International Journal of Pure and Applied Mathematics
Volume 57 No. 3 2009, 419-433

SPECIAL SEMI-GROUPS IN ELEMENTARY NUMBER THEORY

Mohamed Mansour
Die Eidgenössische Technische Hochschule (ETH) – Zürich
(Swiss Federal Institute of Technology – Zurich)
Automatic Control Laboratory
ETL I 11, Physikstrasse 3, Zurich, 8092, SWITZERLAND
e-mail: mansour@control.ee.ethz.ch
url: www.control.ethz.ch/info/people/mansour

Abstract: A new definition of a prime number is given, showing also its relation with the solution of a quadratic equation. Different trivial classifications of odd natural numbers as well as a new grouping of them, in two commutative semi-groups and their cross mapping into a set closed under multiplication, is given. In this grouping the prime numbers are distributed between the two semi-groups. The first semi-group has, as generators the primes which are the sum of two squares, one odd and the other even. The second semi-group has as generators the rest of the primes. The third set is generated by cross multiplication of the first two semi-groups. Combining a trivial classification with this grouping we may get a simplification in checking primness of some natural numbers and some information on the factorization. Also some extensions of Wilson Theorem is presented using these classifications and two new terms are introduced; the single number of sos prime and its multiplication factor.

AMS Subject Classification: 11Axx, 11Exx,
Key Words: number theory, prime number, sos prime

1. Definition of a Prime

We define an odd composite number as follows:

Received: November 14, 2009

Definition. An odd natural number $x > 1$ is composite if $\exists n$ and m such that

$$x = n^2 + 2nm = (n+m)^2 - m^2, \tag{1}$$

where n is odd and is greater than 1 and $m = 0, 1, 2, 3, 4, 5, \ldots$ n is a factor.

Let $n \to 2n + 3$ where $n, m = 0, 1, 2, 3, 4, 5, \ldots$. Then

$$x = 4n^2 + 4nm + 12n + 6m + 9 \tag{2}$$

can be written

$$x = \begin{bmatrix} n & m & 1 \end{bmatrix} \begin{bmatrix} 4 & 2 & 6 \\ 2 & 0 & 3 \\ 6 & 3 & 9 \end{bmatrix} \begin{bmatrix} n \\ m \\ 1 \end{bmatrix}, \tag{3}$$

i.e. x is composite if $\exists n$ and m such that (3) is satisfied; otherwise x is prime.

From (1) $n = -m + \sqrt{m^2 + x}$. Choose $m = \frac{x-1}{2}$ then $n = 1$ which is the same for primes and composites. However for x composite with factor 3 we have $n = 3$ and $m = \frac{x-9}{6}$. For x composite with factor 5, we have $n = 5$ and $m = \frac{x-25}{10}$. For x composite with factor p we have $n = p$ and $m = \frac{x-p^2}{2p}$. Hence x is prime if equation (1) has only one solution $n = 1$; otherwise x is composite. In this case it is easy to show that the number of solutions is equal to the number of different factors which are less than plus the trivial solution $n = 1$. Also it is known that any odd number is a difference between two squares, one odd and the other even, e.g. $29 = 15^2 - 14^2$ and $45 = 23^2 - 22^2 = 9^2 - 6^2 = 7^2 - 2^2$. It is easy to see that for a prime there is only one difference of squares, namely $((x+1)/2)^2((x-1)/2)^2$ and for a composite there are as many solutions as there are different factors less than $\sqrt{x}$ in addition to the above solution as for primes. For a prime factor $p < \sqrt{x}$ the solution is $((x+p^2)/2p)^2((x-p^2)/2p)^2$. For composite numbers fulfilling $5 + 4k^*$, they are given by $n^2 + 4nk = (n+2k)^2(2k)^2$. For composite numbers fulfilling $3 + 4k^*$, they are given by $n^2 + 2n + 4nk = (n+1+2k)^2(1+2k)^2$. n is a factor of the composite number, $n = 3, 5, 7, \ldots$, and $k = 0, 1, 2, 3, \ldots$.

