iauroudbar.ac.ir

Abstract

For each non-prime odd number as $F = pq$, if we consider m/n as an approximation for q/p and choose $k = mn$, then by proving some lemmas and theorems, we can compute the values of m and n. Finally, by using Fermat's factorization method for F and $4kF$ as difference of two non-consecutive natural numbers, we should be able to find the values of p and q. Then we introduce two new and powerful sieves for separating composite numbers from prime numbers.

Keywords: *Prime numbers, lemmas and theorems, Fermat's factorization method, sieve*

1. Introduction

There are many features for identification of prime numbers from non-prime numbers. In this paper, we attempt to identify very important properties about non-prime odd numbers by proving some theorems and lemmas. In 1643, Fermat a French mathematician described a method for factorization of big odd numbers by a letter to Marin Mersenne .In composite numbers as $F = pq$, by propose $k_r = q/p \approx\ m/n$ and $K = mn$,we introduce two new sieves for factorization of non-prime odd numbers by developing Fermat's factorization method. The first sieve ($\alpha - s$ sieve) based on the relation $(\lfloor\sqrt{F}\rfloor + \theta)^2 - F = \left(\frac{p-q}{2}\right)^2$ and the second sieve ($\beta - s$ sieve) based on the relation $\left(\lfloor\sqrt{4kF}\rfloor + \theta\right)^2 - 4kF = (mp - nq)^2$ (θ is a natural number). We show these sieves are very convenient for big numbers, because we don't use long calculation within process of them.

.

2. Development of Fermat's factorization method

We know each non-prime odd number as $F = pq$ $(3 \leq p < q)$, can be written as a difference of squares of two nonconsecutive natural numbers as following:

$$\begin{cases} p = 2m+1 \\ q = 2n+1 \end{cases} \Longrightarrow \; F = pq = (m+n+1)^2 - (m-n)^2$$

It is clear that by assuming $k_r = \frac{q}{p}$, we have $F = k_r p^2$.

Therefore, for each natural number bigger than 1 as k, we can write $4kF$ as difference of squares of two even numbers or odd numbers, in which F is a non-prime odd number:

$$4kF = 4k(pq) = (2kp)\,(2q) = (q+kp)^2 - (q-kp)^2$$

If we assume $k = mn$, in this case, we can write:

$$4kF = 4mnpq = (mp+nq)^2 - (mp-np)^2$$

***Definition:** In this paper, the expressions $\left(\lfloor\sqrt{4kF}\rfloor + \theta\right)^2 - 4kF$ and $\left(\lfloor\sqrt{F}\rfloor + \theta\right)^2 - F$ are shown by $\beta(k,\theta)$ and $\alpha(\theta)$ respectively.*

If F is a square number, this means that it's a non-prime number and if F isn't a square number, and $\alpha(\theta)$ is a square, then according to the identity $F = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ and

definition of $\alpha(\theta)$, we have:

$$\alpha(\theta) \; = (\lfloor\sqrt{F}\rfloor + \theta)^2 - F \Rightarrow \begin{cases} \dfrac{p+q}{2} = \lfloor\sqrt{F}\rfloor + \theta \\ \dfrac{p-q}{2} = \sqrt{\alpha(\theta)} \end{cases} \Rightarrow \begin{cases} p = (\lfloor\sqrt{F}\rfloor + \theta) - \sqrt{\alpha(\theta)} \\ q = (\lfloor\sqrt{F}\rfloor + \theta) + \sqrt{\alpha(\theta)} \end{cases}$$

If kF is a square number and assume $k_r = \frac{q}{p}$, it means that:

$$F = k_r p^2 \Longrightarrow kF = kk_r p^2 \Longrightarrow kk_r = t^2.$$

Since t and k are natural numbers, so F will be divided on k_r.This means that F is a non-prime number. If kF isn't a square number and $\beta(k,\theta)$ is a square number, then we will have:

$$4kF = (q+kp)^2 - (q-kp)^2 = \left(\lfloor\sqrt{4kF}\rfloor + \theta\right)^2 - \beta(k,\theta) \Rightarrow \begin{cases} q + kp = \lfloor\sqrt{4kF}\rfloor + \theta \\ |q - kp| = \sqrt{\beta(k,\theta)} \end{cases}$$

$$\Rightarrow p = \frac{(\lfloor\sqrt{4kF}\rfloor + \theta) \mp \sqrt{\beta(k,\theta)}}{2k} \, , q = \frac{(\lfloor\sqrt{4kF}\rfloor + \theta) \pm \sqrt{\beta(k,\theta)}}{2}$$

By assuming $k = mn$, *we will have:*

$$p = \frac{\left(\lfloor\sqrt{4kF}\rfloor + \theta\right) \mp \sqrt{\beta(k,\theta)}}{2m} \quad , q = \frac{\left(\lfloor\sqrt{4kF}\rfloor + \theta\right) \pm \sqrt{\beta(k,\theta)}}{2n}$$

When F *is a non-prime number, both* p *and* q *are natural numbers bigger than 1.*

Lemma 1: *Whenever* k *is a natural even number such that* $x > \frac{(K-2)^2}{8}$ *and* x *is a natural number, in this case, we will have:*

$$\left\lfloor\sqrt{x^2+kx}\right\rfloor = x + \frac{k-2}{2}.$$

Proof: *From the basic algebra, we have:*

$$(x+\frac{k}{2}-1)^2 < x^2+kx < (x+\frac{k}{2})^2 \Rightarrow x+\frac{k}{2}-1 < \sqrt{x^2+kx} < x+k.$$

If $x+\frac{K}{2}-1$ *isn't the biggest integer number smaller than* $\sqrt{x^2+kx}$, *we should have at least:*

$$\left(x+\frac{K}{2}-1\right)+1 < \sqrt{x^2+kx} \Rightarrow x^2+kx+\frac{K^2}{4} < x^2+kx. \qquad (1)$$

Since $\frac{K^2}{4} > 0$, *therefore the inequality (1) isn't correct. So* $x+\frac{K}{2}-1$ *is the biggest integer number smaller than* $\sqrt{x^2+kx}$ *and based on the bracket function definition, we will have*

$$\left\lfloor\sqrt{x^2+kx}\right\rfloor = x + \frac{k-2}{2}.$$

Because $\left(x+\frac{K}{2}-1\right)^2 < x^2+kx$, *so we will have* $x > \frac{(K-2)^2}{8}$. ■

Lemma 2: *Suppose* x *is a natural number and* k *is a natural even number such that* $x > \frac{(K+2)^2}{8}$. *Then, we will have:*

$$\left\lfloor\sqrt{x^2-kx}\right\rfloor = x - \frac{k+2}{2} \quad .$$

Proof: *From basic algebra, we have:*

$$(x-\frac{k+2}{2})^2 < x^2-kx < (x-\frac{k}{2})^2 \Rightarrow x-\frac{k+2}{2} < \sqrt{x^2-kx} < x-\frac{k}{2} \quad .$$

If $x-\frac{k+2}{2}$ *isn't the biggest integer component smaller than* $\sqrt{x^2+kx}$, *then we should have:*

$$\left(x-\frac{k+2}{2}\right)+1<\sqrt{x^2-kx} \Longrightarrow (x^2-kx)+\frac{k^2}{4}<x^2-kx \qquad \textit{(1)}$$

Because $\frac{k^2}{4}$*>0, so the inequality (1) is incorrect and* $x-\frac{k+2}{2}$ *is the biggest integer number smaller than* $\sqrt{x^2-kx}$ *and from bracket function definition, we will have:*

$$\left\lfloor\sqrt{x^2-kx}\right\rfloor = x-\frac{k+2}{2},$$

And so:

$$(x-\frac{k+2}{2})^2<x^2-kx \Longrightarrow\ x>\frac{(k+2)^2}{8}\ . \qquad ■$$

In this paper, the approximate value of a number as x *will be shown in the form of* $\sim(x)$ *or* $\tilde{x}$.

Theorem 1*: For each natural odd number as* $F=pq, (1\leq p<q)$ *if we assume*$\tilde{k}_r=\sim(q/p)=m/n$ *and* $|\tilde{k}_r-k_r|$=0 · $\overline{a_1\dots a_s}$ *, by choosing k=mn, the result of* $\beta(k,1)$ *will be square when* $\overline{a_1\dots a_s}\,p^2<\sqrt{4F\times10^s}\ \pm 1$.

Proof*: If* $\tilde{k}_r>k_r$*, we can write:*

$$\tilde{K}_r=\frac{m}{n}=\frac{q}{p}+0.\overline{a_1\dots a_s}=\frac{10^Sq+\overline{a_1\dots a_s}\,p}{10^Sp}.$$

If we choose m= $10^Sq+\overline{a_1\dots a_s}\,p$ *and* $n=\ 10^Sp$*, then we will have:*

$$k=mn=10^{2S}F+\overline{a_1\dots a_s}\,p^2\times10^S\Rightarrow 4kF=(2\times10^SF)^2+(2p^2\,\overline{a_1\dots a_s})(2\times10^S\,F) \qquad (1)$$

Now, by assuming $\overline{a_1\dots a_s}\,(2p^2)=k'$ *and* $x=2\times10^SF$*, we arrive at* $4kF=x^2+k'x$*. Since* k' *is even, so by lemma (1), we get*

$$\left\lfloor\sqrt{4kF}\right\rfloor=\left\lfloor\sqrt{x^2+k'x}\right\rfloor=x+\frac{k'-2}{2}=2\times10^SF+\overline{a_1\dots a_s}\,p^2-1\Rightarrow$$

$$\beta(k,1)=(\left\lfloor\sqrt{4kF}\right\rfloor+1)^2-4kF=(2\times10^SF+\overline{a_1\dots a_s}\,p^2)^2-4kF,$$

and therefore, according to the relation (1), we will obtain $\beta(k,1)=(\overline{a_1\dots a_s}\,P^2)^2$*. Consequently, based on the lemma (1) and by assuming* $x>\frac{(k'-2)^2}{8}$ *, we should have:*

$$k'<\sqrt{8x}+2\Longrightarrow\overline{a_1\dots a_s}.P^2<\sqrt{4F\times10^S}+1.$$

In the case that $\tilde{k}_r<k_r$*, the proof is similar to the above and we should have:*

$$\overline{a_1\dots a_s}\,P^2<\sqrt{4F\times10^S}-1. \qquad ■$$

Note1: *For each natural odd number, when* $p = 1$*, then we have* $\beta(k,1) = (\overline{a_1 \dots a_s})^2$.

Whenever $\left|\tilde{k}_r - k_r\right| = 10^{-s}$*, then we have* $\beta(k,1) = 1$.

