Research Article

Introducing two New Methods for Factorization Natural Odd Numbers

Ramazanali Maleki Chorei [a]

[a] Pharm.D , Tabriz School of Pharmacy, Iran.

Article History: Received: 5 April 2021; Accepted: 14 May 2021; Published online: 22 June 2021

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 methods for separating composite numbers from prime numbers.

Keywords: Prime numbers, odd numbers, Fermat's factorization method, new methods, composite number

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 methods for factorization of non-prime odd numbers by developing Fermat's factorization method. The first method is $\alpha - s$ method that based on the relation $(\lfloor\sqrt{F}\rfloor + \theta)^2 - F = \left(\frac{p-q}{2}\right)^2$ and the second method is $\beta - s$ method that based on the $\left(\lfloor\sqrt{4kF}\rfloor + \theta\right)^2 - 4kF = (mp - nq)^2$.(θ is a natural number) We show this methods 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 $F = pq$ $(3 \le p < q)$, 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 $F = k_r p^2$.

For each natural number bigger than 1 as k, we can write 4kF as difference of squares of two even numbers or odd numbers as bellow, 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:

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

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 k_r is also a natural number. This means that F based on relation $F = k_r p^2$is a non-prime number. If kF isn't a square number and $\beta(k, \theta)$ is a square number, then we will have:

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

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

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

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

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:

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

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:

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

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:

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

In this paper, the approximate value of a number as x will be shown in the form of ~(x) or x̃.

Theorem 1: For each natural odd number as $F = pq, (1 \le p < q)$ if we assume $\tilde{k}_r = \sim(q/p) = m/n$ and $|\tilde{k}_r - k_r| = 0 \cdot \overline{a_1 \dots a_s}$, by choosing k=mn, the result of $\beta(k,1)$ will be square when $\overline{a_1 \dots a_s}\, p^2 < \sqrt{4F \times 10^s} \pm 1$.

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

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

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

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

Now, by assuming $\overline{a_1 \dots a_s}\,(2p^2) = k'$ and $x = 2 \times 10^S F$, we arrive at $4kF = x^2 + k'x$. Since k' is even, so by lemma (1), we get

$$\lfloor \sqrt{4kF} \rfloor = \lfloor \sqrt{x^2 + k'x} \rfloor = x + \frac{k' - 2}{2} = 2 \times 10^S F + \overline{a_1 \dots a_s}\, p^2 - 1 \Rightarrow$$

$$\beta(k,1) = (\lfloor \sqrt{4kF} \rfloor + 1)^2 - 4kF = (2 \times 10^S F + \overline{a_1 \dots a_s}\, p^2)^2 - 4kF,$$

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:

$$k' < \sqrt{8x} + 2 \Longrightarrow \overline{a_1 \dots a_s}.P^2 < \sqrt{4F \times 10^S} + 1.$$

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

$$\overline{a_1 \dots a_s}\, P^2 < \sqrt{4F \times 10^S} - 1. \quad \blacksquare$$

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

Whenever $|\tilde{k}_r - k_r| = 10^{-s}$, 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:

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

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

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

$$\delta = q - p < \sqrt{8p} + 2 \Longrightarrow F < \left(p + \sqrt{2p}\right)^2 \Longrightarrow P > \sqrt{F} + 1 - \sqrt{\left(\sqrt{F}+1\right)^2 - F}\,. \quad \blacksquare$$

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:

$$\lfloor \sqrt{x^2 + kx} \rfloor = x + \tfrac{k-1}{2}\,.$$

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:

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

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 $\lfloor\sqrt{x^2+kx}\rfloor = x+\frac{k-1}{2}$. 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 $F = pq, (1 \le p < q)$, 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 $|mp-nq| = 0.\overline{a_1 \dots a_s}\, np < 2\sqrt{nq}+1$,

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

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 $\tilde{k}_r > k_r$: $\frac{m}{n} > \frac{q}{p} \Rightarrow \tilde{k}_r - k_r = 0.\overline{a_1 \dots a_s} = \frac{m}{n} - \frac{q}{p} = \frac{mp-nq}{np}$. (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 $mp-nq = 0.\overline{a_1 \dots a_s}\, np < 2\sqrt{nq}+1$.

