*Int Jr. of Mathematical Sciences & Applications*
*Vol. 5, No. 2, (July-December, 2015)*

*ISSN No: 2230-9888*
*www.journalshub.com*

# Efficient Simple Tests For Primality

***Fayez Fok Al Adeh*[1].**

[1]President of the Syrian Cosmological Society

P.O.Box:13187,Damascus,SyriaTels:00963-11-2776729,2713005

*Corresponding Author Email address: hayfa@scs-net.org

**ABSTRACT**

**The tests form a general method to decide whether a given positive odd integer is composite or prime. The tests are based on the divisibility properties of the sum of two squared positive integers. The algorithms comprising the tests are polynomial- time algorithms.**

**Keywords :Algorithm, Composite,Generating Function,Greatest Common Divisor,Prime,Quotient,Remainder,Solving Polynomial Equation,Square.**

**Subj.Class: Number Theory,General Mathematics**

## INTRODUCTION

If x is an odd positive integer, then the simplest way to discover whether it is composite or prime is to try and divide x by every number from one up to $\sqrt{x}$ . If x is a ten – digit number ,the number of necessary operations may exceed 100000,but if x is a fifty – digit number, the number of elementary steps may rise to a one followed by 25 zeros. The ultra – computer running at 1 teraflop will take in the order of one million years to complete the job on average. That does not sound terribly efficient. The problem is that the number of steps is rising exponentially in the number of digits of the given number. Algorithms like this, that require an exponentially increasing number of steps with respect to the size of the input are regarded as intractable. They are non polynomial- time algorithms.

However,there is a more

Efficient algorithm for finding prime factors of large composites. It is based on finding another positive integer M which is relatively prime to x . M is called the seed. The key step is to calculate the order of M with respect to x . Now in the next step the seed is raised to a power equal to the order and the square root is taken. From this last result add 1 or subtract 1` to give a pair of numbers N1 and N2. In the final step,the greatest common divisor of x and N1 and also of x and N2 are calculated. The pair of greatest common divisors thus obtained are factors of x .Because the seed number is chosen randomly, there is no guarantee for the success of the method. The problem with this algorithm, is that ,for conventional computer,finding the order of large numbers also requires a large number of steps which would grow exponentiolly. Peter Shor's great insight was to discover that finding the order of a number is an easy job in quantum computing. But to use Shor's algorithm on a large scale, we have to wait until quantum computing is introduced in the empirical applications.

**Efficient Simple Tests For Primality**

**TEST -1 –**

Given an odd positive integer x >1, we have to dicide whether x in prime or composite.

TEST – 1 – employs any updated algorithm for calculating the square root of a number. Since the algorithm gives approximate value of the square root, we can check for the two odd integral values less and greater than the approximate one. If the square root of x is an integer, then x is composite,and we are done. Else ,we move to TEST-2-.

**TEST – 2 –**

Consult an updated table of primes. Let the largest known prime in the table be Z. We divide x successively by the primes in the table.The division operations will not take too much time on a moderate computer. If one of the primes divides x , then x is composite, and we are done.

Else,we move to TEST-3- .

**TOWARDS TEST – 3 –**

We proceed to formulate TEST -3 – by proving the following theorem.

Theorem -1- Given two positive integers x and y (x > y,x,y >1). If (xy+1) divides $(x^2+y^2)$ , then the quotient must be a square.

First of all, we prove the following lemma.

Lemma 1-1 If x and y are relatively prime positive integers (x > y, x,y>1), then (xy+1) does not divide $(x^2+y^2)$.

Proof : Suppose that ( xy+1) divides $(x^2+y^2)$ i.e.

**(1 )** $(xy+1) \mid ( (x^2+y^2)$

The notation m | n refers here to the fact that the integer m divides the integer n.

we know that

**(2)** $(xy+1 ) \mid (x^2 y^2-1)$

from (1) we deduce that

**(3)** $(xy+1) \mid (x^2y^2+y^4)$

using **(2)** and **(3)** we arrive at the result

**(4)** $(xy+1) \mid (y^4+1)$

i.e. there exists a positive integer r such that

**(5)** $\mathbf{r(xy+1)} = y^4+1$

taking residues mod y we deduce that

**(6)** $r \equiv 1 \mod y$

this means that there exists a positive integer w such that

**(7)** $\mathbf{r = wy+1}$

using **(7)** we rewrite **(5)** in the form

**(8)** $(xy+1)(wy+1) = y^4+1$

it is evident from (8) that w cannot be greater than y or equal to y , in fact

**(9)** $w<y$

from (8) we get the following equality:

**(10)** $xwy + x+w = y^3$

according to **(10),** if w and y have a common divisor,then this divisor must also divide x. This contradicts our assumption that x and y are relatively prime. Hence w and y are relatively prime.

equation (8) tells us that

**(11)** $(wy+1) \mid (y^4+1)$

also we know that

**(12)** $(wy+1) \mid (w^2y^2-1)$

from **(11)** and **(12)** we arrive at the result

**(13)** $(wy+1) \mid y^2(w^2+y^2)$

since $(wy+1)$ and $y^2$ have no common prime divisor, we deduce that

**(14)** $(wy+1) \mid (w^2+y^2)$

We began with two positive relatively prime integers:x,y (x>y) satisfying the divisibility condition **(1)** and ended with two positive relatively prime integers:the original y ,and a new positive integer w **(w<y) satisfying** the divisibility condition **(14).**

Beginning with **(14)** and repeating similar steps**, we** arrive at two positive relatively prime integers:the original w ,and a new positive integer s (s<w) satisfying a similar divisibility condition:

**(15)** $(sw+1) \mid (s^2+w^2)$

We cannot go on repeating similar steps,because of the principle of the impossibility of infinite descent.This proves the lemma.