2. Trivial Grouping of Natural Numbers

1. Two arithmetic series $3 + 4k$ and $5 + 4k$ each containing almost half the primes. Later we show the use of this classification in getting some information on factorization.

2. Three arithmetic series $3+6k$, $5+6k$ and $7+6k$. The first series contains composite numbers with prime factor 3 except 3 itself which is prime. Each

one of the two other series has almost half the primes.

3. Combining the two classifications or dividing each series in (2) into two series we get six arithmetic series: $3+12k$, $5+12k$, $7+12k$, $9+12k$, $11+12k$ and $13+12k$. The series $3+12k$ and $9+12k$ have all the composite numbers who have prime factor 3 (exept 3 itself which is prime). Each of the other four series has almost one quarter of the primes. Each series can be divided in two series and so on.

3. A New Classification of Natural Numbers

Now consider all the odd natural numbers who are sum of squares (denoted sos) a_2+b_2 where a is odd and b even and $(a,b)=1$ or $(a,b)=c$ where c itself is sos. The sos numbers <100 are : $5,13,17,25,29,37,41,53,61,65,73,85,89,97$, eleven primes and three composites. "The sos numbers constitute a set A which can be proved to be a commutative semi-group under multiplication and whose generating set is the sos primes." Proof of closeness under multiplication: $(a_1^2+b_1^2)(a_2^2+b_2^2)=(a_1a_2+b_1b_2)^2+(a_1b_2-a_2b_1)^2$. Without loss of generality let $(a_2^2+b_2^2)$ be prime. Assume $a_1a_2+b_1b_2=\alpha A$ and $a_1b_2-a_2b_1=\alpha B$, α is not sos, then $a_1(a_2^2+b_2^2)=\alpha(a_2A+b_2B)$ and $b_1(a_2^2+b_2^2)=\alpha(b_2A-a_2B)$ then $a_1\&b_1$ have α as a factor which is no sos. This is contradiction hence the sos set is closed under multiplication hence a commutative semi-group. The generating set of this semi-group is the set of sos primes. We show that x is sum of squares, if and only if $2x$ is a sum of odd squares. Let $x=a_2+b_2$ then $2x=2a^2+2b^2=(b-a)^2+(b+a)^2$. The proof in the other direction is similar. Now consider another commutative semi-group whose generating set is the set of primes which are not sos (denote them by nsos primes). The nsos numbers <100 are: 3, 7, 9, 11, 19, 21, 23, 27, 31, 33, 43, 47, 49, 57, 59, 63, 67, 69, 71, 77, 79, 81, 83, 93, 99, thirteen primes and twelve composites. Denote this set by B. A third set C is obtained through cross multiplication of $A\&B$ $C=A\times B$. This set is also closed under multiplication as the original sets are closed under multiplication.

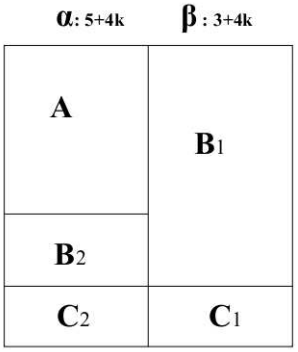
Combinig the above classification with the trivial classification $3+4k$ and $5+4k$ we get the following diagram:

A: sos numbers;

B: nsos primes and the generated composites. $B=B_1\cup B_2$;

B_1: nsos primes and their odd number of multiplications;

B_2: even number of multiplications of the nsos primes;



$C = A \times B = C_1 \cup C_2$;

C_1: cross multiplication $A \times B_1$;

C_2: cross multiplication $A \times B_2$.