If $\tilde{k}_r < k_r$: $\frac{m}{n} < \frac{q}{p} \Rightarrow k_r - \tilde{k}_r = 0.\overline{a_1 \dots a_s} = \frac{q}{p} - \frac{m}{n} = \frac{nq-mp}{np}$. (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: $nq-mp = 0.\overline{a_1 \dots a_s}\, np < 2\sqrt{mp}+1$. ■

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 $(\frac{(\sqrt{q}+1)^2}{P}, \frac{(\sqrt{q}-1)^2}{P})$ 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:

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

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:

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

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

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

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

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:

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

so we can conclude $k \neq k_r$.

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

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

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

If we propose $k_{min} = \frac{(\sqrt{q}-1)^2}{p}$ and $k_{max} = \frac{(\sqrt{q}+1)^2}{p}$ and show the difference of K_{min} and K_{max} by δ_K then for every integer number which is lied in that interval, the result of $\beta(k,1)$ will be square. Therefore, we have $\delta_K = k_{max} - k_{min} = \frac{4\sqrt{q}}{p}$ .We will have the Maximum value of δ_K when $P = 1$. In this case, we have $\delta_{Kmax} = 4\sqrt{F}$ .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_K 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: $p = 17, q = 43 \Rightarrow 21 < k \leq 26 \Rightarrow N = 26 - 21 = 5.$

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

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

Based on lemma (1) , we should have :

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

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

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

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

Theorem 6: For each non-prime odd number as $F = pq(3 \le p < q)$, 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

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

Proof: In the identity $4kF = 4k(pq) = (q+kp)^2 - (q-kp)^2$,since kF can not be square, thus we have

$\theta = \lfloor kp + q - \sqrt{4kpq}\rfloor + 1 = kp + q + \lfloor -\sqrt{4kpq}\rfloor + 1 = kp + q + (-\lfloor\sqrt{4kpq}\rfloor - 1) + 1$

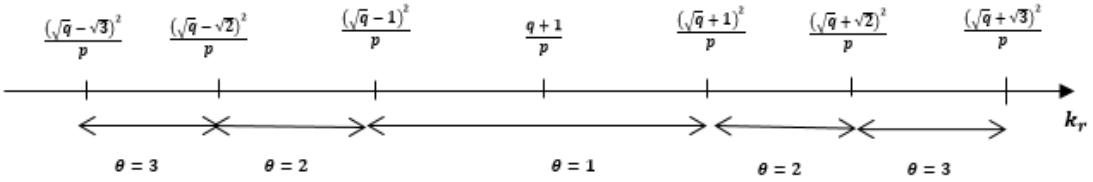
$= kp + q - \lfloor\sqrt{4kpq}\rfloor \Rightarrow \beta(k,\theta) = (kp+q)^2 - 4kpq = (kp-q)^2.$

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

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

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

In the sequel we have :



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

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

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

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

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

Theorem 7: For each non-prime odd number as $F = pq(3 \le p < q)$, 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:

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

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

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

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

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

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

Theorem 8: For each non-prime natural numbers as $F = pq\ (3 \le p < q)$, 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:

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

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

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_m, so we will get:

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

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:

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

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

3. Introducing $\alpha - s$ method

Since for each odd composite number we have:

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

Therefore if we propose S=x+y+1 and R=x y, 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:

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

If suppose $p_{min} = \frac{\sqrt{F}}{2}$ then we should have $S_{max} = \sqrt{F}$

and from $F = k_r p^2$ we have $s = \frac{k_r+1}{2}\sqrt{\frac{F}{k_r}}$.