Theorem 2: *In a non-prime odd number as* $F = pq \ (1 \le p < q)$*, if* $p > \sqrt{F} + 1 - \sqrt{(\sqrt{F}+1)^2 - F}$*, then the result of* $\alpha(1)$ *will be square and we will have:*

$$\alpha(1) = (\lfloor\sqrt{F}\rfloor + 1)^2 - F = (\frac{\delta}{2})^2 = (\frac{q-p}{2})^2.$$

Proof: *Since* $\delta = q - p$ *is even, then from lemma* (2) *we have:*

$$\lfloor\sqrt{F}\rfloor = \lfloor\sqrt{pq}\rfloor = \left\lfloor\sqrt{p(p+\delta)}\right\rfloor = \left\lfloor\sqrt{p^2 + \delta.P}\right\rfloor = p + \frac{\delta - 1}{2} = \frac{q+p}{2} - 1$$

$$\Rightarrow \ \alpha(1) = (\frac{p+q}{2})^2 - pq = (\frac{q-p}{2})^2 = (\frac{\delta}{2})^2$$

In this case, according to lemma (1)*, we have:*

$$\delta = q - p < \sqrt{8p} + 2 = 2\sqrt{2p} + 2 \Longrightarrow \frac{F}{p} - p < 2\sqrt{2p} + 2 \Longrightarrow F < \left(p + \sqrt{2p}\right)^2$$

$$\Longrightarrow p + \sqrt{2p} - \sqrt{F} > 0 \Longrightarrow P > \sqrt{F} + 1 - \sqrt{\left(\sqrt{F}+1\right)^2 - F} \ . \qquad \blacksquare$$

Lemma 3: *If* k *is a natural odd number and* x *is a natural number such that* $x > (\frac{k-1}{2})^2$*, then we will have:*

$$\left\lfloor\sqrt{x^2 + kx}\right\rfloor = x + \frac{k-1}{2}.$$

Proof: *From the basic algebra, we will have:*

$$(x + \frac{k-1}{2})^2 < x^2 + kx < (x + \frac{k}{2})^2 \ \Rightarrow x + \frac{k-1}{2} < \sqrt{x^2 + kx} < x + \frac{k}{2}.$$

If $x + \frac{k-1}{2}$ *is not the biggest integer number smaller than* $\sqrt{x^2 + kx}$ *, then, we should have at least:*

$$\left(x + \frac{k-1}{2}\right) + 1 < \sqrt{x^2 + kx} \Rightarrow \left(x + \frac{k+1}{2}\right)^2 < x^2 + kx \Rightarrow (x^2 + kx) + x + (\frac{k+1}{2})^2 < x^2 + kx. \quad (1)$$

Because $x + (\frac{k+1}{2})^2 > 0$*, so the inequality* (1) *is not correct and therefore this means that* $x + \frac{k-1}{2}$ *is the biggest integer number smaller than* $\sqrt{x^2 + kx}$*. Then, according to definition of the bracket function, we should have* $\left\lfloor\sqrt{x^2 + kx}\right\rfloor = x + \frac{k-1}{2}$*. But* $(x + \frac{k-1}{2})^2 < x^2 + kx$*, so we should have*

$x > (\frac{k-1}{2})^2$. ■

Theorem3: *In a natural odd number as* $F = pq, (1 \leq p < q)$, *by assuming* $k_r = q/p$ *and* $\tilde{k}_r = \sim(q/p) = m/n$, *we will have* $\beta(k,1) = (mp - nq)^2$.

In the case that $\tilde{k}_r > k_r$,*we should have* $|mp - nq| = 0.\overline{a_1 \ldots a_s}\, np < 2\sqrt{nq} + 1$,

and in the case that $\tilde{k}_r < k_r$, *we should have* $|mp - nq| = 0.\overline{a_1 \ldots a_s}\, np < 2\sqrt{mp} + 1$.

Proof: *By assuming* $k = mn$,*we have* $\lfloor\sqrt{4kF}\rfloor = \lfloor\sqrt{4mnpq}\rfloor = \lfloor\sqrt{PQ}\rfloor$ *which* $P = 2mp$ *and* $Q = 2nq$.

If $\tilde{k}_r > k_r$: $\frac{m}{n} > \frac{q}{p} \Rightarrow \tilde{k}_r - k_r = 0.\overline{a_1 \ldots a_s} = \frac{m}{n} - \frac{q}{p} = \frac{mp-nq}{np}$. (1)

According to lemma (1), *we will have:*

$$\delta = P - Q = 2mp - 2nq \Rightarrow \lfloor\sqrt{4kF}\rfloor = \lfloor\sqrt{PQ}\rfloor = \left\lfloor\sqrt{Q(Q+\delta)}\right\rfloor = Q + \frac{\delta - 2}{2}$$

$$= \frac{P+Q}{2} - 1 = (mp + nq) - 1 \Rightarrow \beta(k,1) = (mp + nq)^2 - 4mnpq = (mp - nq)^2.$$

Based on lemma (1), *we have:*

$$\delta = P - Q < \sqrt{8Q} + 2 \Rightarrow mp - nq < 2\sqrt{nq} + 1,$$

and according to the relation (1), *we can write* $mp - nq = 0.\overline{a_1 \ldots a_s}\, np < 2\sqrt{nq} + 1$.

If $\tilde{k}_r < k_r$: $\frac{m}{n} < \frac{q}{p} \Rightarrow k_r - \tilde{k}_r = 0.\overline{a_1 \ldots a_s} = \frac{q}{p} - \frac{m}{n} = \frac{nq-mp}{np}$. (2)

According to lemma (1), *we have:*

$$\delta = Q - P = 2nq - 2mp \Rightarrow \lfloor\sqrt{4kF}\rfloor = \lfloor\sqrt{4mnpq}\rfloor = \lfloor\sqrt{PQ}\rfloor = \left\lfloor\sqrt{P(P+\delta)}\right\rfloor = \left\lfloor\sqrt{P^2 + P\delta}\right\rfloor$$

$$= P + \frac{\delta - 2}{2} = \frac{P+Q}{2} - 1 = nq + mp - 1 \Rightarrow \beta(k,1) = (nq + mp)^2 - 4mnpq = (mp - nq)^2.$$

According to lemma (1), *we should have:*

$$\delta = Q - P < \sqrt{8P} + 2 \Rightarrow nq - mp < 2\sqrt{mp} + 1 .$$

Based on the relation (2), *we will have:* $nq - mp = 0.\overline{a_1 \ldots a_s}\, np < 2\sqrt{mp} + 1$. ■

Theorem 4: *For each natural odd number as* $F = pq, (1 \le p < q)$, *the value of* $\beta(k,1)$ *will be square when* k *lies in interval* $\left(\frac{(\sqrt{q}+1)^2}{P}, \frac{(\sqrt{q}-1)^2}{P}\right)$ *except in a case that* $k = k_r$.

Proof (1): If $k > \frac{q}{p}$, *in this case* $2kp > 2q$ *and because the result of* $\delta = 2kp - 2q$ *is even, then from lemma* (1), *we will have:*

$$\lfloor\sqrt{4kF}\rfloor = \left\lfloor\sqrt{(2kp)(2q)}\right\rfloor = \left\lfloor\sqrt{2q(2q+\delta)}\right\rfloor = \left\lfloor\sqrt{(2q)^2+2q\delta}\right\rfloor = 2q + \frac{\delta-2}{2} = q + kp - 1$$

$$\Rightarrow \beta(k,1) = (q+kp)^2 - 4kpq = (q-kp)^2.$$

According to lemma (1), *we should have:*

$$\delta = 2kp - 2q < \sqrt{8(2q)} + 2 \Rightarrow kp - q - 1 < 2\sqrt{q} \Rightarrow kp < (\sqrt{q}+1)^2 \Rightarrow k < \frac{(\sqrt{q}+1)^2}{p}. \qquad (1)$$

If $k < \frac{q}{p}$, *in this case* $2kp < 2q$ *and because the result of* $\delta = 2q - 2kp$ *is even, then from lemma* (1), *we will get:*

$$\lfloor\sqrt{4kF}\rfloor = \left\lfloor\sqrt{(2kp)(2q)}\right\rfloor = \left\lfloor\sqrt{(2kp)(2kp+\delta)}\right\rfloor = \left\lfloor\sqrt{(2kp)^2+2kp\delta}\right\rfloor = 2kp + \frac{\delta-2}{2}$$

$$= q + kp - 1 \Rightarrow \beta(k,1) = (q+kp)^2 - 4kpq = (q-kp)^2.$$

Based on the lemma (1), *we should have:*

$$\delta = 2q - 2kp < \sqrt{8(2kp)} + 2 \Rightarrow q - kp < 2\sqrt{kp} + 1 \Rightarrow q < (\sqrt{kp}+1)^2 \Rightarrow k > \frac{(\sqrt{q}-1)^2}{p}. \qquad (2)$$

Now, from (1) *and* (2), *we will have* $\frac{(\sqrt{q}-1)^2}{p} < k < \frac{(\sqrt{q}+1)^2}{p}$, *thus if* $k = k_r$, *we can write:*

$$k = k_r = \frac{q}{p} \Rightarrow 4kF = 4q^2 \Rightarrow \beta(k,1) = (2q+1)^2 - 4q^2 = 4q + 1 \ne |kp - q| = 0$$

so, we can conclude $k \ne k_r$.

Proof (2): *According to theorem*(3), *when we assume* $k = \tilde{k}_r = m$ *and* $n = 1$, *we will have:*

$$\begin{cases} \tilde{k}_r > k_r \Rightarrow kp - q < 2\sqrt{q} + 1 \\ \tilde{k}_r < k_r \Rightarrow q - kp < 2\sqrt{kp} + 1 \end{cases} \Rightarrow \begin{cases} k < \frac{(\sqrt{q}+1)^2}{p} \\ k > \frac{(\sqrt{q}-1)^2}{p} \end{cases} \Rightarrow \quad \frac{(\sqrt{q}-1)^2}{p} < k < \frac{(\sqrt{q}+1)^2}{p}$$

or $\left(\frac{\sqrt{F}-\sqrt{P}}{p}\right)^2 < k < \left(\frac{\sqrt{F}+\sqrt{P}}{P}\right)^2$ ■

If we propose $k_{min} = \frac{(\sqrt{q}-1)^2}{p}$ *and* $k_{max} = \frac{(\sqrt{q}+1)^2}{p}$ *and shown the difference of* K_{min} *and* K_{max} *by* δ *then for every integer number which is lied in that interval, the result of* $\beta(k,1)$ *will be square. Therefore, we have* $\delta = k_{max} - k_{min} = \frac{4\sqrt{q}}{p}$.

We will have the Maximum value of δ *when* $P = 1$. *In this case, we have* $\delta_{max} = 4\sqrt{F}$.

If the number of natural numbers located in interval (k_{min}, k_{max}) *are demonstrated by* N, *so we will have* $N = \lfloor k_{max} \rfloor - \lfloor k_{min} \rfloor$.

If $k = k_r$ *and it is located in interval* (K_{min}, K_{max}), *then we will have* $N = \lfloor K_{max} \rfloor - \lfloor K_{min} \rfloor - 1$.

When the value of δ *is maximum, then the value of* N *will be maximum too.*

$$\begin{cases} P = 1 \\ q = F \end{cases} \Rightarrow \begin{cases} \lfloor k_{min} \rfloor = \left\lfloor (\sqrt{F}-1)^2 \right\rfloor \\ \lfloor k_{max} \rfloor = \left\lfloor (\sqrt{F}+1)^2 \right\rfloor \end{cases} \Rightarrow N_{max} = \lfloor k_{max} \rfloor - \lfloor k_{min} \rfloor - 1$$

$$= \left\lfloor F + 2\sqrt{F} + 1 \right\rfloor - \left\lfloor F - 2\sqrt{F} + 1 \right\rfloor - 1 = (F+1) + \left\lfloor 2\sqrt{F} \right\rfloor - (F+1) - \left\lfloor -2\sqrt{F} \right\rfloor - 1$$

$$= \left\lfloor 2\sqrt{F} \right\rfloor - \left(-\left\lfloor 2\sqrt{F} \right\rfloor - 1\right) - 1 = \left\lfloor 4\sqrt{F} \right\rfloor.$$

Example1: Find the value of N *in* $F = 17 \times 43 = 6851$.

Answer: $p = 17, q = 43 \Rightarrow 21 < k \leq 26 \Rightarrow N = 26 - 21 = 5$.

Then we can see that:

$k = 22 \Rightarrow \beta(22{,}1) = 5^2, k = 23 \Rightarrow \beta(23{,}1) = 12^2, k = 24 \Rightarrow \beta(24{,}1) = 5^2,$

$k = 25 \Rightarrow \beta(25{,}1) = 44^2, k = 26 \Rightarrow \beta(26{,}1) = 39^2.$

Theorem 5: *For odd natural numbers as* $F = pq$, *by propose* $k_r = \frac{q}{p} \simeq \frac{m}{n}$, $(m,n) = 1$ *and choose* k= r^2mn , *when* r *is a natural number, then the value of* $\beta(k,1)$ *will be square.*

Proof: *For proof in the first case, we propose* $\frac{m}{n} > \frac{q}{p}$

Therefore $\frac{rm}{rn} > \frac{q}{p} \Rightarrow \quad rmp > rnp \Rightarrow \quad \left\lfloor \sqrt{4kF} \right\rfloor = \left\lfloor \sqrt{(2rmp)(2rnq)} \right\rfloor = \sqrt{PQ}$

If $P = 2rmp$, $Q = 2rnq$, *then we have* $\delta = P - Q = 2rmp - 2rnq > 0$.