It is easy to see that A, B, and C include all the odd numbers > 1

$$\alpha = A \cup B_2 \cup C_2, \qquad \beta = B_1 \cup C_1.$$

To show that we have

$$\begin{aligned}(3+4k_1)(3+4k_2) &= 9+4k_3 = 5+4k,\\ (3+4k_1)(3+4k_2)(3+4k_3) &= 27+4k_4 = 3+4k,\\ (5+4k_1)(5+4k_2) &= 5+4k,\\ (5+4k_1)(3+4k_2) &= 15+4k_3 = 3+4k.\end{aligned}$$

Remark 1. It can be easily shown that the sum of odd squares is always the set A multiplied by 2. This is on the assumption that a and b are either co-prime or have common factors which are sos. Also the addition of even squares under the same condition is $2i$ times a sos number where $i > 1$.

Remark 2. To prove that an odd natural number x is in A: x should be expressed as $x = 5 + 4k$, i.e. in $\alpha.x$ should not have nsos prime factors less than $\sqrt{x}$. This is possible because B_2 and C_2 have even number of nsos prime factors. Thus the effort is approximately half the effort for proving primness.

4. Some Applications

1. $\mathbf{2^n - 1}$: $2^n - 1$ - 3 has factor 4, hence $2^n - 1$ is in β.

If n even it has an odd number of nsos primes including 3 and is in $\mathbf{B_1}$ or

$\mathbf{C_1}$. If n odd it has an odd number of nsos primes and is in $\mathbf{B_1}$ or $\mathbf{C_1}$. If n prime then it is a Mersenne number.

2. $\mathbf{2^n + 1}$: 2^n+1 -5 has factor 4, hence 2^n+1 is in α.

If n even it is sos number and is in $\mathbf{A}$. If n odd it has even nsos primes including 3 and is in $\mathbf{B_2}$ or $\mathbf{C_2}$.

3. $\mathbf{10^n - 1}$: 10^n-1 is in β.

If n even or odd it has odd number of nsos primes including 3×3 and is in $\mathbf{B_1}$ or $\mathbf{C_1}$.

4. $\mathbf{10^n + 1}$: $10^n + 1$ is in α.

If n even then it is sos number and hence in $\mathbf{A}$. If n odd it has even number of nsos primes and hence in $\mathbf{B_2}$ or $\mathbf{C_2}$.

5. The squares of sos primes are sos and are the solution of Fermat Theorem for quadratics. Actually the same holds for the squares of any sos number which is a matter of scaling.

5. Sos Prime Decomposition of Sos Composite Numbers

(A) Different sos prime factors:

For two sos prime factors p_1 & p_2

$$\begin{aligned} x = p_1p_2 &= ({a_1}^2 + {b_1}^2)({a_2}^2 + {b_2}^2) \\ &= (a_1a_2 - b_1b_2)^2 + (a_1b_2 + a_2b_1)^2 \\ &= (a_1a_2 + b_1b_2)^2 + (a_1b_2 - a_2b_1)^2. \end{aligned} \tag{4}$$

These two decompositions are valid also if p_1 & p_2 are composite factors. (4) shall be used often in this section, e.g. p_1=5, p_2= 13 then

$$65 = (1^2 + 2^2)(3^2 + 2^2) = 1^2 + 8^2 = 7^2 + 4^2.$$

Each multiplication gives two new decompositions using (4), so that for x = $p_1p_2p_3$ we get 4 decompositions.

For x= p_1p_2 .....p_n we get 2^{n-1} decompositions, e.g. p_1 =5, p_2 = 13, p_3=17

$$\begin{aligned} x = 1105 &= 31^2 + 12^2 \\ &= 33^2 + 4^2 \\ &= 9^2 + 32^2 \\ &= 23^2 + 24^2. \end{aligned}$$

(B) Equal sos prime factors:

For x=$p^2 = a^2+b^2$ we get $(a^2- b^2)^2 + (2ab)^2$ only one solution (2a).

For x =$p^3=(a^2+b^2)^3$ we get two solutions.

$$(a^3 - 3ab^2)^2 + (3a^2b - b^3)^2, \tag{3a}$$

and

$$(a^3 + ab^2)^2 + (a^2b + b^3)^2 = (a^2 + b^2)^2(a^2 + b^2). \tag{3b}$$

(3b) is a scaling of p.