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

When the difference between S_p and $S_{\sqrt{F}}$ is represented by n, then 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:

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

By considering the points mentioned, we can recommend a method to identify an odd 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:

$$\begin{cases} k = \text{ odd } \Rightarrow S = \text{ even} \\ k = \text{ even } \Rightarrow S = \text{ odd} \end{cases}$$

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 $S_{e \text{ or } o}^{f_1}$ as

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

Therefore, for different cases , we have:

$$F = 2k + 1 = \overline{\ldots 1} \quad \Rightarrow \quad \begin{cases} k = \text{odd} \ , \ S_e^1 = (0{,}4\ ,6) \\ k = \text{even} \ , \ S_o^1 = (1\ ,5\ ,9) \end{cases}$$

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

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

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

It is noteworthy to mention that in this method 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 method. 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 method 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 or not. By using only a few digits on the right side of S and F, we will be able to eliminate many values of S. If $\alpha = \overline{e_m e_{m-1} \ldots e_3 e_2 e_1}$is a prefect square number, then we will be able to use the following notes in this method.

Note 3: We can easily show

$$\begin{cases}\overline{a_n a_{n-1} \dots a_m a_{m-1} \dots a_1}^2 = \overline{\dots b_m b_{m-1} \dots b_1} \\ \overline{a_m a_{m-1} \dots a_1}^2 = \overline{\dots c_m c_{m-1} \dots . c_1}\end{cases} \Rightarrow \overline{b_m b_{m-1} \dots b_1} = \overline{c_m c_{m-1} \dots . c_1}$$

and

$$\overline{a_n a_{n-1} \dots a_m a_{m-1} \dots a_1} \pm \overline{b_r b_{r-1} \dots b_m b_{m-1} \dots b_1} = \overline{c_s c_{s-1} \dots c_m c_{m-1} \dots . c_1} \Rightarrow$$
$$\overline{a_m a_{m-1} \dots a_1} \pm \overline{b_m b_{m-1} \dots b_1} = \overline{\dots c_m c_{m-1} \dots . c_1}$$

Note 4: For all square numbers we always have $e_1 \in \{0, 1, 4, 5, 6, 9\}$.
Note 5: If e_1=5, then $E_3 = \overline{e_3 e_2 e_1} \in \{025,\ 225, 625\}$.

For proving, by assume $\alpha = (\overline{\dots l_3 l_2 l_1})^2$ we should have:

$$(\overline{l_3 l_2 l_1})^2 = (\overline{l_3 l_2 5})^2 = 10^4 l_3^2 + (2l_1 l_3 + l_3) \times 10^3 + (l_2^2 + l_2) \times 10^2 + 5^2$$
$$\Rightarrow \begin{cases}\overline{e_2 e_1} = 5^2 = \overline{25} \\ e_3 = l_2^2 + l_2 \Rightarrow e_3 \in \{0,2,6\}\end{cases}$$

Note 6: 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 7: 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 9: 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:
$E_N - (2i - 1)^2 = 2^N m_i \quad (1 \le i \le 2^{N-3}, N > 3)$

and in a way that α is even, we have:
$E_N - (2i - 2)^2 = 2^N m_i \quad (1 \le i \le 2^{N-3}, N > 3)$

(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 α is a perfect square number, we will have:

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

If we continue, receive to 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:

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

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

$$\begin{vmatrix} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ E_N - (2n_1 - 1)^2 = 2^N m_{n_1} \end{vmatrix}$$

Thus we will have:

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

Therefore:

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

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:

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

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

$$\begin{vmatrix} E_N - 0^2 = 2^N m_1 \\ E_N - 2^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ E_N - (2n_1 - 2)^2 = 2^N m_{n_1} \end{vmatrix}$$

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:

$$\begin{vmatrix} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ E_N - (2i-1)^2 = 2^N m_i \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ E_N - [2n_1 - (2i-1)]^2 = 2^N m_{n_1 - i} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ E_N - (2n_1 - 3)^2 = 2^N m_{n_1 - 1} \\ E_N - (2n_1 - 1)^2 = 2^N m_{n_1} \end{vmatrix}$$