Based on lemma (1) , *we should have:*

$$\lfloor\sqrt{PQ}\rfloor = \lfloor\sqrt{Q(\ Q+\delta\ )}\rfloor = Q + \frac{\delta - 2}{2} = \frac{P+Q}{2} - 1 = rmp - rnq - 1 \ \ =>$$

$$\beta(k,1) = \left(\lfloor\sqrt{4kF}\rfloor + 1\right)^2 - 4kF = (rmp + rnq)^2 - 4r^2mnpq = (rmp - rnq)^2.$$

Therefore we should have $rmp - rnq < 2\sqrt{rnq} + 1$.

In the case $\frac{m}{n} < \frac{q}{p}$ *, the proof is similar as above.* ■

Theorem 6: *For each non-prime odd number as* $F = pq(1 \le p < q)$, *if we assume*

$\theta = \lfloor(\sqrt{kp} - \sqrt{q})^2\rfloor + 1$ *and* kF *doesn't be square, then the value of* $\beta(k,\theta)$ *will be square so that*

$$\frac{\left(\sqrt{q}+\sqrt{\theta-1}\right)^2}{p} \le k < \frac{\left(\sqrt{q}+\sqrt{\theta}\right)^2}{p} \quad \text{and} \quad \frac{\left(\sqrt{q}-\sqrt{\theta}\right)^2}{p} < k \le \frac{\left(\sqrt{q}-\sqrt{\theta-1}\right)^2}{p} \ .$$

Proof: *In the identity* $4kF = 4k(pq) = (q+kp)^2 - (q-kp)^2$*,since* kF *can not be square, thus we have* $\theta = \lfloor kp + q - \sqrt{4kpq}\rfloor + 1 = kp + q + \lfloor-\sqrt{4kpq}\rfloor + 1 = kp + q + (-\lfloor\sqrt{4kpq}\rfloor - 1) + 1$

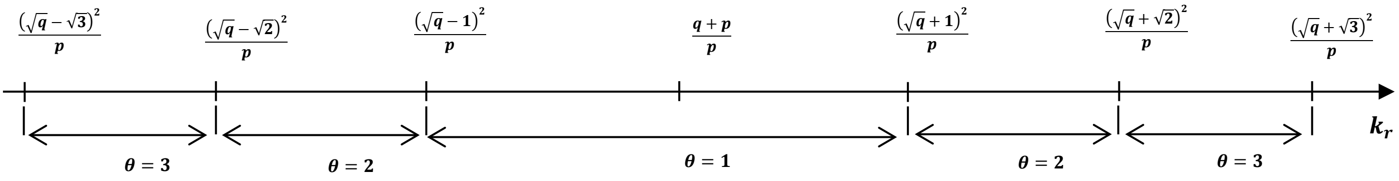
$= kp + q - \lfloor\sqrt{4kpq}\rfloor \Rightarrow \beta(k,\theta) = (kp+q)^2 - 4kpq = (kp-q)^2.$

At that rate for any k value, we can write:

$$\theta = \left\lfloor\left(\sqrt{kp}-\sqrt{q}\right)^2\right\rfloor + 1 \ \ => \ \ \theta - 1 \le \left(\sqrt{kp}-\sqrt{q}\right)^2 < \theta \ => \ \sqrt{\theta-1} \le \left|\sqrt{kp}-\sqrt{q}\right| < \sqrt{\theta} \ \ =>$$

$$\frac{\left(\sqrt{q}+\sqrt{\theta-1}\right)^2}{p} \le k < \frac{\left(\sqrt{q}+\sqrt{\theta}\right)^2}{p} \quad , \quad \frac{\left(\sqrt{q}-\sqrt{\theta}\right)^2}{p} < k \le \frac{\left(\sqrt{q}-\sqrt{\theta-1}\right)^2}{p}$$ ■

In the sequel we have:


$\frac{(\sqrt{q}-\sqrt{3})^2}{p}$
$\frac{(\sqrt{q}-\sqrt{2})^2}{p}$
$\frac{(\sqrt{q}-1)^2}{p}$
$\frac{q+p}{p}$
$\frac{(\sqrt{q}+1)^2}{p}$
$\frac{(\sqrt{q}+\sqrt{2})^2}{p}$
$\frac{(\sqrt{q}+\sqrt{3})^2}{p}$
k_r
$\theta = 3$
$\theta = 2$
$\theta = 1$
$\theta = 2$
$\theta = 3$

For example when $F = 89 \times 911 = 81{,}079$ *and* $\theta = 7$ *, we can calculate k values as bellow:*

$$\frac{\left(\sqrt{q}+\sqrt{\theta-1}\right)^2}{p} \le k < \frac{\left(\sqrt{q}+\sqrt{\theta}\right)^2}{p} \ => \frac{\left(\sqrt{911}+\sqrt{6}\right)^2}{89} \le k < \frac{\left(\sqrt{911}+\sqrt{7}\right)^2}{89} \ =>$$

11/9 $\le k <$ *12/1* $=> k = 12 => \beta(k,\theta) = \beta(12,7) = (1972+7)^2 - 3{,}891{,}792 = 157^2$

We can observe when $\theta = 6$ *, we can't find any value for k.*

Note 2: *For any value of k as a natural number, exist a nonnegative integer number as* θ

$\left(\theta = \left\lfloor \left(\sqrt{kp} - \sqrt{q}\right)^2 \right\rfloor + 1\right)$ *, so that* $\beta(k,\theta)$ *should be square. Whiles for any value of* θ *, may don't be exist a value for k.*

Generalized form of theorem 6: *For each non-prime odd number as* $F = pq(1 \le p < q)$*, by assuming* $m > n$ *(m,n are natural numbers), if we choose* $\theta = \lfloor (\sqrt{mp} - \sqrt{nq})^2 \rfloor + 1$ *and* $mnpq$ *doesn't be square, then the value of* $\beta(k,\theta)$ *will be square.*

Proof: *According to the identity* $4kF = 4mnpq = (mp + nq)^2 - (mp - np)^2$ *and if* $4mnpq$ *doesn't be square, so we should have:*

$$\theta = \lfloor mp + nq - 2\sqrt{mnpq} \rfloor + 1 = mp + nq + \lfloor -\sqrt{4mnpq} \rfloor + 1$$

$$= mp + nq + \left(-\lfloor \sqrt{4mnpq} \rfloor - 1\right) + 1 = mp + nq - \lfloor \sqrt{4mnpq} \rfloor$$

$$\Rightarrow \beta(k,\theta) = (\lfloor \sqrt{4mnpq} \rfloor + \theta)^2 - 4mnpq = (mp - nq)^2. \qquad \blacksquare$$

For example, when $F = 17 \times 23 = 391$ *and propose m=5 and n=2, then we should have:*

$$\theta = \left\lfloor \left(\sqrt{mp} - \sqrt{nq}\right)^2 \right\rfloor + 1 = \left\lfloor \left(\sqrt{5 \times 17} - \sqrt{2 \times 23}\right)^2 \right\rfloor + 1 = 6 \text{ and } k = mn = 10 \Rightarrow$$

$$\beta(k,\theta) = \beta(10,6) = (125 + 6)^2 - 15640 = 1521 = 39^2$$

Generalized form of theorem 4: *For each non-prime natural numbers as* $F = pq\ (1 \le p < q)$*, if we have* $\tilde{k}_r = \sim(q/p) = m/n$ *and* $k = mn$*, then the value of* $\beta(k,1)$ *would be square whenever:*

$$\frac{(\sqrt{nq}-1)^2}{p} < m < \frac{(\sqrt{nq}+1)^2}{p}.$$

Proof: *From theorem* (3)*, we have:*

$$\begin{cases} \tilde{k}_r > k_r \Rightarrow mp - nq < 2\sqrt{nq} + 1 \Rightarrow mp < (\sqrt{nq} + 1)^2 \Rightarrow m < \dfrac{(\sqrt{nq} + 1)^2}{p} \\ \tilde{k}_r < k_r \Rightarrow nq - mp < 2\sqrt{mp} + 1 \Rightarrow nq < (\sqrt{mp} + 1)^2 \Rightarrow m > \dfrac{(\sqrt{nq} - 1)^2}{p} \end{cases}$$

$$\Rightarrow \frac{(\sqrt{nq}-1)^2}{p} < m < \frac{(\sqrt{nq}+1)^2}{p}. \qquad \blacksquare$$

According to $q = \sqrt{k_r F}$ *and* $P = \sqrt{\frac{F}{k_r}}$ *as well as assuming* $M_{max} = \frac{(\sqrt{nq}+1)^2}{p}$ *and* $M_{min} = \frac{(\sqrt{nq}-1)^2}{p}$*, if difference of* M_{min} *and* M_{max} *will be shown by* δ*, so we will get:*

$$\delta = M_{max} - M_{min} \Rightarrow \delta = \frac{4\sqrt{nq}}{p} = 4\sqrt{\frac{nF}{P^3}} = 4\sqrt[4]{\frac{k_r^3 n^2}{F}}.$$

If we propose $\tilde{k}_r = \frac{m}{n} = a \cdot \overline{b_1 b_2 \dots b_s} = \frac{\overline{ab_1 \dots b_s}}{10^s}$ *then by choosing* $n = 10^s$ *and* $= \overline{ab_1 \dots b_s}$ *,*

we should have:

$$\frac{(\sqrt{10^s q}-1)^2}{p} < m < \frac{(\sqrt{10^s q}+1)^2}{p} \quad or \quad \left(\frac{\sqrt{10^s F}-\sqrt{p}}{p}\right)^2 < m < \left(\frac{\sqrt{10^s F}+\sqrt{p}}{p}\right)^2$$

$$\Rightarrow \delta = \frac{4\sqrt{10^s q}}{p} = 4\sqrt{\frac{10^s F}{p^3}} = 4\sqrt[4]{\frac{k_r^3 \times 10^{2s}}{F}}$$

If we show the number of natural numbers that is located in interval (M_{min}, M_{max}) *by* N*, so for any* k_r *we should have:*

$$\lfloor M_{max} \rfloor - \lfloor M_{min} \rfloor = N \Rightarrow N - 1 < \delta < N + 1 \; or \;\; \delta - 1 < N < \delta + 1$$

In other way $\lfloor \delta \rfloor = N$ *or* $\lfloor \delta \rfloor = N - 1$*, therefore for each value of* s *and* N*, we can conclude:*

$$\sqrt[3]{\left(\frac{N-1}{4}\right)^4 \frac{F}{10^{2s}}} < k_r < \sqrt[3]{\left(\frac{N+1}{4}\right)^4 \frac{F}{10^{2s}}}$$

For any value of S *, we define* $k_{(s):i}$ *as below*

$$k_{(s):i} = \sqrt[3]{\left(\frac{i}{4}\right)^4 \frac{F}{10^{2s}}} \;\Rightarrow\; \begin{cases} N = 1 \;=>\; 1 \le k_r < k_{(s):2} \\ N = 2 \;=>\; k_{(s):1} \le k_r < k_{(s):3} \\ \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \\ N = i + 1 \;=>\; k_{(s):i} \le k_r < k_{(s):(i+2)} \end{cases}$$

Then for any $k_{(s):i}$ *we have:*

$$\begin{cases} \delta = \sqrt[4]{\frac{k_r^3 \times 10^{2s}}{F}} \\ k_{(s):1} = \sqrt[3]{\left(\frac{i}{4}\right)^4 \frac{F}{10^{2s}}} \end{cases} \;=>\; \delta = i \;=>\; N = i$$

Since we have $k_{(s):i} \le k_{(s-1):i}$*, therefore we should have:*

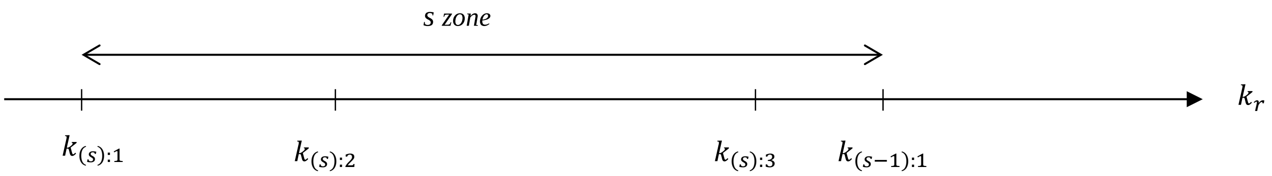
$$\sqrt[3]{\left(\frac{i}{4}\right)^4 \frac{F}{10^{2s}}} \leq \sqrt[3]{\left(\frac{1}{4}\right)^4 \frac{F}{10^{2(s-1)}}} \;=>\; i < \sqrt{10} \;=>\; i_{max} = \lfloor \sqrt{10} \rfloor = 3$$

We can calculate s_{max} *for F as below:*

$$\sqrt[3]{\left(\frac{1}{4}\right)^4 \frac{F}{10^{2s}}} = 1 => s = log\frac{\sqrt{F}}{16} => s_{max} = \left\lceil log\frac{\sqrt{F}}{16} \right\rceil$$

If we propose i as a natural number from zero to s_{max} *, then define s value as* $s = s_{max} - i$.