Proof of Theorem -1-

the assumed divisibility condition is

**(16)** $(xy+1) \mid (x^2+y^2)$

according to **(16)** ,lemma 1-1 implies the existence of a greatest common divisor w of x and y : i.e.

**(17)** $x = aw$

**(18)** $y = bw$

**(19)** $a>b$ (since $x >y$)

**so, the rational fraction**

**(20)** $\frac{(x^2+y^2)}{(xy+1)}$

must be an integer, we have

**(21)** $\frac{(x^2+y^2)}{(xy+1)} = \frac{w^2(a^2+b^2)}{w^2ab+1}$

a and b are relatively prime positive integers.

here we have two cases: either

**(22)** $(w^2ab + 1) \mid (a^2+ b^2)$ i.e.

$(a^2+ b^2)> (w^2ab + 1)$ or

**(23)** $(w^2ab + 1) =(a^2+ b^2)$

assume **(22),** we know that

**(24)** $(w^2ab + 1) \mid (w^4a^2b^2 - 1)$

from **(22) we deduce that**

**(25)** $(w^2ab + 1) \mid w^4 b^2(a^2 + b^2) = (w^4a^2b^2 + w^4b^4)$

Using (24) and (25) we get

**(26)** $(w^2ab + 1) \mid (w^4b^4+1)$ i.e.

**(27)** $\mathbf{r}(w^2ab + 1) = (w^4b^4+1)$

where r is a positive integer.

taking the residues mod $w^2b$

**(28)** $\mathbf{r} \equiv 1 \mod w^2b$

**i.e. there exists a positive integer m such that**

**(29)** $\mathbf{r} = mw^2 b + 1$

**thus (27) takes the form**

**(30)** $(w^2ab + 1)( mw^2 b + 1 ) = (w^4b^4+1)$

**assume that**

**(31)** $m \geq b$ hence

**(32)** $( mw^2 b + 1 ) \geq (w^2b^2+1)$

we have also,since a>b

**(33)** $(w^2ab+1) > (w^2b^2+1)$

from (32) and (33) we get

**(34)** $(w^2ab + 1)( mw^2 b + 1 ) > (w^2b^2+1)^2 > (w^4b^4+1)$

**this contradiction leads us to the result that**

**(35)** $m < b$

**expanding (30) we get**

**$mw^4ab^2 + w^2ab + mw^2b + 1 = w^4b^4 + 1$ i.e.**

**(36)** $\mathbf{mw^2ab + a + m = w^2b^3}$

suppose that there exists a prime number which divides both b and m , then according to (36), this prime number must divide a, contrary to the fact that a and b are relatively prime. Therefore b and m are also relatively prime**.**

(30) tells us that

**(37)** $( mw^2 b + 1 ) \mid (w^4b^4+1)$ but

**(38)** $( mw^2 b + 1 ) \mid (m^2w^4b^2-1)$

from **(37)** and **(38) we deduce that**

**(39)** $( mw^2 b + 1 ) \mid (m^2w^4b^2+w^4b^4)= w^4b^2(m^2+b^2)$

it is evident that $( mw^2 b + 1 )$ and $w^4b^2$ have no prime factor in common, therefore

**(40)** $( mw^2 b + 1 ) \mid (m^2+b^2)$

We began with two positive relatively prime integers:a,b (a>b) satisfying the divisibility condition **(22)** and ended with two positive relatively prime integers:the original b ,and a new positive integer m **(m<b) satisfying** the divisibility condition **(40).**

Beginning with **(40)** and repeating similar steps**, we** arrive at two positive relatively prime integers: the original m ,and a new positive integer s (s<m) satisfying a similar divisibility condition:

**(41)** $( w^2sm+1) \mid (m^2+ s^2)$

We cannot go on repeating similar steps,because of the principle of the impossibility of infinite descent.Therefore,our assumption (22) is false and we are left with the result (23) that

**(23)** $w^2ab+1 = a^2+ b^2$

(21) and (23) prove Theorem -1-

We return to our main problem: given an odd positive integer x>1, to decide whether x is composite or prime. If there exists a positive integer y (y<x) such that the divisibility condition (1) is satisfied, then according to Theorem -1- :

**(42)** $(x^2+y^2) = w^2(xy+1)$

where w is the greatest common divisor of x and y.

Here we have three cases :

Case -1-

**(43)** $y^2> w^2 >x$

from (42) we get

$\mathbf{x^2+y^2=}$ $w^2(xy+1)>x(xy+1)$ i.e.

**(44)** $x^2+y^2> x^2y+x$ hence

**(45)** $x(x-1) > y(x^2 - y)$

**since $y^2 > x$ we get**

**$x(x-1) > y(x^2-y) > \sqrt{x}(x^2-y)$ i.e.**

**(46)** $\sqrt{x}(x-1) > (x^2 - y)$ but $x > \sqrt{x}$ **,** therefore

**(47)** $x(x-1) > \sqrt{x}(x-1) > (x^2-y)$ **hence**

$x^2 - x > x^2 - y$ i.e.

**(48)** $-x > -y$ , $x < y$

this contradicts our main assumption that $y < x$.

Therefore, Case -1- does not occur**.**

**TEST -3 –**

We deal here with

Case -2-

**(49)** $w^2 \leq y^2 < x$

from (42)

**(50)** $y^2 = x(w^2y - x) + w^2$

if $w^2y - x > 0$ then

**(51)** $y^2 > x$

contrary to our assumption (49)

if $w^2y - x < 0$ then $x(w^2y - x) < 0$ and hence

$x(w^2y - x) + w^2 < w^2$ i.e. $y^2 < w^2$

contrary to our assumption (49)

therefore

**(52)** $w^2y - x = 0$

in this case (50) tells us that $y^2 = w^2$ i.e.