In general case by attention to symmetrical position for any twoE_N test we can conclude:

$E_N - (2i-1)^2 = 2^N m_i \ , E_N - [2n_1 - (2i-1)]^2 = 2^N m_{n_1 - i} \Rightarrow$

$[2n_1 - (2i-1)]^2 - (2i-1)^2 = (2n_1)(2n_1 + 4i + 2) = 2^N(2n_1 + 4i + 2) = K \times 2^N \Rightarrow$

$[2n_1 - (2i-1)]^2 = (2i-1)^2 + K \times 2^N \Rightarrow E_N - [2n_2 - (2i-1)]^2 = E_N - (2i-1)^2 + K \times 2^N$

$= 2^N m_{n_1 - i} \Rightarrow E_N - (2i-1)^2 = 2^N\left(m_{n_1 - i} - K \times 2^N\right) = 2^N m_i$

Therefore the total number of the remaining values of A for E_N tests decreases from $2^{N-1}$to 2^{N-2} .

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

The ascending arrangement of the remaining A values in E_N tests, are as below:

$$\begin{vmatrix} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ E_N - (2i-1)^2 = 2^N m_i \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ E_N - [2n_2 - (2i-1)]^2 = 2^N m_{n_2 - i} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ E_N - (2n_2 - 3)^2 = 2^N m_{n_2 - 1} \\ E_N - (2n_2 - 1)^2 = 2^N m_{n_2} \end{vmatrix}$$

Therefore by attention to symmetrical position for any twoE_N test, we can conclude:

$[2n_2 - (2i-1)]^2 - (2i-1)^2 = (2n_2)(2n_1 + 4i + 2) = 2^N(n_1 + 2i + 1) = K \times 2^N \Rightarrow$

$[2n_2 - (2i-1)]^2 = (2i-1)^2 + K \times 2^N \Rightarrow E_N - [2n_2 - (2i-1)]^2 = E_N - (2i-1)^2 + K \times 2^N$

$= 2^N m_{n_2 - i} \Rightarrow E_N - (2i-1)^2 = 2^N\left(m_{n_2 - i} - K \times 2^N\right) = 2^N m_i$

Because the number of E_N tests can be calculated by $n_3 = 2^{N-3}$.

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

$$\begin{cases} E_N - 1^2 = 2^N m_1 \\ E_N - 3^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ E_N - (2n_N - 1)^2 = 2^N m_{n_N} \end{cases}$$

consequently 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:

$$\begin{cases} E_N - 0^2 = 2^N m_1 \\ E_N - 2^2 = 2^N m_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ E_N - (2n_N - 2)^2 = 2^N m_{n_N} \end{cases}$$

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 10: 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 as a'_N and represent the result of $\overline{a'_N a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$ by E'_N, therefore $E'_N - x^2$ can be count by 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 a'_N in a way that $\acute{a}_N = a_N \pm r$, and r can have one of the digits from 1 to 9, then we will have:

$$E'_N = \overline{a'_N a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1} = \overline{(a_N \pm r) a_{N-1} \dots a_1}^2 - \overline{f_N f_{N-1} \dots f_1}$$

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

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

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

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 should have:

$$E'_N = T \times 2^N + E_N \Rightarrow E'_N = T \times 2^N + 2^N m + x^2 \Rightarrow E'_N - x^2 = (T + m) \times 2^N$$

It means $E'_N - x^2$ can be counts by 2^N and the proof is complete. ■

Note 8: 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:

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

In this method we can use theorems 9 and 10 in E_N tests as follow .If for one value of E_N as $\overline{a_N a_{N-1} \dots a_1}$ the result of E_N test will be positive then the result of E_N tests for another value of E_N with equal in $N - 1$ right digits, are positive .In other words ,If E_N test for $\overline{a_N a_{N-1} \dots a_1}$ will be positive then we can conclude when a_N change from 1 to 9 , the result of E_N test should be positive and vice versa ..