For any s we have:



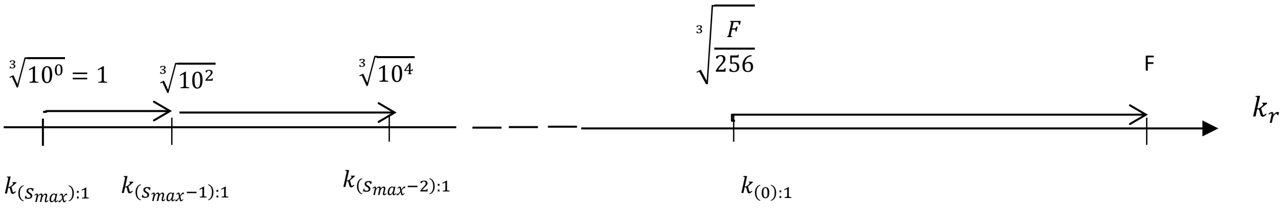
For any s we have:

$$k_{(s):1} = \sqrt[3]{\left(\frac{1}{4}\right)^4 \frac{F}{10^{2(s_{max}-i\,)}}} < \sqrt[3]{\left(\frac{1}{4}\right)^4 \frac{F}{10^{2(s-i\,)}}}$$

In this case from $s = log\frac{\sqrt{F}}{16}$ *we should have:*

$$k_{(s):1} < \sqrt[3]{10^{2i}}$$

Therefore:



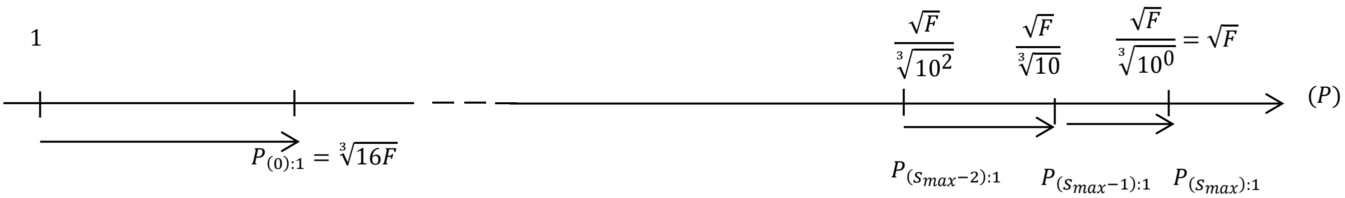
For calculated the value of $P_{(s):1}$ *,we should have:*

$$\begin{cases} P_{(s):1} = \sqrt{\dfrac{F}{k_{(s):1}}} \\ k_{(s):1} = \sqrt[3]{\left(\frac{1}{4}\right)^4 \frac{F}{10^{2s}}} \end{cases} \;=>\; P_{(s):1} = \sqrt[3]{16 \times 10^s \times F}$$

$$s_{max} = \left\lceil log\frac{\sqrt{F}}{16} \right\rceil \;,\; s = s_{max} - i \quad => \quad P_{(s):1} > \frac{\sqrt{F}}{\sqrt[3]{10^i}}$$

Therefore:

$$\frac{\sqrt{F}}{\sqrt[3]{10^{s_{max}}}}$$


1
$\frac{\sqrt{F}}{\sqrt[3]{10^2}}$
$\frac{\sqrt{F}}{\sqrt[3]{10}}$
$\frac{\sqrt{F}}{\sqrt[3]{10^0}} = \sqrt{F}$
(P)
$P_{(0):1} = \sqrt[3]{16F}$
$P_{(s_{max}-2):1}$
$P_{(s_{max}-1):1}$
$P_{(s_{max}):1}$

Since $s_{max} = \left[log\frac{\sqrt{F}}{16}\right]$, *thus for any* s_{max}, *we have* $256 \times 10^{2(s_{max}-1)} < F \leq 256 \times 10^{2s_{max}}$

Therefore in $\beta(k, 1)$ *test we can do as bellow:*

$k_{(s):1} < k_r < k_{(s-1):1} => n = 10^s \ => \ k = 10^s m$

If $k_r = n^2$ *, by choose* $1 \leq n < \sqrt[3]{10}$ *, then* k_r *located in* s_{max} *zone because we have* $< \sqrt[3]{100}$.

We can observe in any s zone for a natural number as F, when the value of F increases, then the difference between $\sqrt{F}$ *and* $p_{(s):1}$ *increases, because :*

$$\sqrt{F} - p_{(s):1} = \sqrt{F} - p_{(s_{max}-i):1} = \sqrt{F} - \frac{F}{\sqrt[3]{10^i}} = \sqrt{F}\left(1 - \frac{1}{\sqrt[3]{10^i}}\right)$$

3.Introducing $\alpha - s$ *Sieve*

Since for each odd composite number we have:

$$\begin{cases} F = pq \quad , & 3 \leq p \leq q \\ P = 2x + 1 \ , & q = 2y + 1 \end{cases} \Rightarrow F = 4xy + 2(x + y) + 1 = 2k + 1$$

Therefore, if we propose S=x+y+1 and R=xy, then we will have:

$$K = \frac{F - 1}{2} = 2\,xy + \ x + y \ = 2R + S - 1$$

By assuming $\alpha = S^2 - F$ *so that* α *becomes a square number, we will to have:*

$$S = \frac{p + q}{2} \Rightarrow \ \alpha = S^2 - F = \left(\frac{p + q}{2}\right)^2 - pq = \left(\frac{p - q}{2}\right)^2$$

In general case, for each value of S, we can obtain its corresponding p as follows:

$$S = \frac{p + q}{2} \Rightarrow q = 2S - p \Rightarrow F = pq = p(2S - p) \Rightarrow \begin{cases} P = S - \sqrt{S^2 - F} \\ q = S + \sqrt{S^2 - F} \end{cases}$$

Therefore by assuming $\alpha = S^2 - F = t^2$, *we will have* $P = S - t$ *and* $q = S + t$.

For any F=p q we can conclude that $S = \frac{F+p^2}{2p}$ *or* $S = \left(\frac{k_r+1}{2}\right)\sqrt{\frac{F}{k_r}}$ *and for any of the two different values of P, we have:*

doi:10.20944/preprints202009.0742.v1

$$p_1 < p_2 \Rightarrow S_{p_1} > S_{p_2} \Rightarrow \Delta S_{p_1,p_2} = S_{p_1} - S_{p_2} = \frac{\Delta p}{2}\left(\frac{F}{p_1 p_2} - 1\right)$$

It is seen that for one definite number as F and a constant value of Δp*, with increase in values of* p_1 *and* p_2*, the* Δ *S is decreased. In other words, with decrease in p values, the* S_p *values, increase.*

When the difference between S_p *and* $S_{\sqrt{F}}$ *is represented by n, we will have:*

$$n = S_p - S_{\sqrt{F}} = \frac{F + p^2}{2p} - \sqrt{F} \Rightarrow n = \frac{\left(\sqrt{F} - p\right)^2}{2p} \Rightarrow \begin{cases} p = \left(n + \sqrt{F}\right) - \sqrt{(n + \sqrt{F})^2 - F} \\ q = \left(n + \sqrt{F}\right) + \sqrt{(n + \sqrt{F})^2 - F} \end{cases}$$

In this case we have:

$$S = \frac{p+q}{2} = \lfloor \sqrt{F} \rfloor + n \Rightarrow \ \alpha = S^2 - F = t^2 = \left(\frac{p-q}{2}\right)^2$$

By considering the points mentioned, we can recommend a sieve to identify an odd composite number is prime or composite. This is based on the premise that if we are able to find values of S in a way that the value of α becomes square, therefore F will be a composite number.

By considering the relation K=2R+S-1 we will have:

$$\left| \begin{array}{l} k = \ an\ odd\ number \ \Rightarrow \ S = \ an\ even\ number \\ \\ k = an\ even\ number \ \Rightarrow \ S = \ an\ odd\ number \end{array} \right.$$

The process of calculating the value of $\alpha = S^2 - F$ *and establishing the fact that whether it is square numbers or not, is called α test. Any interval of 10 consecutive S is called the test domain. The reason for defining such a concept as the test domain is due to the repetition of the first digit on the right side of S values in it. For any natural odd number as F, considering the oddness or evenness of K and the digit on the right side of it, a unique array for values of S can be stated as follows; in which o represents the oddness of S and e represents the evenness of it. Therefore for any odd number in the form of* $F = \overline{\ldots f_2 f_1}$ *on the condition that K is even or odd, we define* $S^{f_1}_{e\ or\ o}$ *as*

$S^{f_1}_{e\ or\ o}$ *= (digits on the right side of S in one domain).*

Therefore, for different cases, we have:

$$F = 2k + 1 = \overline{\ldots 1} \ \Rightarrow \begin{cases} k = odd\ , \ \ S^1_e = (0{,}4\ {,}6) \\ k = even \ \ , S^1_o = (1\ {,}5\ {,}9) \end{cases}$$

$$F = 2k + 1 = \overline{\ldots 3} \ \Rightarrow \begin{cases} k = odd \ \ , \ \ S^3_e = (2\ {,}8\ ) \\ k = even \ \ , \ S^3_o = (3\ {,}7\ ) \end{cases}$$

$$F = 2k + 1 = \overline{\dots 7} \Rightarrow \begin{cases} k = odd \quad , \quad S_e^7 = (4\,,6) \\ k = even \quad , \quad S_o^7 = (1\,,9) \end{cases}$$

$$F = 2k + 1 = \overline{\dots 9} \Rightarrow \begin{cases} k = odd \quad , \quad S_e^9 = (0\,,2\,,8) \\ k = even \quad , \quad S_o^9 = (3\,,5\,,7) \end{cases}$$

It is noteworthy to mention that in this sieve by finding the first response point, the compositeness of the F number will become obvious. From now the S of any response point will be represented by S_r. *In this case we will have* $S_r = S_{min} + (n-1) \times 10$.

Here n represents the number of the test domain which contains the response point (or S_r) *and* S_{min} *also is the value of S in first test domain which has a digit on the right side equal to* S_r.*Therefore for each response point we will have* $S_r = \frac{p+q}{2}$.

For any α test, we will eliminate the values of S in test domains as much as possible. In other words, some values of S for which α does not become square number (or perfect square) will be eliminated. These processes of eliminating the S values and reaching the response points are called α - S sieve. When F has more than two numbers as p, then the probability of reaching the first response point will be much. One of the significant points about this sieve is the increase in density of the existence probability of P values by decreasing S value. In order to establish the compositeness of an odd number, we only need to reach the first response point.