For x=$p^4=(a^2+b^2)^4$, (3a) produces two solutions:

$$(a^4 - 6a^2b^2 + b^4)^2 + (4a^3b - 4ab^3)^2, \tag{4a}$$

and

$$(a^4 - b^4)^2 + (2a^3b + 2ab^3)^2 \ = (a^2 + b^2)^2[(a^2 - b^2)^2 + (2ab)^2]. \tag{4b}$$

(4b) is a scaling 0f (2a).

And (3b) produces one solution (because (3b) is a scaling of p and p^2 gives only one solution).

$$(a^4 - b^4)^2 + (2a^3b + 2ab^3)^2. \tag{4c}$$

(4c) is the same as (4b). Hence we have only two solutions (4a) and (4b).

For x=$p^5=(a^2+b^2)^5$, (4a) produces two solutions

$$(a^5 - 10a^3b^2 + 5ab^4)^2 + (5a^4b - 10a^2b^3 + b^5)^2, \tag{5a}$$

and

$$\begin{aligned}(a^5 - 2a^3b^2 - 3ab^4)^2 + (3a^4b + 2a^2b^3 - b^5)^2 \\ = (a^2 + b^2)^2[(a^3 - 3ab^2)^2 + (3a^2b - b^3)^2]\end{aligned} \tag{5b}$$

which is a scaling of (3a). (4b) produces two solutions.

$$(a^5 - 2a^3b^2 - 3ab^4)^2 + (3a^4b + 2a^2b^3 - b^5)^2 \tag{5c}$$

which is the same as (5b), and

$$\begin{aligned}(a^5 + 2a^3b^2 + ab^4)^2 + (a^4b + 2a^2b^3 + b^5)^2 \\ = (a^2 + b^2)^4(a^2 + b^2),\end{aligned} \tag{5d}$$

which is a scaling of p.

Thus we have three solutions (5a), (5b), (5d).

For x=$p^6=(a^2+b^2)^6$, (5a) produces two solutions

$$(a^6 - 15a^4b^2 + 15a^2b^4 - b^6)^2 + (6a^5b - 20a^3b^3 + 6ab^5)^2, \tag{6a}$$

and

$$(a^6 - 5a^4b^2 - 5a^2b^4 + b^6)^2 + (4a^5b - 4ab^5)^2 \tag{6b}$$

$$= (a^2+b^2)^2[(a^4-6a^2b^2+b^4)^2+(4a^3b-4ab^3)^2]$$

which is scaling of (4a). (5b) produces two solutions

$$(a^6-5a^4b^2-5a^2b^4+b^6)^2+(4a^5b-4ab^5)^2 \tag{6c}$$

which is the same as (6b), and

$$(a^6+a^4b^2-a^2b^4-b^6)^2+(2a^5b+4a^3b^3+2ab^5)^2 \tag{6d}$$

$$= (a^2+b^2)^4[(a^2-b^2)^2+(2ab)^2]$$

which is scaling of (2a). (5d) produces one solution

$$(a^6+a^4b^2-a^2b^4-b^6)^2+(2a^5b+4a^3b^3+2ab^5)^2 \tag{6e}$$

which is the same as (6d).

Hence only three solutions (6a), (6b), (6d).

For x=p^7=(a^2+b^2)^7, (6a) produces two solutions

$$(a^7-21a^5b^2+35a^3b^4-7ab^6)^2+(7a^6b-35a^4b^3+21a^2b^5-b^7)^2 \tag{7a}$$

and

$$(a^7-9a^5b^2-5a^3b^4+5ab^6)^2+(5a^6b-5a^4b^3-9a^2b^5+b^7)^2 \tag{7b}$$

$$= (a^2+b^2)^2[(a^5-10a^3b^2+5ab^4)^2+(5a^4b-10a^2b^3+b^5)^2],$$

which is scaling of (5a).