**(53)** $y = w$

substituting in (42) we get $x^2 + w^2 = w^3x + w^2$ i.e.

**(54)** $x = w^3$

TEST -3- can employ any simple algorithm to check if x is a cube of an integer. Since the algorithm gives approximate value of the cubic root, we can check for the two odd integral values less and greater than the approximate one .If x is a cube of an integer, then the divisibility condition (42) is satisfied and x is (afortiori) composite.

In case TEST -3- fails, we move on to TEST-4-

**TOWARDS TEST – 4 –**

We proceed to formulate TEST - 4 - by considering:

Case - 3 –

**(55)** $y^2>x>w^2$

according to Theorem -1- $(x^2+y^2) = w^2(xy+1)$ i.e.

**(56)** $x^2 =(w^2x –y ) y+w^2$ if

**(57)** $w^2 x=y$ then $x^2=w^2$ i.e.

**(58)** $x=w$

contrary to our assumption (55)

if $w^2x-y<0$ then$(w^2x-y)y<0$ and hence

$x^2= (w^2x-y)y+w^2<w^2$ i.e.

**(59**) $x<w$

this contradicts (55), so we are left with the result that

**(60)** $w^2x-y>0$

we can prove in this case that an infinite sequence of values of x and y satisfy the divisibility condition of Theorem -1- , let

**(61)** $x_1 =w^2x-y ,y_1 =x$

we have that

**(62)** $x_1^2+ y_1^2= (w^4x^2+y^2-2w^2xy) +x^2$

$= (x^2+y^2)+ w^2x( w^2x-2y)$

$= w^2(xy+1)+w^2x(w^2x-2y)$

$= w^2xy+w^2+w^4x^2-2w^2xy$

$= w^4x^2-w^2xy+w^2$

$= w^2(w^2x^2-xy+1)$

$= w^2[x(w^2x-y)+1]$

$= w^2(x_1y_1+1)$

according to (53) ,(54) and (61) the first elements of the sequence would be : ( where $y_{n+1} = x_n$ )

**(63)**

| | | |
|---|---|---|
| n=0 | $x_0=o$ | $y_0=-w$ |
| n=1 | $x_1=w$ | $y_1=0$ |
| n=2 | $x_2=w^3$ | $y_2=w$ |
| n=3 | $x_3=w^5-w$ | $y_3=w^3$ |
| n=4 | $x_4=w^7-2w^3$ | $y_4=w^5-w$ |
| n=5 | $x_5=w^9-3w^5+w$ | $y_5=w^7-2w^3$ |

note that lines n=0 and n=1 correspond to Case -1- ,while line n=2 corresponds to Case -2-.This sequence of numbers,satisfies according to (61) the recurrence:

**(64)** $x_{n+2} = w^2x_{n+1} - x_n$ given that

**(65)** $x_0=0$ $x_1=w$ $x_2=w^3$

we will solve for the generating function

**(66)** $A(z)=A=\sum_{n\geq 0} x_n z^n$

multiply (64) by $z^n$ and sum over all values of n

$\sum_{n\geq 0} x_{n+2}z^n = w^2\sum_{n\geq 0} x_{n+1}z^n - \sum_{n\geq 0} x_n z^n$ **i.e.**

**(67)** $\frac{A-wz}{z^2} = \frac{w^2A}{z} - A$

from which we get

**(68)** $A=\frac{wz}{z^2-w^2z+1}$

rewrite (68) in the form

**(69)** $A= \frac{w}{\sqrt{w^4-4}}\left( \frac{1}{1-zz_1} - \frac{1}{1-zz_2} \right)$

where $z_1 = \frac{w^2+\sqrt{w^4-4}}{2}$

$z_2 = \frac{w^2-\sqrt{w^4-4}}{2}$ therefore

**(70)** $A = \frac{w}{\sqrt{w^4-4}} \left(\sum_{j\geq 0} z_1^j z^j - \sum_{j\geq 0} z_2^j z^j\right)$

now $x_n$ is the coefficient of the $n^{th}$ power of z,i.e.

**(71)** $x_n = \frac{w}{\sqrt{w^4-4}} \left[\left(\frac{w^2+\sqrt{w^4-4}}{2}\right)^n - \left(\frac{w^2-\sqrt{w^4-4}}{2}\right)^n\right]$

this is the required general formula.

Let us prove that,if n is a multiple of 3, then the corresponding element of the sequence would be even,and hence must be discarded,since it cannot be equated to the given positive odd integer x. Since w divides the given positive odd integer x, it must be odd. Suppose that for some value of n which is a multiple of 3 (n=3m), the corresponding element $x_n$ of the sequence is even,while $y_n$ is odd. According to (64),$x_n$ would be odd and $y_n$ even for n=3m+1. Now,for n=3m+2, and using (64) again, we conclude that both $x_n$ and $y_n$ are odd.Employing(64) for n=3m+3 leads us to the conclusion that the element $x_n$ of the sequence is even,while $y_n$ is odd .In reference to (63), we see that for n=3,the element $x_3$ of the sequence is even,while $y_3$ is odd (because w is odd). By mathematical induction, our claim is justified.The first elements of the sequence given in (63) can be easily deduced from (71) .

If the given positive odd integer x equals an element of the sequence $x_n$ for some value of n, then x must be composite.