One of the benefits of this sieve is the fact that in many cases we do not need α test for all values of S in order to identify whether α is a square number. By using only a few digits on the right side of S and F, then we will be able to eliminate many values of S. If $\alpha = \overline{e_m e_{m-1} \dots e_3 e_2 e_1}$*is a prefect square number, then we will be able to use the following notes in this sieve.*

Note 3: e_1 *can only have the values as 0, 1, 4, 5, 6, 9.*

Note 4: *If* e_1*=5, then* $E_3 = \overline{e_3 e_2 e_1}$ *must be as one of the member of the set* $\{025,\ 225, 625\}$. *For proving, by assume* $\alpha = (\overline{\dots l_3 l_2 l_1})^2$ *we should have:*

$$(\overline{l_3 l_2 l_1})^2 = (\overline{l_3 l_2 5})^2 = 10^4 l_3^2 + (2 l_1 l_3 + l_3) \times 10^3 + (l_2^2 + l_2) \times 10^2 + 5^2$$

$$\Rightarrow \begin{cases} \overline{e_2 e_1} = 5^2 = \overline{25} \\ e_3 = l_2^2 + l_2 \text{ و } l_2 : 0 \rightarrow 9 \Rightarrow e_3 \in \{0,2,6\} \end{cases}$$

Note 5: *If* e_1*=0, then* $E_3 = \overline{e_3 e_2 e_1}$ *will necessarily a member of the set* $\{000,100,400,500,600,900\}$.

For perfect square numbers with the digit zero on their right side, the number of zeros on their right side must always be even.

Note 6: *In the case that α is an even number, we have* $E_3 - 0 = 8m$ *or* $E_3 - 4 = 8m$ *and in the case* *that α is an odd number, we have* $E_3 - 1 = 8m$.

Therefore, by selecting E_N for big value of N we can eliminate more test points in a way that fewer test points will remain for α test and this is very suitable for large numbers. In doing so, we will utilize the following theorems.

Theorem 7*: If the natural number as $\alpha = \overline{e_M e_{M-1} \dots e_3 e_2 e_1}$ is a square number and the N digit on the right side is represented by E_N=$\overline{e_N e_{N-1} \dots e_2 e_1}$, then in a way that α is odd, we have:*

$$E_N - (2i-1)^2 = 2^N m_i \qquad (1 \le i \le 2^{N-3} \text{ و } N > 3)$$

and in a way that α is even, we have:

$$E_N - (2i-2)^2 = 2^N m_i \qquad (1 \le i \le 2^{N-3} \text{ و } N > 3)$$

(m_i is a natural number)

Proof*: Since any natural number can be represented by $2k_r + l_r$ in a way that if the number is even, then $l_r = 0$ and if it is odd, then $l_r = 1$ and that k_r is a non-negative integer number; therefore, by assuming that Δ is a perfect square number, we will have:*

$$\alpha = \overline{e_M e_{M-1} \dots e_3 e_2 e_1} = (2k_1 + l_1)^2 = (2(2k_2 + l_2) + l_1)^2 \quad = (2(2(2k_3 + l_3) + l_2) + l_1)^2$$

$$= \cdots = [2^N k_N + (2^{N-1} \times l_N + 2^{N-2} \times l_{N-1} + \cdots + 2l_2 + l_1)]^2$$

We will continue the operation above until the value of k_r in $2k_r + l_r$ equal to 1.

When we assume:

$$A = 2^{N-1} \times l_N + 2^{N-2} \times l_{N-1} + 000 + 2l_2 + l_1$$

It can be seen that A equivalent to a number in base 2 as below:

$$A = (\overline{l_N l_{N-1} \dots l_3 l_2 l_1})_2$$

Therefore:

$$\alpha = (2^N k_N + A)^2 = (2^N k_N^2 + 2k_N A) \times 2^N + A^2$$

By assuming $T = 2^N k_N^2 + 2k_N A$,we will have:

$$\alpha = T \times 2^N + A^2 \qquad (1)$$

On the other hand, we can write:

$$\alpha = \overline{e_M e_{M-1} \dots e_3 e_2 e_1} = \overline{e_M e_{M-1} \dots e_{N+1}} \times 10^N + \overline{e_N e_{N-1} \dots e_1}$$

By assuming $E_N = \overline{e_N e_{N-1} \dots e_1}$ and $S = \overline{e_M e_{M-1} \dots e_{N+1}}$, we will have:

$$\alpha = S \times 10^N + E_N \qquad (2)$$

From (1) and (2) we can conclude that:

$$E_N - A^2 = (T - S \times 5^N) \times 2^N = 2^N \times Q$$

It means that 2^N *counts the number* $E_N - A^2$.

Since we have:

$$A_{max} = (\overline{111\ldots1})_2 = 2^{N-1} + 2^{N-2} + \cdots + 2 + 1 \Rightarrow A_{max} = 2^N - 1$$

Therefore the number of the tests that we can do in a definite E_N *will be as below:*

$$\left|\begin{array}{l} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ E_N - (2n_1 - 1)^2 = 2^N m_{n_1} \end{array}\right.$$

Thus we will have:

$$2^N - 1 = 2n_1 - 1 \;\Rightarrow\; n_1 = 2^{N-1}$$

Therefore:

$$E_N - (2i - 1)^2 = 2^N m_i \quad , \qquad 1 \le i \le 2^{N-1}$$

For the case that α *is even, we have* $l_1 = 0$ *and its proof is like the previous one; then for this case we will have:*

$$A_{max} = (\overline{111\ldots1})_2 = 2^{N-1} + 2^{N-2} + \cdots + 2 + 0 \Rightarrow A_{max} = 2^N - 2$$

Therefore, the number of E_N *tests, when* Δ *is even, will be as below:*

$$\left|\begin{array}{l} E_N - 0^2 = 2^N m_1 \\ E_N - 2^2 = 2^N m_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots.... \\ E_N - (2n_1 - 2)^2 = 2^N m_{n_1} \end{array}\right.$$

Thus we have:

$$2^N - 2 = 2n_1 - 2 \;\Rightarrow\; n_1 = 2^{N-1}$$

Then in general case we will have:

$$E_N - (2i - 2)^2 = 2^N m \quad , \; 1 \le i \le 2^{N-1}$$

To continue the proof, we first consider a case in which α *is odd and for a definite* E_N *test with the arrangement of A values in ascending order, therefore we should have:*

$$\left|\begin{array}{l} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots. \\ E_N - (2x-1)^2 = 2^N m_x \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ E_N - (2y-1)^2 = 2^N m_y \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ E_N - (2n_1-1)^2 = 2^N m_{n_1} \end{array}\right.$$

Since we have $\Delta A_{max} = (2n_1 - 1) - (-1) = 2n_1 = 2^N$ *therefore for two value of A with difference* 2^{N-1} *so that* $(2x-1) = 2 \times 2^{N-2} - i$ *and* $(2y-1) = 2 \times 2^{N-1} - i$ *(when i is a odd number and located in interval from 1 to* $2^{N-1} - 1$ *) then we have:*

$$(2y-1)^2 - (2x-1)^2 = (2^{N-1}) \times (2x + 2y - 2) = 2^N (y + x - 1)$$

Therefore the number of E_N *tests can be calculated by* $n_2 = 2^{N-2}$.

In an ascending arrangement of the A values, for both of its values which lie in a symmetrical position, we will have:

$$\left|\begin{array}{l} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots. \\ E_N - [2(i+1)-1]^2 = 2^N m_{i+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ E_N - [2(n_2 - i) - 1]^2 = 2^N m_{n_2 - i} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ E_N - [2n_2 - 3]^2 = 2^N m_{n_2 - 1} \\ E_N - [2n_2 - 1]^2 = 2^N m_{n_2} \end{array}\right.$$

$$\Rightarrow \quad [2(n_2 - i) - 1]^2 - [2(i+1) - 1]^2 = (2n_2 - 4i - 2)(2n_2)$$

$$= (2 \times 2^{N-2} - 4i - 2)(2 \times 2^{N-2}) = (2^{N-2} - 2i - 1) \times 2^N$$

Since the result of $(2^{N-2} - 2i - 1)$*is positive, then N must be a number greater than 3. Therefore the total number of the remaining values of A decreases from* 2^{N-2}*to* 2^{N-3} *,which is represented by* n_N.

Thus in general case when α *is odd, for every* E_N *test we will have:*

$$\left|\begin{array}{l} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots. \\ E_N - (2n_N - 1)^2 = 2^N m_{n_N} \end{array}\right.$$

Then the total number of E_N *tests equal to* $n_N = 2^{N-3}$.

For the case in which α *is even, the proof process is completely similar and for each* E_N *test we have:*

$$\left|\begin{array}{l} E_N - 0^2 = 2^N m_1 \\ E_N - 2^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots. \\ E_N - (2n_N - 2)^2 = 2^N m_{n_N} \end{array}\right.$$

In a way that the total number of each E_N test is calculated like that of the previous case, thus we will have $n_N = 2^{N-3}$, therefore the proof is complete.■

***Theorem 8**: When $E_N - x^2$ by assuming that $E_N = \overline{a_N a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$ can be counts by 2^N, and when we replace a_N with another digit like as $\acute{a_N}$ and represent the result of $\overline{\acute{a_N} a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$ by $\acute{E_N}$, therefore $\acute{E_N} - x^2$ can also count 2^N.*

***Proof**: If in $E_N = \overline{a_N a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1} = 2^N + x^2$,we replace a_N with the digit $\acute{a_N}$ in a way that a $\acute{a_N} = a_N \pm r$, and r can have one of the digits from 1 to 9, then we will have:*

$$\acute{E_N} = \overline{\acute{a_N} a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1} = \overline{(a_N \pm r) a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$$

$$= \overline{(a_N \pm r) a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1} = ((\pm r) \times 10^{N-1} + \overline{a_N a_{N-1} \dots a_1}\ \ )^2 - \overline{f_N f_{N-1} \dots f_1}$$

$$= r^2 \times 10^{2N-2} \pm 2r \times 10^{N-1} \times \overline{a_N a_{N-1} \dots a_1} + \overline{a_N a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$$

$$. = (r^2 \times 5^{2N-2} \times 2^{N-2} \pm r \times 5^{N-2} \times \overline{a_N a_{N-1} \dots a_1}) \times 2^N + \overline{a_N a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$$

By assuming $T = r^2 \times 5^{2N-2} \times 2^{N-2} \pm r \times 5^{N-2} \times \overline{a_N a_{N-1} \dots a_1}$, we will have:

$$\acute{E_N} = T \times 2^N + E_N \Rightarrow \acute{E_N} = T \times 2^N + 2^N m + x^2 \ \ \Rightarrow \acute{E_N} - x^2 = (T + m) \times 2^N$$

It means $\acute{E_N} - x^2$ can be count by 2^N and the proof is complete. ■

***Note 7**: When the values of E_N are even, we can decrease the number of E_N test. As an example, for E_5 to E_7 we have:*

$$N = 5 \ \Rightarrow \left|\begin{array}{l} E_5 - 0^2 = 32m \\ E_5 - 2^2 = 32m \\ E_5 - 4^2 = 32m \end{array}\right. , \quad N = 6 \ \Rightarrow \left|\begin{array}{l} E_6 - 0^2 = 64m \\ E_6 - 2^2 = 64m \\ E_6 - 4^2 = 64m \\ E_6 - 6^2 = 64m \end{array}\right. , N = 7 \ \Rightarrow \left|\begin{array}{l} E_7 - 0^2 = 128m \\ E_7 - 2^2 = 128m \\ E_7 - 4^2 = 128m \\ E_7 - 6^2 = 128m \\ E_7 - 8^2 = 128m \\ E_7 - 10^2 = 128m \\ E_7 - 14^2 = 128m \end{array}\right.$$

In this sieve we can use theorems 7 and 8 in E_N tests as below.

$$if\ \ E_l^-\, then \left|\begin{array}{l} \overline{0a_{l-1} \dots a_1}\boxtimes \\ \overline{1a_{l-1} \dots a_1}\boxtimes \\ \qquad . \\ \qquad . \\ \qquad . \\ \overline{9a_{l-1} \dots a_1}\boxtimes \end{array}\right. \begin{array}{l} \textit{All the S} \\ \textit{values} \\ \textit{eliminated} \\ \textit{from } E_{l+1} \\ \textit{tests.} \end{array} \qquad , \qquad if\ \ E_l^+\, then \left|\begin{array}{l} \overline{0a_{l-1} \dots a_1} \\ \overline{1a_{l-1} \dots a_1} \\ \qquad . \\ \qquad . \\ \qquad . \\ \overline{9a_{l-1} \dots a_1} \end{array}\right. \begin{array}{l} \textit{All the S values} \\ \textit{remain for } E_{l+1} \\ \textit{tests.} \end{array}$$