(6b) produces two solutions

$$(a^7-9a^5b2-5a^3b^4+5ab^6)^2+(5a^6b-5a^4b^3-9a^2b^5+b^7)^2 \tag{7c}$$

which is the same as (7b), and

$$(a^7-a^5b^2-5a^3b^4-3ab^6)^2+(3a^6b+5a^4b^3+a^2b^5-b^7)^2$$

$$= (a^2+b^2)^4[(a^3-3ab^2)^2+(3a^2b-b^3)^2]$$

which is scaling of (3a). (6d) produces two solutions

$$(a^7-a^5b^2-5a^3b^4-3ab^6)^2+(3a^6b+5a^4b^3+a^2b^5-b^7)^2, \tag{7e}$$

which is the same as 7d and

$$(a^7+3a^5b^2+3a^3b^4+ab^6)^2+(a^6b+3a^4b^3+3a^2b^5+b^7)^2=(a^2+b^2)^6(a^2+b^2) \tag{7f}$$

which is scaling of p. Thus we have four solutions (7a), (7b), (7d), (7f).

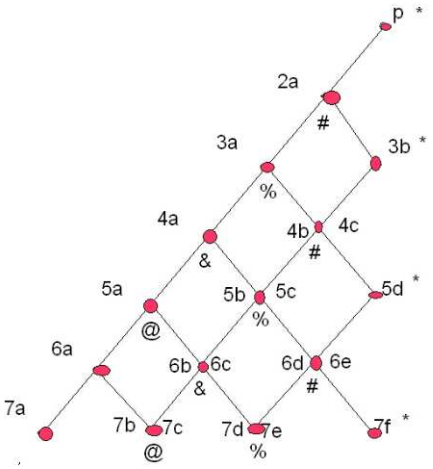
Example. p=5, p^7 = 78125. Then:

(7a) gives 29^2+278^2;

(7b) gives 205^2+190^2;

(7d) gives 275^2+50^2;

and (7f) gives 125^2+250^2.



For p^1,p^2,... p^7 we get the following representation

The scaled nodes have the same marking. From the symmetry and the construction we can deduce the following results:

p or p^2 we get one solution;

p^3 or p^4 we get two solutions;

p^5or p^6 we get three solutions, and so on;

p^{m-1} or p^m we get m/2 solutions where m is even, i.e. if we have $x=p_1{}^m p_2p_3 \dots p_n$ then the number of solutions is $m/2(2^{n-1}) = m.2^{n-2}$.

6. Wilson Theorem and its Extensions

Wilson Theorem.

$$p \text{ is prime, if and only if } (p-1)! + 1 = 0(\mathrm{mod}p). \tag{5}$$

This theorem gives a necessary and sufficient condition for p to be prime, but it is not practical to use due to the excessive computation time for large numbers. The following extensions are in the direction of reduction of computation time. If this direction is followed further we may get after a while a practical algorithm for checking primality..The following extensions can be proved in a trivial way

Extension 1. p is prime, if and only if

$$(p-2)!-1=0(\mathrm{mod}p). \tag{6}$$

Proof. (p-1)! +1=0 (mod p) → (p-2)!.(p-1) +1 =0 (mod p) →
-(p-2)! +1= 0 (mod p)→ (p-2)! -1 =0 (mod p).

Extension 2. p is prime, if and only if

$$(p-3)!-\frac{p-1}{2}=0(\mathrm{mod}p). \tag{7}$$

Proof. (p-2)! -1 =0 (mod p)→(p-3)! (p-2) -1 =0(mod p)→
(p-3)! (-2) +p -1 =0(mod p)→ (p-3)! -$\frac{p-1}{2}$ =0 (mod p).
Also: p is prime, if and only if (p-3)!.2+1=0(mod p).