Assume that for some n ,it is the case that:

**(72)** $x= \frac{w}{\sqrt{w^4-4}} [(\frac{w^2+\sqrt{w^4-4}}{2})^n - (\frac{w^2-\sqrt{w^4-4}}{2})^n]$

where x is the given positive odd integer,we make the substitution

**(73)** $t =\frac{w^2+\sqrt{w^4-4}}{2}$ hence

**(74)** $w= \frac{\sqrt{t^2+1}}{\sqrt{t}}$ (72) takes the form

**(75)** $x = \frac{\sqrt{t(t^2+1)}}{t^2-1}( t^n - \frac{1}{t^n})$

if we expand this equation in powers of t,we get

**(76)** $t^{4n+2}+ t^{4n}-x^2 t^{2n+3}-2t^{2n+2}+ 2 x^2 t^{2n+1}-2t^{2n}-x^2t^{2n-1}+t^2+1=0$

in reference to (72),where it is evident that w divides x,assume that $w \leq Z$ (Z the largest known prime mentioned in TEST -2 -). w cannot be prime ,since this would contradict the negative result of TEST -2 - . If w is composite , then some prime p less than or equal to Z divides w , and hence divides x . Again this would contradict the negative result of TEST -2-. Therefore w> Z, i.e. $w\geq Z+2$.

We make use of the following very well known theorem;

A theorem for the upper limit to the real roots:

If ,in a real equation

f(z) $=a_0z^n + a_1z^{n-1} +\ldots..+ a_n(a_0 > 0)$

the first negative coefficient is preceded by k coefficients which are positive or zero, and if G denotes the greatest of the numerical values of the negative coefficients, then each real root is less than $1+ \sqrt[k]{G/a_0}$

in case of equation (76) we have

**(77)** $a_0$=1 G=$x^2$ k=2n-1

therefore, the upper limit to the real roots t in this case is

**(78)** $t \leq 1+x^{\frac{2}{2n-1}}$

according to (73)

**(79)** $\frac{w^2+\sqrt{w^4-4}}{2} = t \leq 1+x^{\frac{2}{2n-1}}$

since Z+2≤ w (Z the largest known prime mentioned in TEST – 2 –), we have

$$w^2+\sqrt{(Z+2)^4-4} \leq w^2+\sqrt{w^4-4} \leq 2(1+x^{\frac{2}{2n-1}})$$

i.e.

**(80)** $w \leq [2(1+x^{\frac{2}{2n-1}}) - \sqrt{(Z+2)^4-4}]^{\frac{1}{2}}$

according to (71),the given positive odd integer x would be equal to an element of the sequence $x_n$,i.e.

**(81)** $x= \frac{w}{\sqrt{w^4-4}}[(\frac{w^2+\sqrt{w^4-4}}{2})^n - (\frac{w^2-\sqrt{w^4-4}}{2})^n]$

hence we have

**(82)** $x = \frac{w}{\sqrt{w^4-4}}(\frac{w^2+\sqrt{w^4-4}}{2})^n[1-(\frac{w^2-\sqrt{w^4-4}}{w^2+\sqrt{w^4-4}})^n]$

$$< \frac{w}{\sqrt{w^4-4}}(\frac{w^2+\sqrt{w^4-4}}{2})^n$$

$$= \frac{w^{2n+1}}{w^2\sqrt{1-\frac{4}{w^4}}}\frac{1}{2^n}(1+\frac{\sqrt{w^4-4}}{w^2})^n$$

$$< \frac{w^{2n+1}}{w^2\sqrt{1-\frac{4}{w^4}}}\frac{1}{2^n}2^n$$

$$= \frac{w^{2n-1}}{\sqrt{1-\frac{4}{w^4}}}$$

since Z+2 ≤ w we have

**(83)** $(Z+2)^4 \leq w^4$

$$\frac{1}{(Z+2)^4} \geq \frac{1}{w^4}$$

$$-\frac{4}{(Z+2)^4} \leq -\frac{4}{w^4}$$

$$1-\frac{4}{(Z+2)^4} \leq 1-\frac{4}{w^4}$$

$$\sqrt{1-\frac{4}{(Z+2)^4}} \leq \sqrt{1-\frac{4}{w^4}}$$

$$\frac{1}{\sqrt{1-\frac{4}{(Z+2)^4}}} \geq \frac{1}{\sqrt{1-\frac{4}{w^4}}}$$

**from (82)**

**(84)** $x < \frac{w^{2n-1}}{\sqrt{1-\frac{4}{w^4}}} \leq \frac{w^{2n-1}}{\sqrt{1-\frac{4}{(Z+2)^4}}}$

therefore

**(85)** $w^{2n-1} > x\sqrt{1-\frac{4}{(Z+2)^4}}$ i.e.

$\mathbf{w > x^{\frac{1}{2n-1}}}\left(1-\frac{4}{(Z+2)^4}\right)^{\frac{1}{2(2n-1)}}$

if, for a given n , we assume that $x = x_n$ , we get a polynomial equation in the unknown w .In this case (80) and (85) represent the upper and lower bounds of the unknown w, respectively.

rewrite equation (72) in the form

**(86)** $x = w\left[\left(\frac{w^2+\sqrt{w^4-4}}{2}\right)^{n-1} + \left(\frac{w^2+\sqrt{w^4-4}}{2}\right)^{n-2}\left(\frac{w^2+\sqrt{w^4-4}}{2}\right) + \cdots + \left(\frac{w^2-\sqrt{w^4-4}}{2}\right)^{n-1}\right]$

according to (86), and since x is given,we note that if w increases, n decreases,and vice versa.

If we assume that t is known, and ofcourse x is known, then we can determine the value of n as follows, rewrite (75) in the form

**(87)** $\frac{x(t^2-1)}{\sqrt{t(t^2+1)}} = t^n - \frac{1}{t^n}$

making the following substitutions**:**

**(88)** $\mathbf{d} = \frac{x(t^2-1)}{\sqrt{t(t^2+1)}}$ $v = t^n$

transforms (87) into a quadratic equation

**(89)** $v^2 - dv - 1 = 0$

taking the positive root of (89)

**(90)** $v = \frac{d+\sqrt{d^2+4}}{2}$

and substituting $t^n$ for v according to (88),we can calculate the value of the unknown n assuming that t is known.