Theorem 11: 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:

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

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

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

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

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 12: 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:

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

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

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. 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 13: 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:

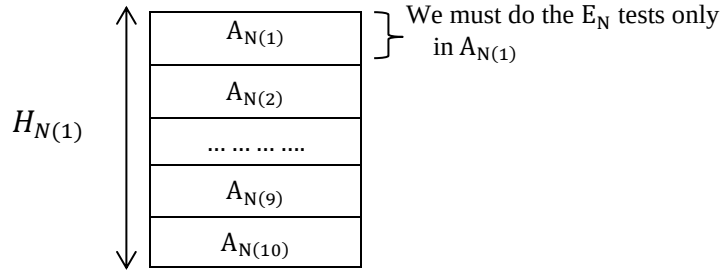
$X = \Delta E_{N(1,2)} \xrightarrow{+200} \Delta E_{N(2,3)} \xrightarrow{+200} \Delta E_{N(3,4)} \xrightarrow{+200} \dots$

$\Rightarrow E_{N(1)} \xrightarrow{X} E_{N(2)} \xrightarrow{X+200} E_{N(3)} \xrightarrow{X+2\times200} E_{N(4)} \xrightarrow{X+3\times200} E_{N(5)} \longrightarrow \cdots$

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

If we represent the i th part of the S values with the number 10^N by $H_{N(i)}$ and the j th part 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 part with the number

10^{N-1}in the $H_{N(1)}$part. 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 part 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 parts 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 $\alpha - S$ method can be calculated by $n_{\alpha-E_N^+} = \left\lceil \frac{S_{max}-S_{min}}{10^N} \right\rceil \times 10w$. Consequently the algorithm of $\alpha - S$ method can be as bellow:

$F = \overline{f_M \dots f_1} \Rightarrow K = \frac{F-1}{2} \Rightarrow$ K = odd ⇒ select $S_e^{f_1}$ or K = even ⇒ select $S_0^{f_1}$
⇒ the values of S_{min} in D_1 ⇒ doing E_3 test on the values of S_n . ($S_n = S_{min} + (n-1) \times 10$)
⇒ the values of $S_{E_3^+}$ ⇒ doing E_{N1} test on $S_{E_3^+}$. If $E_{N_1}^+$ then we go to doing E_{N2} test and if $E_{N_1}^-$ then we continue E_{N1} test on $S_{E_3^+}$. ($E_{N1} - (2i-1)^2 = 2^{N_1} m_i$, $1 < i \leq 2^{N_1-3}$)

In this case if $E_{N_1}^+$ then we go to E_{N2} test .If $E_{N_2}^+$ then we go to E_{N_3} test and if $E_{N_2}^-$ then we continue E_{N2} test on $S_{E_{N_1}^+}$. ($E_{N2} - (2i-1)^2 = 2^{N_2} m_i$, $2^{N_1-3} < i \leq 2^{N_2-3}$)

If $E_{N_2}^+$ then we go to E_{N_3} test. By continue this process we reach to S values with E_N^+ in $A_{N(1)}$, then select S values with E_N^+ in $H_{N(1)}$. In continuation we select S values with E_N^+ in residue H_N parts. (from $H_{N(2)}$ to $H_{N(n_{max})}$) then we doing α test on S values with E_N^+ in all H_N parts .If α test for one value of S is positive (or α is a perfect square number),then we can calculate p and q values.

in the $\alpha - S$ method it is better to do the E_N tests for the three value of N . (E_3, E_{N_1}, E_{N_2}) So that

D	S	E_3	E_{N_1}	E_{N_2}	α test
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, $\Rightarrow S_0^9 = (3,5,7)$

The first set of S by 10^3 length	E_3	E_5
501,950,075,865,932	$E_3 = \overline{100} \longrightarrow E_3^+$	$E_5^- \longrightarrow \boxtimes$