Extension 3. For p=7+6k where k=0,1,2,.... p is prime, if and only if

$$(p-4)!+\frac{p-1}{6}=0(\mathrm{mod}p). \tag{8}$$

Proof. (p-3)! - $\frac{p-1}{2}$ =0 (mod p)→ (p-4)!.(p-3)-$\frac{p-1}{2}$ =0(mod p)→
(p-4)! +$\frac{p-1}{6}$ =0 (mod p)

Extension 4. For p=3+4k, where k= 0,1,2,... p is prime if and only if

$$\frac{p-1}{2}!+1=0(\mathrm{mod}p) \text{ or } \frac{p-1}{2}!--1=0(\mathrm{mod}p). \tag{9}$$

Proof. (p-1)! +1 =0 (mod p) → ($\frac{p-1}{2}$)!.(p-1).(p-2)...$\frac{p+1}{2}$+1=
0(mod p) → ($\frac{p-1}{2}$)!^{2} -1 =0 (mod p)→ $\frac{p-1}{2}$!+1=0 (mod p)
or $\frac{p-1}{2}$! -1=0 (mod p)

Extension 5. For p=5+4k where k=0,1,2,... p is prime, if and only if

$$\frac{p-1}{2}\frac{p-1}{2})!^2+1=0(\mathrm{mod}p). \tag{10}$$

Proof. (p-1)! +1 =0 (mod p)→($\frac{p-1}{2}$)!..(p-1).(p-2)....$\frac{p+1}{2}$ +1= 0(mod p)→
($\frac{p-1}{2}$)!^{2} +1 =0(mod p)

Extension 6. For p=3+4k where k=0,1,2,... p is prime, if and only if

$$\frac{p+1}{4}!.(1.3.5.7...\frac{p-5}{2})+(-1)^{(\text{p-3})/4}.2exp.\frac{p-3}{4}=0(\mathrm{mod}p). \tag{11}$$

Proof. $\frac{p-1}{2}$! + 1 =0 (mod p)→ $\frac{p+1}{4}$! .$\frac{p-1}{2}$.$\frac{p-3}{2}$....$\frac{p+5}{4}$ + 1 =0 (mod p) →
$\frac{p+1}{4}$!. 1.3.5.7....$\frac{p-5}{2}$ + (-1)$^{(\text{p-3})/4}$ .2 exp. $\frac{p-3}{5}$ =0 (mod p)

Extension 7. From extension 4 we have $\frac{p-1}{2}$! + 1(or -1)= 0 (mod p).
For $\frac{p-1}{2}$!= 2.3.4..... $\frac{p-1}{2}$ we show that this is composed of $\frac{p-3}{4}$ pairs n

and m who give either nm= +1(mod p) , or nm= -1(mod p).

Let n be an integral $2 < n < \frac{p-1}{2}$

Therefore the following equation is satisfied:

$$r.p + (or-)1 = 0(\mathrm{mod} n) \text{ and } m = \frac{rp + (or-1)1}{n},$$

where r_{min} is less or equal $\frac{n-1}{2}$ for n odd and less or equal $\frac{n+1}{3}$.

For n even: This can be shown to be satisfied using the window of n including the prime p. This means that $2< m < \frac{p-1}{2}$.

m is different from n and for n=2 we get m=$\frac{p-1}{2}$.

In general:

For n=2, r=1, m=$\frac{p-1}{2}$,

n=3, r=1, m= $\frac{p+(or-)1}{3}$,

n=4, r=1, m=$\frac{p+1}{4}$,

n=5, r=1 for p beginning with ziffer 1 or 9 & m=$\frac{p-1}{5}$ or $\frac{p+1}{5}$ respectively,

r=2 for p beginning with ziffer 3 or 7 & m=$\frac{p-1}{2}$ or $\frac{2p+1}{5}$ respectively,

n=6, r=1, m=$\frac{p+(or-1)}{2}$,

n=7, $1 \leq r \leq 3$, m=$\frac{rp+(or-)1}{7}$,

n=8, $1 \leq r \leq 3$, m=$\frac{rp+(or-)1}{8}$,

n=9, $1 \leq r \leq 4$, m=$\frac{rp+(or-)1}{9}$,

n=10, r=1 for p beginning with ziffer 1 or 9 & m=$\frac{p-1}{10}$ or $\frac{p+1}{10}$ respectively,

r=3 for p beginning with ziffer 3 or 7 & m=$\frac{3p+1}{10}$ or $\frac{3p-1}{10}$ respectively.

and so on.