To get an upper bound for n, according to what we have already mentioned, we substitute (Z+2) for w in (73) and go on to solve equation (89) and get the positive root v. Using this root we get a value for n

from (88). From this value, we calculate the least positive integer not divisible by 3 greater than or equal to the value.Let this integer be $n_2$

Let r be the greatest odd positive integer less than or equal to $\sqrt{x}$. To get a lower bound for n, according to what we have already mentioned, we substitute r for w in (73) and go on to solve equation (89) and get the positive root v. Using this root we get a value for n from (88). From this value, we calculate the greatest positive integer not divisible by 3 less than or equal to the value. Let this integer be $n_1$.

W e are ready now for TEST – 4 –

**TEST -4 –**

We formulat TEST -4 – as an algorithm applicable on any moderate computer.

1. for i=$n_2$ to $n_1$ step -1.
2. if i is divisible by 3 ,then goto 18.
3. Substitute i for n in (85) and get the lower bound $r_1$ of the unknown w. let $w_1$ be the greatest positive odd integer less than or equal to $r_1$ .
4. Substitute i for n in (80) and get the upper bound $r_2$ of the unknown w.let $w_2$ be the least positive odd integer greater than or equal to $r_2$.
5. if i $\neq n_2$ , then goto 10.
6. for j= $w_1$ to $w_2$ step 2.
7. if j divides x , then goto 20.
8. next j .
9. goto 16
10. for j =$w_1$ to $v_1$ step2.
11. if j divides x,then goto20.
12. next j.
13. for j =$v_2$ to $w_2$ step2.
14. if j divides x ,then goto 20.
15. next j .
16. $v_1$= $w_1$-2.
17. $v_2$= $w_2$+2.
18. next i .
19. print :TEST -4- has already failed, goto the section entitled: TOWARDS TEST -5-.
20. halt, print:x is composite and we are done.

**TOWARDS TEST -5-**

Now it is the case that although the divisibility condition of Theorem -1- does not hold,yet x may be composite. So,we assume that for a positive integer y (y<x) ,we have:

**(91)** $x^2+y^2$= a (xy+1)+b

where a is the quotient, and b the remainder.

here we have three cases:

Case -1-

**(92)** $y^2$ > a+b>a>x

**therefore**

**(93)** $x^2+y^2$= a (xy+1)+b

= a xy+a+b

$> x^2$y+a+b

$> x^2y+x$ i.e.

$x(x-1) > y(x^2-y)$

from (92)

**(94)** $x(x-1) > y(x^2-y) > \sqrt{x}\,(x^2-y)$ i.e.

$\sqrt{x}\,(x-1) > (x^2-y)$

but $x > \sqrt{x}$ hence

**(95)** $x(x-1) > (x^2-y)$

$x^2-x > x^2-y$

$-x > -y$

$x < y$

this contradicts our main assumption that y<x,therefore Case -1- does not occur.

Case -2-

**(96)** $a < a+b \leq y^2 < x$

from (91)

**(97)** $y^2 = x(ay-x) + a+b$

if $ay-x > 0$ i.e. $ay > x$ then

**(98)** $y^2 > x$

this contradicts (96)

if $ay-x < 0$ then from (97)

**(99)** $y^2 < a + b$

again this contradicts (96)

therefore

**(100)** $ay-x=0$ $x=ay$

we give in (111) the first elements of a sequence, this

corresponds to $x_2$ and $y_2$ in the line n=2 of that

sequence.

we write (100) in the form

**(101)** $y=\frac{x}{a}=w$

we use the letter w here, because the divisibility condition (42) is a special case of the non – divisibility (91), where $w^2$ corresponds to a ,and b equals zero. In the special case, (101) takes the form $y_2=w=\frac{x_2}{w^2}=\frac{w^3}{w^2}$

Case -3-

**(102)** $y^2>x>a+b>a$

from (91)

**(103)** $x^2=y(ax-y)+a+b$ if

**(104)** $ax-y=0$ then $ax=y$

which means that x<y,in contradiction to our original assumption x>y.

if ax-y<0, then from (103)

**(105)** $x^2<a+b$

since $y^2<x^2$ we have

**(106)** $y^2<x^2<a+b$

this contradicts (102) .therefore

**(107)** $ax-y>0$

we can prove in this case that an infinite sequence of values of x and y satisfy (91).

let

**(108)** $x_1=ax-y \quad y_1=x$

we have that

**(109)** $x_1^2+y_1^2=(ax-y)^2$

$=a^2x^2+y^2-2axy+x^2$
$=x^2+y^2+a^2x^2-2axy$
$=a(xy+1)+b+a^2x^2-2axy$
$=a+b-axy+a^2x^2$
$=ax(ax-y)+a+b$
$=ay_1x_1+a+b$
$=a(x_1y_1+1)+b$

thus there is a recurrence of the form

**(110)** $x_{n+2}=a\,x_{n+1}-x_n$

which generates the sequence $x_n$ .

according to (91),(101),(108),and (110),the first elements of the sequence would be(where $y_{n+1}=x_n$ )

**(111)**

| | | |
|---|---|---|
| n=0 | $x_0=0$ | $y_0 = -\sqrt{a+b}$ |
| n=1 | $x_1=\sqrt{a+b}$ | $y_1 = 0$ |
| n=2 | $x_2=a\sqrt{a+b}$ | $y_2 = \sqrt{a+b}$ |
| n=3 | $x_3=(a^2-1)\sqrt{a+b}$ | $y_3 =a\sqrt{a+b}$ |
| n=4 | $x_4=a(a^2-2)\sqrt{a+b}$ | $y_4 =(a^2-1)\sqrt{a+b}$ |

note that lines n=0 and n=1 correspond to case -1- ($y^2>a+b>a>x$) which does not occur, while line n=2 corresponds to case -2- ($a<a+b\leq y^2<x$).