D_1	501,950,075,865,933 501,950,075,865,935	$E_3 = \overline{260} \longrightarrow \boxtimes$ $E_3 = \overline{996} \longrightarrow \boxtimes$	
D_2	501,950,075,865,937 501,950,075,865,943 501,950,075,865,945	$E_3 = \overline{740} \longrightarrow \boxtimes$ $E_3 = \overline{020} \longrightarrow \boxtimes$ $E_3 = \overline{796} \longrightarrow E_3^+$	$E_5^- \longrightarrow \boxtimes$
D_3	501,950,075,865,947 501,950,075,865,953 501,950,075,865,955	$E_3 = \overline{580} \longrightarrow \boxtimes$ $E_3 = \overline{980} \longrightarrow \boxtimes$ $E_3 = \overline{796} \longrightarrow E_3^+$	$E_5^- \longrightarrow \boxtimes$

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:

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

It is observed that only by E_5 test, the S values are eliminated from 3 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 method, 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 $\beta - s$ method

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:

$$\beta(k,\theta) = S^2 - 4kF = t^2 \implies p = \frac{S \mp t}{2m}\ , q = \frac{S \pm t}{2n}$$

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 prefect square, is called $\beta - S$ method. In this method, we represent N digits on the right side of $\beta(k,\theta)$ value by E_N and we do the E_N tests like $\alpha - S$ method. To use this method on S values only from $k_r = 1$ to $k_r = 4$, is equal to apply this method for the p values from $\sqrt{F}$ to $\frac{\sqrt{F}}{2}$ .This is one of the most important benefits of this sieve. In this method 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:

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

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

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

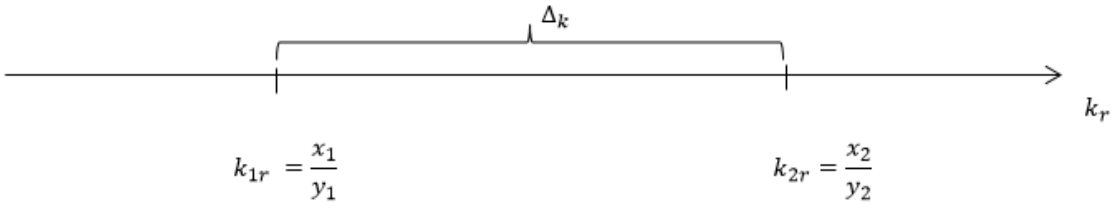
$$\beta(k,\theta) = S^2 - 4kF = (mp+nq)^2 - 4(mn)(pq) = (mp-nq)^2 = t^2$$

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:

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

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

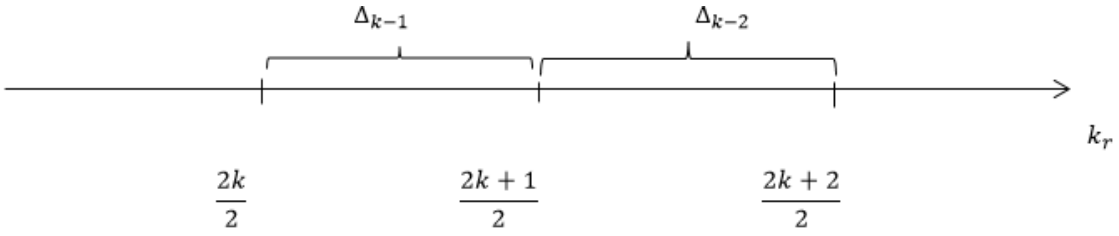
$$k_r = \frac{q}{p} = \frac{x_2}{y_2} \quad , \quad F = k_r p^2 \Rightarrow \begin{cases} p = \sqrt{\frac{F}{k_r}} = \sqrt{\frac{y_2F}{x_2}} \\ q = \frac{x_2}{y}\sqrt{\frac{y_2F}{x_2}} \end{cases} \Rightarrow S_u = x_1p + y_1q = (x_1+x_2)\sqrt{\frac{y_2F}{x_2}}$$