Example 1. n=7 & p=19 then r=3, m=8

p= 23 r=3, m=10,

p=31 r=2, m=9,

p=43 r=1, m=6,

p=47 r=3, m=20,

p=59 r=2, m=17,
p=67 r=2, m=19,
p=71 r=1, m=10,
p=79 r=3, m=34,
p=83 r=1, m=12.

One can get a table for every nsos prime and every n. Thus we can state the following theorem:

"p satisfying p=3+4k is a prime if and only if the numbers 2,3,4,. . . , $\frac{p-1}{2}$ can be grouped in pairs such that each pair gives +(or-)1(mod p). (12)

Extension 8. From extension 5 we have $(\frac{p-1}{2})!^2$ +1=0(mod.p).

Similar to the above the integers between 2 and $\frac{p-1}{2}$ can be grouped in pairs n and m such that nm+(or-) 1=0(mod p).

However the number of integers is odd such that there is an integer s which we call single integer associated with p. It is clear that s^2 +1=0 (mod p) i.e. s^2+1 =rp. Thus all the sos primes which are given by k^2+1 give s=k and r=1 such as 17, 37, 101, 197,. . . .

The following table gives s and r for different sos primes:

p	r	s
5	1	2
13	2	5
17	1	4
29	5	12
37	1	6
41	2	9
53	10	23
61	2	11
73	10	27
89	13	34
97	5	22
101	1	10
109	10	33
113	2	15
137	10	37
149	13	44

157	5	28
173	37	80
181	2	19
193	34	81
197	1	14
229	50	107
233	34	89
241	17	64
257	1	16

. . . . . .

We have n$<\frac{p-1}{2}$ & rp=s^2 +1 $\rightarrow$ rp$<$ $(\frac{p-1}{2}$ $)^2$ +1$\rightarrow$

r(p-1) $<$ ($\frac{p-1}{2}$ $)^2$ $\rightarrow$ r$<$ $\frac{p-1}{4}$

We can formulate the following theorem:

"p satisfying p=5+4k is prime if and only if the numbers 2,3,4,. . . . . $\frac{p-1}{2}$ can be grouped in pairs which give +(or-)1 (mod *p) and a single number s where* s^2+1=rp

$$2<s<\frac{p-1}{2}." \tag{13}$$

The equation s^2 +1=rp has infinite number of solutions. If s is the solution inside the range, then lp[Warning: Draw object ignored]s_o is a solution where l=1,2,3,. . .

We call s the single number of the sos prime and r the multiplication factor of the sos prime.

To solve the equation: s^2 +1=rp, let p=a^2+b^2 and r=c^2+d^2.

Therefore rp= $(ac+bd)^2$ +$(ad-bc)^2$ .Choose c and d such that ad-bc =1. A scheme of doing that can be as follows for e.g. p=53, 53=7^2+2^2.

r=3^2+1=10 and s =7x3+2x1=23.

From the above we formulate the following theorem:

" p satifying p= 5+4k is prime if and only if there exists only one single number and no solution of s^2 *=rp in the range*

$$2<s<fracp-12." \tag{14}$$

The condition no solution of s^2 =rp isadded because powers of sos primes have such such solutions.

Example 2. p=13.

Wilson: 12! +1=479001601 =0 (mod 13).

Extension 1: 11! -1=39916799= 0 (mod 13).

Extension 2: 10! -6 = 3628794 =0 (mod 13).

Extension 3: 9! +2 =362882 =0 (mod 13).

Extension 5: $6!^2$ +1 =518401 =0 (mod 13).

Extension 8: (2,6),(3,4), s=5 & r=2.

Example 3. p=19.

Extension 4: 9!+1 =362881= 0 (mod 19).