Theorem 9: *When E_N test for a definite S is positive, then E_{N-r} test is positive for that S.*

Proof*: From theorem (4) we have:*

$$E_N - x^2 = 2^N m \Rightarrow \overline{e_N e_{N-1} \dots e_1} - x^2 = 2^N m_1$$

$$\Rightarrow \overline{e_N e_{N-1} \dots e_{N-r+1}} \times 10^{N-r} + \overline{e_{N-\iota} \dots e_1} - x^2 = 2^N m_1$$

$$\Rightarrow \overline{e_{N-\iota} \dots e_1} - x^2 = 2^N m_1 - \overline{e_N e_{N-1} \dots e_{N-r+1}} \times 5^{N-r} \times 2^{N-r}$$

$$.= 2^{N-i}\left(2^i m_1 - \overline{e_N e_{N-1} \dots e_{N-r+1}} \times 5^{N-r}\right) = 2^{N-r} m_2 \Rightarrow E_{N-r} - x^2 = 2^{N-r} m_2$$

It means the number 2^{N-r} counts $E_{N-r} - x^2$. In other words E_{N-r} test is positive and the proof is complete. ■

Therefore in every E_N test for a definite S except for values of x for which E_{N-1} test is positive, all the tests related to the other values of x are eliminated from the E_N tests. Thus total number of E_N tests can be calculated as follows:

$$n_{E_N} \approx 2^{N-3} - 2^{N-4} + 1 = 2^{N-4} + 1$$

Theorem 10*: If $E_N - x^2 = 2^N m$, i.e. E_N test will be positive, then $E_M - x^2$ for each M greater than N can be count by 2^N.*

Proof*:*

$$E_N - x^2 = 2^N m \Rightarrow \overline{e_N e_{N-1} \dots e_1} - x^2 = 2^N m_1 \Rightarrow \overline{e_M e_{M-1} \dots e_{N+1}} \times 10^N + \overline{e_N e_{N-1} \dots e_1} - x^2$$

$$= 2^N m_1 + \overline{e_M e_{M-1} \dots e_{N+1}} \times 10^N = 2^N (m_1 + \overline{e_M e_{M-1} \dots e_{N+1}} \times 5^N) = 2^N m_2$$

$$\Rightarrow \overline{e_M e_{M-1} \dots e_2 e_1} - x^2 = 2^N m_2 \Rightarrow E_M - x^2 = 2^N m_2$$

It means that the 2^N counts $E_M - x^2$ and the proof is complete. ■

In E_N tests for a definite S, only for a one value of x, the test result is positive. It is because if we assume for the two different values x_1 and x_2 the test result is positive, then it means x_1 and x_2 will have the same outcome.

Theorem 11*: If values of E_N for two values of S with a difference equal to10 ,from the two domains of the consecutive test is represented by $E_{N(i+1)}$and $E_{N(i)}$ in a way that i represents the number of the test domain, then values of $\Delta E_{N(i,i+1)} = E_{N(i+1)} - E_{N(i)}$for the two consecutive domains of the $E_N$tests form an arithmetic progression with 200 as common difference.*

Proof*: From E_N definition , we have:*

$$\begin{cases} E_{N(1)} = S_{min}^2 - \overline{f_N \dots f_1} \\ E_{N(i)} = (S_{min} + 10(i-1))^2 - \overline{f_N \dots f_1} \end{cases} \Rightarrow \quad E_{N(i)} = E_{N(1)} + 20(i-1)S_{min} + 100(i-1)^2$$

$$\Rightarrow \begin{cases} E_{N(i+1)} = E_{N(1)} + 20iS_{min} + 100i^2 \\ E_{N(i)} = E_{(N)1} + 20(i-1)S_{min} + 100(i-1)^2 \\ E_{N(i-1)} = E_{N(1)} + 20(i-2)S_{min} + 100(i-2)^2 \end{cases} \Rightarrow \begin{cases} \Delta E_{N(i-1,i)} = 20S_{min} + 100(2i-3) \\ \Delta E_{N(i,i+1)} = 20S_{min} + 100(2i-1) \end{cases}$$

$$\Rightarrow \Delta E_{N(i,i+1)} - \Delta E_{N(i-1,i)} = 200$$

It means the values of $\Delta E_{N(i,i+1)}$ *forms an arithmetic progression with 200 as common difference value.* ■

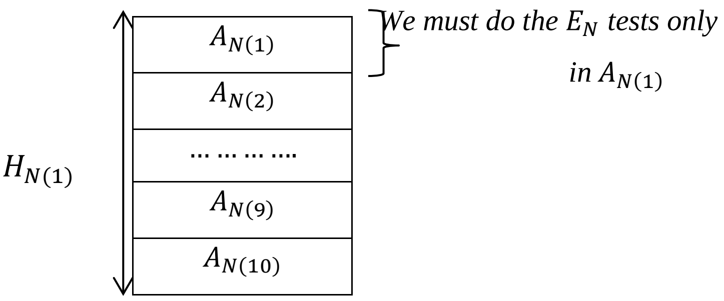
Therefore we will have:

$$X = \Delta E_{N(1,2)} \xrightarrow{+200} \Delta E_{N(2,3)} \xrightarrow{+200} \Delta E_{N(3,4)} \xrightarrow{+200} \dots$$

$$\Rightarrow E_{N(1)} \xrightarrow{X} E_{N(2)} \xrightarrow{X+200} E_{N(3)} \xrightarrow{X+2\times 200} E_{N(4)} \xrightarrow{X+3\times 200} E_{N(5)} \longrightarrow \cdots$$

$$\Rightarrow E_{N(i)} - E_{N(i-1)} = X + (i-2)\times 200 \Rightarrow E_{N(i)} = E_{N(1)} + (i-1)X + (i-1)(i-2)\times 100$$

If we represent the i th group of the S values with the number 10^N *by* $H_{N(i)}$ *and the j th group of the S values with the number* 10^{N-1} *by* $A_{N(j)}$*, in a way that i in them is from 1 to* $\left\lceil\frac{S_{max}-S_{min}}{10^N}\right\rceil$ *and j is from 1 to 10, then according to theorem 8 it will suffice to do the* E_N *tests only for* $A_{N(1)}$*,i.e. the first group with the number* 10^{N-1}*in the* $H_{N(1)}$*group. If the test result for one definite S in* $A_{N(1)}$ *will be positive, it means the result of this test is positive for all the S values that contain N-1 similar digits on the right side and are only different in the first digit on the left side and are located in other nine groups of A. But if the result of* E_N *test is negative for one of the S values in* $A_{N(1)}$*, then this test is negative for all the S values which are only different in their first digit on the left side and are located in the other nine groups of A. If in the first* $A_{N(1)}$ *all the tests of* E_N *are negative, it means that the odd number under the test is a prime number.*



If we assume that the number of E_N^+ *tests in* $A_{N(1)}$ *is equal to w, then the total number of α tests in* $\alpha - S$ *sieve can be calculated by* $n_{\alpha - E_N^+} = \left\lceil\frac{S_{max}-S_{min}}{10^N}\right\rceil \times 10w$ *.*

Note 8*: If* $\alpha = \overline{e_m e_{m-1} \dots e_3 e_2 e_1}$ *will be a prefect square number, then we must to have:*

$\sum_{i=1}^{m} e_i = 9k^2 \sum_{i=1}^{m} e_i = 3k+1$ *or*

In the $\alpha - S$ sieve it is better to do the E_N tests for the two value of N_1 and N_2 in which N_1 is less than N_2 so that we should have fewer E_N tests.

D	S	E_{N_1}	E_{N2}	$test\alpha$
D_1				
D_2				
....	....	....	....	....

If for very large numbers, E_N tests are done by bigger value of N ,Then the number of α tests will be decreased. It should be noted that working on some digits on the right side of a large number is much easier than working on all of its digits and takes much less time. We can observe the number of E_N tests will be rigorous decreased, which is one of the important properties of this sieve.

Example 2: Show that $F = 251,953,878,652,772,860,514,325,499,229$ *is a composite number.*

Answer

$$\lfloor\sqrt{F}\rfloor = 501,950,075,865,935\ , k = \frac{F-1}{2} = even\ , S_{min} = 501,950,075,865,927 \Rightarrow S_O^9 = (3,5,7)$$

The first set of S by 10^3 *length*		E_3	E_5 E_5
D_1	*501,950,075,865,927*	$E_3 = \overline{100} \longrightarrow E_3^+$	$E_5^- \longrightarrow$ ☒
	501,950,075,865,933	$E_3 = \overline{260} \longrightarrow$ ☒	
	501,950,075,865,935	$E_3 = \overline{996} \longrightarrow$ ☒	$E_5^- \longrightarrow$ ☒
D_2	*501,950,075,865,937*	$E_3 = \overline{740} \longrightarrow$ ☒	
	501,950,075,865,943	$E_3 = \overline{020} \longrightarrow$ ☒	
	501,950,075,865,945	$E_3 = \overline{796} \longrightarrow E_3^+$	$E_5^- \longrightarrow$ ☒
D_3	*501,950,075,865,947*	$E_3 = \overline{580} \longrightarrow$ ☒	
	501,950,075,865,953	$E_3 = \overline{980} \longrightarrow$ ☒	
	501,950,075,865,955	$E_3 = \overline{796} \longrightarrow E_3^+$	$E_5^- \longrightarrow$ ☒
D_4	*501,950,075,865,957*	$E_3 = \overline{630} \longrightarrow$ ☒	
	501,950,075,865,963	$E_3 = \overline{140} \longrightarrow$ ☒	
	501,950,075,865,965	$E_3 = \overline{996} \longrightarrow E_3^+$	$E_5^- \longrightarrow$ ☒

D_5	*501,950,075,865,967*	$E_3 = \overline{860} \longrightarrow \boxtimes$	
	501,950,075,865,973	$E_3 = \overline{500} \longrightarrow \boxtimes$	
	501,950,075,865,975	$E_3 = \overline{396} \longrightarrow E_3^+$	$E_5^- \longrightarrow \boxtimes$

It can be seen that for S=504,037,195,361,823, α is a perfect square number and for this first S_r we have:

$$S_r = 504{,}037{,}195{,}361{,}823 \to \alpha = S_r^2 - F = t^2 \Rightarrow\Rightarrow \begin{cases} p = 458{,}215{,}632{,}147{,}113 \\ q = s594{,}858{,}758{,}576{,}533 \end{cases}$$

It is observed that only by E_5 test , the S values are eliminated from 5 domains.

The most important notes regarding to the $\alpha - S$ sieve are mentioned as follows:

***1.** There is no need to know the prime numbers less than the square root of the number under test.*

2**. The results of E_N tests do not depend on the largeness of the numbers under test. They only depend on the type and the arrangement of N digits on the right side**.