we will solve for the generating function

**(112)** $A(z)=A=\sum_{n\geq 0} x_n z^n$

multiply (110) by $z^n$ and sum over all values of n

**(113)** $\sum_{n\geq 0} x_{n+2}z^n=a\sum_{n\geq 0} x_{n+1}z^n-\sum_{n\geq 0} x_n z^n$ **i.e.**

hence

**(114)** $A -x_0-x_1z= az(A-x_0) -Az^2$

**(115)** $Az^2-azA+A=x_0+x_1z-azx_0$

$=x_0+z(x_1-ax_0)$

**(116)** $A=\frac{x_0}{z^2-az+1}+\frac{z(x_1-ax_0)}{z^2-az+1}$

using (111) we get

**(117)** $A=\frac{z\sqrt{a+b}}{z^2-az+1}$

following the same steps as with equation (68), we abtain the result

**(118)** $x_n=\frac{\sqrt{a+b}}{\sqrt{a^2-4}}[(\frac{a+\sqrt{a^2-4}}{2})^n - (\frac{a-\sqrt{a^2-4}}{2})^n]$

the first elements of the sequence given in (111) can

be easily deduced form (118). We mentioned that the divisibility condition (42) is a special case of the non- divisibility (91),where $w^2$ corresponds to a, and b equals zero.In reference to (110) ,we see that all the elements of the sequence (118) are integers,hence (a+b) must be a square. According to what we have already mentioned ,we write $(a+b)=w^2$.Therefore (118) transforms to

**(119)** $x_n=\frac{w}{\sqrt{a^2-4}}[(\frac{a+\sqrt{a^2-4}}{2})^n - (\frac{a-\sqrt{a^2-4}}{2})^n]$

And the first elements of the sequence (111) become

**(120)**

| | | |
|---|---|---|
| n=0 | $x_0=0$ | $y_0 = -w$ |
| n=1 | $x_1=w$ | $y_1 = 0$ |
| n=2 | $x_2=aw$ | $y_2 = w$ |
| n=3 | $x_3=(a^2-1)w$ | $y_3 =a\ w$ |
| n=4 | $x_4=a(a^2-2)w$ | $y_4 =(a^2-1)w$ |

note that every element of the sequence is divisible by w. Whenever we equate the given positive odd integer x with any element of the sequence, we deduce that w must be odd. We can also prove that a must be odd. To this end, we suppose that a is even (and hence b odd, since $w^2 =a+b$).Rewrite (91) in the form

**(121)** $x^2 +y^2= a(xy+1)+b=axy+a+b=axy+w^2$

assume that y is odd, and take the remainders mod 4

**(122)** $1+1\equiv 0(\text{or}2)+1 \bmod 4$

In both cases of the remainders o(or2), equation (122) is impossible, hence y must be even. We conclude that if a is even, then y is even for all values of n in the sequence .In fact if a is even, the elements of the sequence alternate between odd and even values as we can easily prove. (for both sequences of x and y)

If $x_{2n}$ is even and $y_{2n}$ is odd using the recurrence (110) we deduce that $x_{2n+1}$ is odd and $y_{2n+1}$is even and $x_{2n+2}$is even and $y_{2n+2}$is odd .Since $x_2$ is even and $y_2$ is odd, our claim is justified. We conclude therefore that a must be odd and b even. Returning to (121) and taking the remainders mod 2,we get :

**(123)** $1+y^2\equiv y+1 \bmod 2$ i.e. $2 \mid y(y-1)$

and y may be odd or even, which is the case.

Whenever we equate the given positive odd integer x with an element of the sequence, then since w divides such an element, we deduce at once that w must be greater than Z, i.e. $w\geq Z+2$(Z is the largest known prime in TEST-2-). This is because, if $w \leq Z$, then w would be equal to a prime $p\leq Z$ *or* divisible be a prime $p\leq Z$ which means that x would be divisible by the same prime, contradicting the result of TEST -2-

assume that

**(124)** $a \leq Z$

since x and y are both divisible by primes greater than Z, we deduce that a is relatively prime to both x and y The condition of non – divisibility (91) applies, we can follow similar steps and get :

**(125)** $x^2+a^2= a_1(xa+1)+b_1= a_1xa+a_1+b_1= a_1xa+w_1^2$

**(126)** $y^2+a^2= a_2(ya+1)+b_2= a_2ya+a_2+b_2= a_2ya+w_2^2$

It is evident from (125) that if $w_1$ and a have a common divisor, this common divisor would divide x, contradicting our result that x and a are relatively prime. Moreover, if $w_1\geq x$, then from (125)

**(127)** $x^2+a^2= a_1xa+w_1^2 \geq a_1xa+x^2$ i.e. $a\geq a_1x$

contradicting the fact that x>a, hence

**(128)** $w_1<x$

also it is evident from (126) that if $w_2$ and a have a common divisor, this common divisor would divide y,

contradicting our result that y and a are relatively prime. Moreover, if $w_2 \geq y$, then from (126)

**(129)** $y^2+a^2= a_2ya+w_2^2 \geq a_2ya+y^2$ i.e. $a \geq a_2y$

contradicting the fact that the value of each element $y_n$ of the y sequence begining with n=3 onwards is greater than a, hence

**(130)** $w_2<y$

adding (125)and (126) we get

**(131)** $x^2+ y^2+2a^2= a(a_1x+a_2y)+w_1^2 + w_2^2$

taking the remainders mod a

**(132)** $x^2+ y^2\equiv w_1^2 + w_2^2 \mod a$

taking the remainders mod a for equation (121) we get

**(133)** $x^2+ y^2\equiv w^2 \mod a$

from (132) and (133) we arrive at the result

**(134)** $w^2 \equiv w_1^2 + w_2^2 \mod a$

we began with two positive integers x,y satisfying the non-divisibility condition (91) and hence (133) and ended with two positive integers $w_1<x$ and $w_2< y$ satisfying (134),since $w_1$ and a are relatively prime, and $w_2$ and a are also relatively prime, we can formulate two new equations:

**(135)** $w_1^2+a^2= a_3w_1a+w_3^2$

**(136)** $w_2^2+a^2= a_4w_2a+w_4^2$

and conclude that

**(137)** $w_3^2+w_4^2 \equiv w^2 \mod a$

$(w_3 < w_1)$ $and$ $(w_4 < w_2)$

we cannot go on repeating similar steps, because of the principle of the impossibility of infinite descent, thus our assumption that $a \leq Z$ is false and

**(138)** $a \geq Z+2$

Let us equate the given odd positive integer x with an element of the sequence

**(139)** $x=\frac{w}{\sqrt{a^2-4}}[(\frac{a+\sqrt{a^2-4}}{2})^n - (\frac{a-\sqrt{a^2-4}}{2})^n]$

we make the substitution

**(140)** $t = \frac{a+\sqrt{a^2-4}}{2}$ hence (139) takes the form

**(141)** $x=\frac{wt}{t^2-1}$ $(t^n-\frac{1}{t^n})$

we expand this equation in powers of t

**(142)** $wt^{2n}- xt^{n+1}+xt^{n-1}- w =0$

refering to the theorem for the upper limit to the real roots of a polynomial equation, we have for equation (142)

**(143)** $a_0= w$ G=x K=n-1

therefore, the upper limit to the real roots t in this

case is

**(144)** $t \leq 1+(\frac{x}{w})^{\frac{1}{n-1}}$

but $\frac{x}{w} < x$

and since w<x, we have

**(145)** $t\leq 1+(x)^{\frac{1}{n-1}}$

according to (140)

**(146)** $\frac{a+\sqrt{a^2-4}}{2} = t\leq 1+(x)^{\frac{1}{n-1}}$

since Z+2≤ a (Z the largest known prime mentioned in TEST-2- ) we have

**(147)** $a +\sqrt{(Z+2)^2-4} \leq a+\sqrt{a^2-4} \leq 2\ (1+x^{\frac{1}{n-1}})$

i.e.

$a \leq 2\ (1+x^{\frac{1}{n-1}})- \sqrt{(Z+2)^2-4}$

from (139)

**(148)** $x=\frac{w}{\sqrt{a^2-4}}(\frac{a+\sqrt{a^2-4}}{2})^n[1 - (\frac{a-\sqrt{a^2-4}}{a+\sqrt{a^2-4}})^n]$

$< \frac{w}{\sqrt{a^2-4}}(\frac{a+\sqrt{a^2-4}}{2})^n$

$= \frac{a^n w}{a\sqrt{1-\frac{4}{a^2}}}\frac{1}{2^n}( 1+\frac{\sqrt{a^2-4}}{a})^n$

$< \frac{a^n w}{a\sqrt{1-\frac{4}{a^2}}}\frac{1}{2^n} 2^n$

$$= \frac{a^n w}{a\sqrt{1-\frac{4}{a^2}}}$$

Since Z+2 ≤ a

$$\frac{1}{\sqrt{1-\frac{4}{(Z+2)^2}}} \geq \frac{1}{\sqrt{1-\frac{4}{a^2}}}$$

Since w =$\sqrt{\square + \square} < \sqrt{\square}$ we have x<$\frac{\sqrt{\square}\,\square^{\square-1}}{\sqrt{1-\frac{4}{(\square+2)^2}}}$

i.e. $\sqrt{\square}\sqrt{1-\frac{4}{(\square+2)^2}} < a^{n-1}$ hence

**(149)** a> $\square^{\frac{1}{2(\square-1)}}(1-\frac{4}{(\square+2)^2})^{\frac{1}{2(\square-1)}}$

If for a given n,we assume that x= $x_n$ ,we get a polynomial equation in the unknown a .In this case (147) and (149)represent the upper and lower bounds of the unknown a,respectively.

As in the case of divisibility,we have to prove that,if n is a multiple of 3,then its' corresponding element of the sequence $x_n$ is even,and hence must be discarded.

Suppose that for some value of n which is a multiple of 3(n=3m)the corresponding element $x_n$ of the sequence is even,while $y_n$ is odd.According to(110) , $x_n$ would be odd and $y_n$ even for n=3m+1.Now for n=3m+2,and using (110)again,we conclude that both $x_n$ and $y_n$ are odd.Employing(110)for n=3m+3 leads us to the conclusion that the element of the sequence

$x_n$ is even,while $y_n$ is odd.In reference to (120) we see that

for n=3 the element $x_3$ is even,while $y_3$ is odd.By mathematical induction,our claim is justified.

Rewrite(139)in the form

$$x=\sqrt{\square + \square}\,[\,(\frac{\square+\sqrt{\square^2-4}}{2})^{\square-1} + (\frac{\square+\sqrt{\square^2-4}}{2})^{\square-2}(\frac{\square+\sqrt{\square^2-4}}{2}) + \cdots + (\frac{\square-\sqrt{\square^2-4}}{2})^{\square-1}]$$

According to this equation,it is evident that,since x is given ,if a increases,n decreases,and vice versa.

rewrite(141) in the form

**(150)** $\frac{\square(\square^2-1)}{\square\square} = t^n - \frac{1}{\square^{\square}}$

making the following substitutions

**(151)** **d=** $\frac{\square(\square^2-1)}{\square\square}$ v= $t^n$

transforms(150)into a quadratic equation

**(152)** $\square^2$-dv -1=0 taking the positive root of (152)

**(153)** $v = \frac{\square+\sqrt{\square^2+4}}{2}$

**and substituting $t^n$ for v according to(151)**

we can calculate the value of the unknown n.Here we assume that t and w are known,and ofcourse x is known.