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

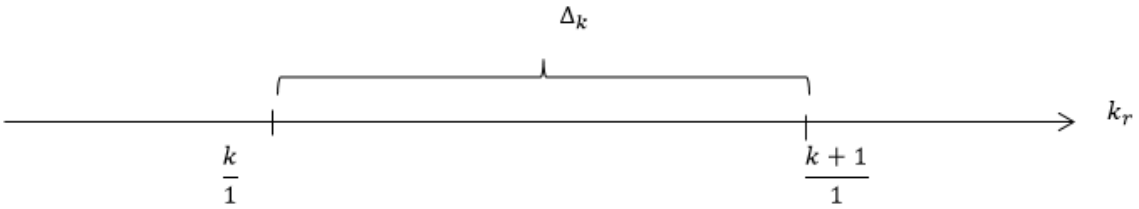
If one S_r is located in the sieve interval of Δ, we represented it by Δ_r.For each S_r in a sieve interval of Δ_r, we have:

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

In orders that the method 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 two 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:



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

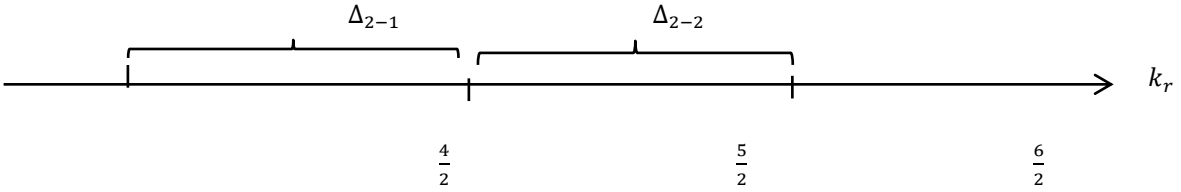
Therefore for the zones between the consecutive integer values of k_r, the length of the intervals ($L = S_u - S_d$) are decreased.

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

The decreasing of the length of consecutive zones for k_r values ,finally to get at zero. In a way that for some consecutive integer value of k_r, the result of $\beta(k,1)$ will be a square number. With the increase in k_r values, the number of consecutive integer values of k on the condition that the result of $\beta(k,1)$ are square, increased accordingly. Therefore based on the theorem(4) ,it is only necessary to do $\beta(k,1)$ test for one integer value of k_r .

Example 3: By selecting k=2 prove that $F = 9,640,669$ is a composite number.

Answer:



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

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

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

$$\begin{vmatrix} m = 4 \\ n = 2 \end{vmatrix} \Rightarrow \begin{vmatrix} p = \frac{S-t}{2m} = \frac{17,622-1426}{2\times 4} = 2381 \\ q = \frac{S+t}{2n} = \frac{17,622+1426}{2\times 2} = 4049 \end{vmatrix}$$

The important benefits of $\beta - S$ method is that we can easily apply it in a arbitrary zone of k_r values. This is particularly very important for some values of k_r since it includes a large part of the interval containing the p values.

Because in general case by attention to

$$S_d = \lfloor \sqrt{4k_1F} \rfloor \ , S_u = (k_1 + k_2)\sqrt{\frac{F}{k_2}} \Rightarrow L = S_u - S_d = \sqrt{\frac{F}{k_2}}\left(\sqrt{k_2} - \sqrt{k_1}\right)^2$$

we can conclude that :

1-By increasing Δk for a natural number as F , then the values of L increases.

2-When the value of Δk has a constant value, if we increase the value of k_1 and k_2, then values of L decreases .If we select $k_1 = \frac{(\sqrt{q}-1)^2}{P}$ and $k_2 = \frac{(\sqrt{q}+1)^2}{P}$, we can see that $L = 1$ and $p \geq \sqrt[3]{16F}$.

By this method we can choice any arbitrary zone of k_r for β test therefore it is the important advantages of this method.

Acknowledgments

The author would like to express his sincere gratitude to Dr. Amir Jafari, associated professor of Sharif University and Dr. Kamyar Hosaini, assistant professor of Islamic Azad University of Rasht, for their 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.