***3**. When we use $E_N$test for N digits on the right side of a definite S in a way that the test result becomes negative, all the S values which contain $N-1$ similar digits on the right side, will be eliminated from the α test.*

***4**. For large numbers, by this sieve, we will reach the answer more quickly and more easily than by tests divisibility test for prime numbers less than its square root. The largeness of the number allows us to do E_N tests for greater N value.*

***5**. We will not need time-consuming and big computations with this sieve because in E_N tests we only use N digits on the right side of the numbers.*

4.Introduce $\beta - s$ Sieve

Whenever by assuming$(1 \le p \le q)\ F = pq$ and $(1 \le n \le m) k = mn$ the result of $\beta(k,\theta)$ is a square number and by representing the phrase $\lfloor\sqrt{4kF}\rfloor + \theta$ by S, therefore the values of p and q can be calculated as follows:

$$\beta(k,\theta) = S^2 - 4kF = t^2 \implies \left| \begin{aligned} p &= \frac{S \mp t}{2m} \\ q &= \frac{S \pm t}{2n} \end{aligned} \right.$$

For any k values we can calculate the values of S and $\beta(k,\theta)$ by placing the consecutive values of natural numbers in $(\theta \ge 1)\theta$.By Considering the theorems and the notes mentioned, from a few number of digits on the right side of $\beta(k,\theta)$ value ,we will be able to eliminate many value of S from the test for which the result of $\beta(k,\theta)$ is not square. This method of sieve, in which by eliminating S values, we want that $\beta(k,\theta)$ to be a square number, is called $\beta - S$ sieve. In this sieve, we represent N digits on the right side *of $\beta(k,\theta)$ value by E_N and we do the E_N tests like $\alpha - S$ sieve. the sieving S values only from $k_r = 1$ to $k_r = \sqrt[3]{100}$ (in S_{max} zone), is equal to sieve the p values from $\sqrt{F}$ to $\frac{\sqrt{F}}{\sqrt[3]{100}}$ in probable interval containing p values.This is one of the most important benefits of this sieve. In this sieve for one definite θ and K, we can assume:*

$$\begin{cases} \lfloor\sqrt{4kF}\rfloor + \theta = S = \overline{\dots a_N \dots a_2 a_1} \\ 4kF = \overline{\dots b_N \dots b_2 b_1} \end{cases}$$

$$\Rightarrow \beta(k,1) = S^2 - 4kF = \overline{\dots e_N \dots e_2 e_1} \;\Rightarrow E_N = \overline{e_N \dots e_2 e_1}$$

If we represent the odd values of a_1 for b_1 by $S_o^{b_1}$ and the even values of a_1 for b_1 by $S_e^{b_1}$,thus we will have:

$$, \quad b_1 = 2 \Rightarrow \begin{cases} S_o^2 = (1{,}9) \\ S_e^2 = (4{,}6) \end{cases} \quad , \quad b_1 = 4 \Rightarrow \begin{cases} S_o^4 = (3{,}5{,}7) \\ S_e^4 = (0{,}2{,}8) \end{cases}, b_1 = 0 \Rightarrow \begin{cases} S_o^0 = (1{,}3{,}5{,}7{,}9) \\ S_e^0 = (0{,}2{,}4{,}6{,}8) \end{cases}$$

$$b_1 = 6 \Rightarrow \begin{cases} S_o^6 = (1{,}5{,}9) \\ S_e^6 = (0{,}4{,}6) \end{cases} \quad , \quad b_1 = 8 \Rightarrow \begin{cases} S_o^8 = (3{,}7) \\ S_e^8 = (2{,}8) \end{cases}$$

When the result of $\beta(k,1)$ is a square number, we will have:

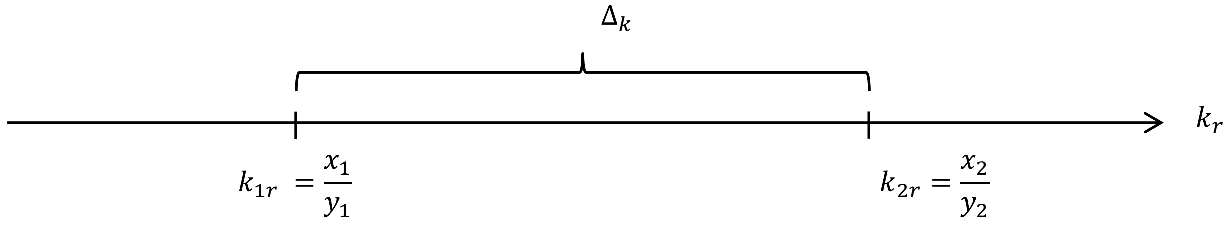
$$\beta(k,\theta) = S^2 - 4kF = (mp + nq)^2 - 4(mn)(pq) = (mp - nq)^2 = t^2$$

Therefore, when we have $S = mp + nq$, the value of $\beta(k,\theta)$ will be a square number and the desired S value, will be $S_r = mp + nq$. Considering that the values of m and n are odd or even, through k=mn we can determine if the values of S are odd or even.

$$\begin{cases} m = odd \\ n = odd \end{cases} \; or \; \begin{cases} m = even \\ n = even \end{cases} \;\Rightarrow S = even$$

$$\begin{cases} m = odd \\ n = even \end{cases} \; or \; \begin{cases} m = even \\ n = odd \end{cases} \;\Rightarrow S = odd$$

In order to use this sieve between two values of k_r, we will do as follows:



By calculating the minimum value of S in the sieve interval of Δ, we will have:

$$S_d = \lfloor\sqrt{4kF}\rfloor = \lfloor\sqrt{4x_1y_1F}\rfloor$$

To calculate the maximum value of S in the sieve interval of Δ, we will do as follows:

$$k_r = \frac{q}{p} = \frac{x_2}{y_2} \quad , \quad F = k_r p^2 \Rightarrow \begin{cases} p = \sqrt{\frac{F}{k_r}} = \sqrt{\frac{y_2F}{x_2}} \\ q = \frac{x_2}{y}\sqrt{\frac{y_2F}{x_2}} \end{cases} \Rightarrow S_u = x_1p + y_1q = (x_1 + x_2)\sqrt{\frac{y_2F}{x_2}}$$

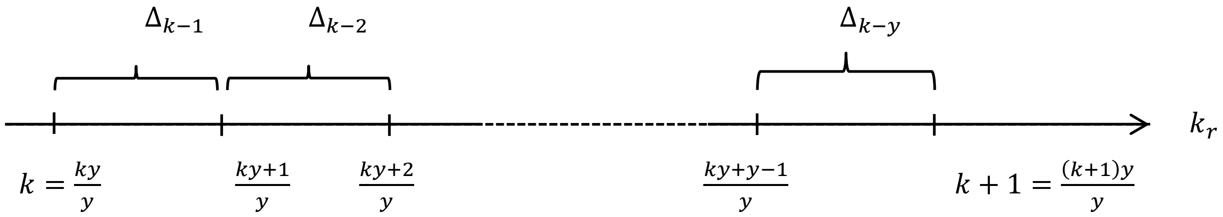
In the best case, If we consider x_1 and x_2 as consecutive integer number and $y_1 = y_2 = y$, then we *will have:*

$$, S_u = (2x_1+1)\sqrt{\frac{yF}{x_1+1}} S_d = \lfloor\sqrt{4x_1yF}\rfloor$$

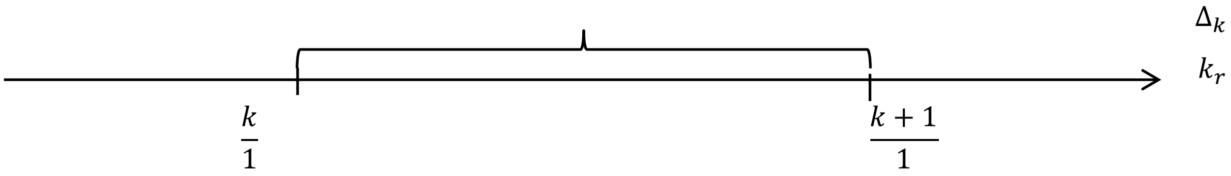
If one S_r *is located in the sieve interval of* Δ*, we represented it by* Δ_r*.For each* S_r *in a sieve interval of* Δ_r*, we have:*

$$\begin{cases} S_r = S_d + \theta = mp + nq \\ \theta = \lfloor(\sqrt{x_1p} - \sqrt{yq})^2\rfloor + 1 \end{cases} \Rightarrow \beta(k,\theta) = (mp-nq)^2 = t^2$$

In orders that the sieve should be easier, between the two consecutive integer values of k_r*, especially for big values of F, it is better to divide the distance into y equal parts in which each part is an independent sieve zone.*



Δ_{k-i} *represents the it h of sieve zone related to K. In a particular case when the distance between the two integer values of consecutive* k_r *is selected as one sieve zone, we will do as follows:*

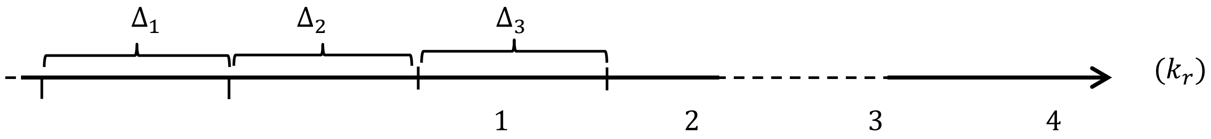


$$S_d = \lfloor\sqrt{4kF}\rfloor \quad , \quad S_u = \left\lceil (2k+1)\sqrt{\frac{F}{k+1}} \right\rceil$$

In zones of Δ_{k-i}*, the length of the sieve intervals is decreased by increasing the i. In other words:*

$$L_{\Delta_{k-i}} = S_{u_{k-i}} - S_{d_{k-i}} \Rightarrow L_{\Delta_{k-1}} > L_{\Delta_{k-2}} > L_{\Delta_{k-3}} > \cdots$$

Therefore, for the sieve zones between the consecutive integer values of k_r*, the length of the intervals are decreased.*



Therefore:

$$L_{\Delta_1} > L_{\Delta_2} > L_{\Delta_3} > \cdots$$

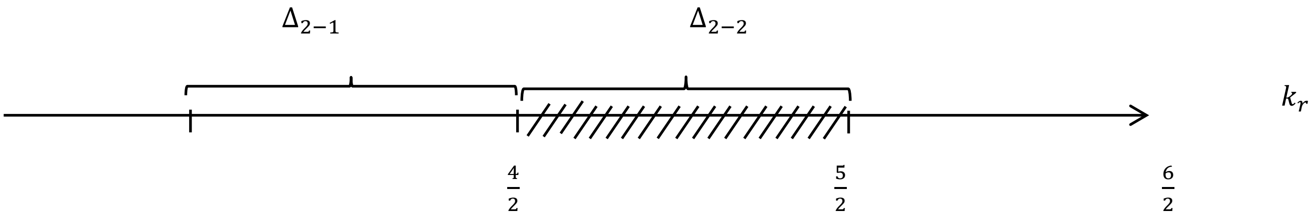
The decreasing of the length of consecutive sieve zones for k_r *values which are located in* $S = 0$ *zone ,finally to get at zero. In a way that for some consecutive integer value of* k_r*, the reslult of* $\beta(k,1)$ *will be a square number. With the increase in* k_r *values in this zone, the number of consecutive integer values of* k_r *are increased accordingly. Therefore it is only necessary to do a* $\beta(k,1)$ *test for one value of* k_r

based on the theorem(4). In general case, for an odd number as F, it is better to do the $\beta - S$ sieve as follows:

$k = 1 \; , \; \Delta_{1-1} \Rightarrow k_r = \frac{y}{y} \longrightarrow 4kF \longrightarrow S^{b_1}_{e \, or \, o} \; , \; S_{d_{1-1}} \; , \; S_{u_{1-1}}$				
D	S	E_{N_1}	E_{N_2}	
D_1				
D_2				
....	....	....	....	....
$k = 2 \; , \; \Delta_{2-1} \Rightarrow k_r = \frac{2y}{y} \longrightarrow 4kF \longrightarrow S^{b_1}_{e \, or \, o} \; , \; S_{d_{2-1}} \; , \; S_{u_{2-1}}$				
D	S	E_{N_1}	E_{N_2}	
D_{2-1}				
D_{2-2}				
....	....	....	....	....