To get an upper bound for n,according to what we have already mentioned,we substitute(Z+2)for a in(140) and also for w in(150)and go on to solve equation(152)and get the positive root v from(153).Using this root ,we get a value for n from(151).From this value,we calculate the least positive integer not divisible by 3 greater than or equal to the value.Let this integer be $m_2$.Let $n_2$ be the greatest of $m_2$and the previous $n_2$of TEST-4-.Ofcourse,if they are equal,we take any one of them.

We know from(102)that x>a+b(=$\square^2$), $h\square\square\square\square\ \square < \sqrt{\square}$.Reviewing the elements of the sequence(111),we arrive at the result that for all values of n≥ *3*, $\square h\square\ \square\square\square\square\square\square\square\square\square\square\ \square < \sqrt{\square}$ is satisfied.

Let r be the greatest odd positive integer less than or equal to $\sqrt{\square}$. To get a lower bound for n,we substitute r for a in (140) and for w in (150) and go on to solve equation (152) and get the positive root v from (153).Using this root we get a value for n from (151).From this value,we calculate the greatest positive integer not divisible by 3 less than or equal to the value.

Let this integer be $m_1$ .Let $n_1$be the smallest of $m_1$ and the previous $n_1$ of TEST-4-.Ofcourse,if they are equal we take any one of them.

since $\square^2(=\square+\square) > \square$, $\square\square$ deduce that $\square > \sqrt{\square}$.

using (149) we arrive at the result

**(154)** $w> \ \square^{\frac{1}{4(\square-1)}}\ (1-\frac{4}{(\square+2)^2})^{\frac{1}{4(\square-1)}}$

This is a lower bound for w.

we get from equation (139)

**(155)** $x=\frac{\square}{\sqrt{\square^2-4}}\ (\frac{\square+\sqrt{\square^2-4}}{2})^{\square}[1\ -\ (\frac{\square-\sqrt{\square^2-4}}{\square+\sqrt{\square^2-4}})^{\square}]$ we have that

**(156)** $\frac{\square-\sqrt{\square^2-4}}{\square+\sqrt{\square^2-4}}=\frac{4}{\square+\sqrt{\square^2-4}}\ \frac{1}{\square+\sqrt{\square^2-4}}<\frac{1}{2}$ hence

$(\frac{\square-\sqrt{\square^2-4}}{\square+\sqrt{\square^2-4}})^{\square} < \frac{1}{2^{\square}}$ therefore

**(157)** $1\ -\ (\frac{\square-\sqrt{\square^2-4}}{\square+\sqrt{\square^2-4}})^{\square}>1-\frac{1}{2^{\square}}$

from (147) we can calculate an upper bound for $\sqrt{\square^2 - 4}$ .Let this upper bound be U1,hence

**(158)** $\frac{1}{\sqrt{\square^2-4}} > \frac{1}{\square 1}$

from (149) we can calculate a lower bound for

$(\frac{\square+\sqrt{\square^2-4}}{2})^2$, let this lower bound be U2.

We deduce from (155) by using (157) that

**(159)** $x > \frac{\square\,\square 2}{\square 1}(1 - \frac{1}{2^{\square}})$ i.e.

$w < \frac{\square\,\square 1}{\square 2(1-\frac{1}{2^{\square}})}$ this is an upper bound for w.

now we are ready for TEST-5-

TEST-5-

1. 1. for i=$n_2$ to $n_1$ step -1.
2. if i is divisible by 3,then goto 15.
3. substitute i for n in (85) and get the old lower bound $r_2$ of the unknown w, let $w_2$ be the greatest positive odd integer less than or equal to $r_2$.
4. substitute i for n in (154) and get the new lower bound $r_1$ of the unknown w, let $w_1$ be the greatest positive odd integer less than or equal to $r_1$
5. if $r_2 < r_1$ then goto 9.
6. for j= $r_1$ to $r_2$ step 2.
7. if j divides x then goto 17.
8. next j.
9. substitute i for n in (80) and get the old upper bound $r_1$ of the unknown w, let $w_1$ be the least positive odd integer greater than or equal to $r_1$.
10. substitute i for n in (156) and get the new upper bound $r_2$ of the unknown w, let $w_2$ be the least positive odd integer greater than or equal to $r_2$.
11. If $w_1 > w_2$ then goto 15.
12. for j= $w_1$ to $w_2$ step 2.
13. If j divides x then goto 17
14. next j
15. next i
16. print : x is prime : halt : we are done.
17. print : x is composite : halt : we are done

## REFERENCES

[ 1 ] Aigner, Martin; Ziegler, Gunter M. (2002)

"Proofs from The Book" ,New York ; Springer – Verlag.

[ 2 ] Ribenboim, Paulo (1988)" The Book of Prime Number Records " , New York; Sprintger.

[ 3 ] Wilf, Herbert S . (1994) " Generatingfunctionology", London; Academic Press.

[ 4 ] Dickson, Leonard Eugene (1922)" First Course in The Theory of Equations " , New York; John Wiley.

[ 5 ] Schroeder, M.R.(1986)" Number Theory in Science and Communication ", New York ; Springer – Verlag.

[ 6 ] Rader, Robert J.(1978) " Advanced Software Design Techniques" , Princeton; Petrocelli Books,Inc.

[ 7 ] Koblitz,Neal (1987)" A Course in Number Theory and Cryptography ", New York ; Springer – Verlag.

[ 8 ] Guy, Richard K.(1994) " Unsolved Problems in Number Theory" , New York ; Springer – Verlag.