Example3: By selecting y=2and k=2 prove that $F = 9,640,669$ *is a composite number.*

Answer:



$$, \; S_{d_{2-1}} = 17,564 \quad , \quad S_{u_{2-1}} = \left\lceil 9\sqrt{\frac{2F}{5}} \right\rceil = 17,673 \quad 4kF = 4 \times 4 \times 2 \times F = 308,501,408$$

We can see, when $S = 17,626$ *then* β *is a prefect square number , since we have*

$$\beta = S_r^2 - 4kF = (17,622)^2 - 308,501,608 = 1426^2 = t^2$$

$$\left| \begin{array}{l} m = 4 \\ n = 2 \end{array} \right. \Rightarrow \left| \begin{array}{l} p = \frac{S-t}{2m} = \frac{17,622 - 1426}{2 \times 4} = 2381 \\ q = \frac{S+t}{2n} = \frac{17,622 + 1426}{2 \times 2} = 4049 \end{array} \right.$$

The important benefits of $\beta - S$ *sieve is that we can easily select a certain sieve zone within any distance from* k_r *values (from 1 to F). This is particularly very important for some values of* k_r *since it includes a large part of the interval containing the p values.*

Example4: By the $\beta - S$ *sieve show that the number* $F = 34,873,477$ *in the sieve zone of* Δ_{3-1} *has an response point.*

Answer

$k = 3$, $12F = 418,481,724$, $S_{d_{3-1}} = 20,456$, $S_{u_{3-1}} = 20,668$

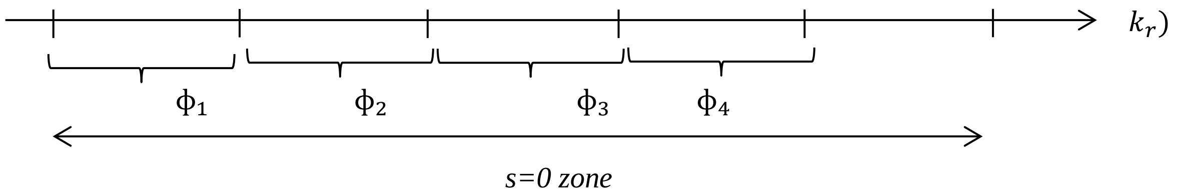
D	S	E_3	β *tests*
D_{3-1}	*20, 458*	$\overline{040} \longrightarrow$ ☒	——
	20, 460	$\overline{776} \longrightarrow +$	$\beta \neq t^2$
	20, 462	$\overline{720} \longrightarrow$ ☒	——
D_{3-2}	*20, 468*	$\overline{300} \longrightarrow$ ☒	——
	20, 470	$\overline{176} \longrightarrow +$	$\beta \neq t^2$
	20, 472	$\overline{060} \longrightarrow$ ☒	——
D_{3-3}	*20,478*	$\overline{760} \longrightarrow$ ☒	——
	20, 480	$\overline{676} \longrightarrow +$	$\beta = 974^2 = t^2$
	20, 482	$\overline{600} \longrightarrow +$	$\beta \neq t^2$

In order to utilize the $\beta - S$ *sieve in the zone of* $S = 0$, *it will only suffice to use the integer values of* k_r, *located in this zone, as the k in* $\beta(k,1)$ *tests.*

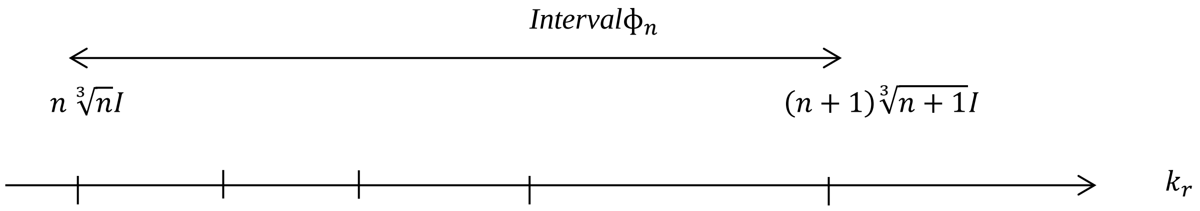
If the value of $\sqrt[3]{\frac{F}{256}}$ *is represented by I, therefore in the zone of S=0, from relations* $\delta = 4\sqrt[4]{\frac{k_r^3}{F}}$ *and* $k_{r(n)} = \sqrt[3]{\left(\frac{n}{4}\right)^4 F}$ *, we will have* $k_{r(n)} = n\sqrt[3]{n}I$ *then we can conclud that* $\delta = N = n$.

In a way that N represents the number of k values for one value of k_r *in order to have the same result for the* $\beta(k,1)$ *tests. Therefore it is suggested that the distance from I to F can be divided as follows:*

$k_r = I$ $\quad k_r = 2\sqrt[3]{2}I$ $\quad k_r = 3\sqrt[3]{3}I$ $\quad k_r = 4\sqrt[3]{4}I$ $\quad k_r = 5\sqrt[3]{5}I$ ……. $k_r = F$



In an arbitrary interval as Φ_n, *some values of k must be used in* $\beta(k,1)$*test which are obtained from the* $k_n + ni$ *in a way that* $k_n = \lceil n\sqrt[3]{n}I \rceil$ *is the minimum value of k and* $k_{n+1} = \lfloor (n+1)\sqrt{n+1}I \rfloor$ *is the maximum value of k.*



$$k_n = \lceil n\sqrt[3]{n}I\rceil \quad k_n + n \quad k_n + 2n \qquad k_n + 3n \qquad \dots \quad \lfloor (n+1)\sqrt[3]{n+1}I\rfloor = k_{n+1}$$

We represent the numbers of k that can be chose for $\beta(k,1)$*tests in* ϕ_n *interval by* N_n *,that is:*

$$N_n = \left\lceil \frac{(n+1)\sqrt[3]{n+1}I - n\sqrt[3]{n}I}{n} \right\rceil = \left\lceil \frac{L_n}{n} \right\rceil$$

It is observed that by increase in n, the length of the ϕ_n *intervals, i.e.* L_n *, will also increase. In other words we have:*

$$\left(2\sqrt[3]{2}I - I\right) < \left(3\sqrt[3]{3}I - 2\sqrt[3]{2}I\right) < \left(4\sqrt[3]{4}I < 3\sqrt[3]{3}I\right) < \cdots \Rightarrow L_1 < L_2 < L_3 < \cdots < L_m < L_{m+1} < \cdots$$

$$\Rightarrow N_1 \ \geq N_2 \ \geq N_3 \ \geq \cdots \geq 1$$

In order to calculate the maximum value of n in S=0 zone, we will have:

$$(n+1)\sqrt[3]{n+1}I = \sqrt[3]{(n+1)^4} \times \sqrt[3]{\frac{F}{256}} = F \ \Rightarrow \ n_{max} = \lceil 4\sqrt{F}\rceil - 1$$

Therefore if we want to have N=1, from differential calculus, we have:

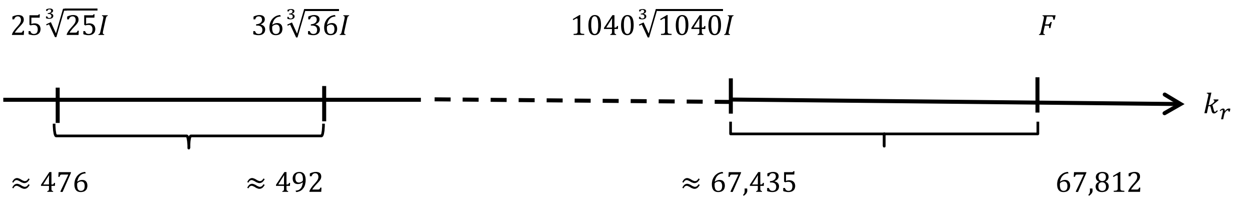
$$(n+1)\sqrt[3]{n+1}I - n\sqrt[3]{n}I = \left(\sqrt[3]{(n+1)^4} - \sqrt[3]{n^4}\right)I \approx \left(\frac{4}{3}\sqrt[3]{n}\right)I < n \Rightarrow n \geq \left\lceil \frac{\sqrt{3F}}{18} \right\rceil$$

As an example, for the number $F = 631,523$ *we will have* $\left\lceil \frac{\sqrt{3F}}{18} \right\rceil = 77$ *, therefore If n=77 then we should have:*

$$L_{77} = 78\sqrt[3]{78}I - 77\sqrt[3]{77}I = 76.737 \Rightarrow N_{77} = \left\lceil \frac{L_{77}}{77} \right\rceil = 1$$

It means that for values of n which are greater than 77, it will be suffice to select an integer number for the β *test in each* ϕ *intrval.*

For example, in S=0 zone, for the number $= 67{,}813$ *, we have:*



It is observed that:

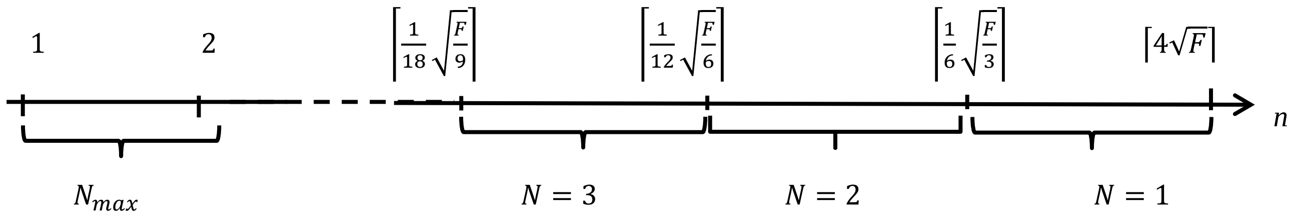
$$\begin{cases} L_{25} = 16 \\ N_{25} = 1 \end{cases} \quad , \dots\dots\dots\dots\dots\dots , \quad \begin{cases} L_{1040} = 378 \\ N_{1040} = 1 \end{cases}$$

From differential calculus, we know that:

$$f(n+\Delta n)-f(n)\approx f'(n)\Delta n\,, f(n)=\sqrt[3]{n^4}\,, f'(n)=\frac{4}{3}\sqrt[3]{n^4}$$

$$\Delta n=1 \quad \Rightarrow \quad \sqrt[3]{(n+1)^4}-\sqrt[3]{n^4}\approx\frac{4}{3}\sqrt[3]{n^4} \quad \approx\frac{nN}{I}=nN\sqrt[3]{\frac{256}{F}}\Rightarrow \quad n=\left\lceil\frac{1}{6N}\sqrt{\frac{F}{3N}}\right\rceil$$

$$\Rightarrow N=\left\lceil\sqrt[3]{\frac{F}{108n^2}}\right\rceil \quad \Rightarrow \quad N_{max}=\left\lceil\sqrt[3]{\frac{F}{108}}\right\rceil$$


1
2
$\left\lceil\frac{1}{18}\sqrt{\frac{F}{9}}\right\rceil$
$\left\lceil\frac{1}{12}\sqrt{\frac{F}{6}}\right\rceil$
$\left\lceil\frac{1}{6}\sqrt{\frac{F}{3}}\right\rceil$
$\lceil 4\sqrt{F}\rceil$
n
N_{max}
$N=3$
$N=2$
$N=1$

For any $\beta(k,1)$value in ϕ_n intervals, we can use E_N tests.

Acknowledgments

The author would like to express his sincere gratitude to Dr. Amir Jafari, associated professor of Sharif University, for his guidance in all steps. I also want to thank my wife, Fariba, and my son Alireza, for their kind encouragement in all conditions.

***References**:*

1.D.M. Burton, "Elementary Number Theory", Mc Graw Hill Companies, 2007.
2.R. Cranal, C. Pomerance, "Prime Numbers", Springer, 2005.
3.D. Wells, "Prime Numbers", Joun Wiley & Sons, 2005.
4.P. Hackman,"Elementary Number Theory", HHH. Production, 2009.
5.T. Koshy, "Elementary Number Theory with Application", Elsevier, 2007.
6.K.C. Chowdhury, "A First course in Number theory", Asian Books Private Limited, 2007.
7.W. Narkiewicz, "The Development of Prime Number theory", Spring, 2000.
8.H.M. Stark, "An Introduction to Number theory", MIT Press, 1987.
9.A. Baker, "A Comprehensive Course in Number theory", Cambridge University Press, 2012.
10.K.H. Rosen, "Elementary Number theory", Pearson Adisson Wisely, 2005.
11.J.J. Tattersall, "Elementary Number Theory", Cambridge University Press, 2005.
12.G.A.Jones, M. Jones, "Elementary Number Theory", Springer, 2005.
13.W. Sierpinsky, "Elementary Theory of Numbers", PWN-Polish Scientific Publishers, 1991.

14.M.B. Nathanson. "Elementary Methods in Number Theory", Springer, 2000.

15.O. Ore, "Number Theory and Its History", Mc Graw Hill Companies, 1948.