Extension 6: 5!.1.3.5.7 $+2^4$ = 120.105 +16 =12616 =0 (mod 19), or 120 (mod 19).105 (mod 19) +16 = 6.10.+16=76=0(mod 19).

Extension 7: (2,9),(3,6),(4,5),(7,8).

7. Conclusions

A new definition of primes was given also relating the primes to the difference of squares. A new grouping of natural numbers is introduced which may give some information on the prime factors or in some cases may reduce the effort to check primness. It is also shown how sos composite numbers can be decomposed to different sum of squares possibilities. Some extensions of Wilsons theorem based on the trivial classifications are discussed and a single number s associated with the sos prime as well as a multiplication factor r are introduced

References

[1] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff, Jr., *Contemporary Mathematics*, American Mathematical Society, **22**, (1983).

[2] A. Jones Gareth, J. Mary Jones, *Elementary Number Theory*, Springer (1998).

[3] Emil Grosswald, *Representation of Integers as Sums of Squares*, Springer (1985).

[4] Thomas Koshy, *Elementary Number Theory with Applications*, Academic Press (2007).

[5] Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhaeuser (1994).

[6] James J. Tattersall, *Elementary Number theory in Nine Chapters*, Cambridge University Press (2005).

Appendix

The classification of odd numbers < 1000 is:
A : 80 sos primes:
5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197, 229, 233, 241, 257, 269, 277, 281, 293, 313, 317, 337, 349, 353, 373, 389, 397, 401, 409, 421, 433, 449, 457, 461, 509, 521, 541, 557, 569, 577, 593, 601, 613, 617, 641, 653, 661, 673, 677, 701, 709, 733, 757, 761, 769, 773, 797, 809, 821, 829, 853, 857, 877, 881, 929, 937, 941, 953, 977, 997

42 sos composites:
25, 65, 85, 125, 145, 169, 185, 205, 221, 265, 289, 305,.325, 365, 377, 425, 445, 481, 485, 493, 505, 533, 545, 565, 625, 629, 685, 689, 697, 725, 745, 785, 793, 841, 845, 865, 905, 925, 901, 949, 965, 985

B : 87 nsos primes:
3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199, 211, 223, 227, 239, 251, 263, 271, 283, 307, 311, 331, 347, 359, 367, 379, 383, 419, 431, 439, 443, 463, 467, 479, 487, 491, 499, 503, 523, 547, 563, 571, 587, 599, 607, 619, 631, 643, 647, 659, 683, 691, 719, 727, 739, 743, 751, 787, 811, 823, 827, 839, 859, 863, 883, 887, 907, 911, 919, 947, 967, 971, 983, 991

113 nsos composites:
9, 21,27, 33, 49, 57, 63, 69, 77, 81, 93, 99, 121, 129, 133, 141, 147, 161, 171, 177, 189, 201, 207, 209, 213, 217, 231, 237, 243, 249, 253, 279, 297, 301, 309, 321, 329, 341, 343, 361, 363, 381, 387, 393, 399, 413, 417, 423, 437, 441, 453, 469, 473, 483, 489, 497, 501, 513, 517, 529, 531, 537, 539, 553, 567, 573, 581, 589, 597, 603, 621, 627, 633, 639, 649, 651, 669, 681, 693, 711, 713, 717, 721, 729, 737, 747, 749, 753, 759, 781, 789, 813, 817, 837, 847, 849, 869, 889, 891, 893, 903, 913, 917, 921, 927, 931, 933, 961, 963, 973, 987, 989, 993

C :177 mixed composites:
15, 35, 39, 45, 51, 55, 75, 87, 91, 95, 105, 111, 115, 117, 119, 123, 135, 143, 153, 155, 159, 165, 175, 183, 187, 195, 203, 215, 219, 225, 235, 245, 247, 255, 259,

261, 267, 273, 275, 285, 287, 291, 295, 299, 303, 315, 319, 323, 327, 333, 335, 339, 345, 351, 355, 357, 369, 371, 375, 385, 391, 395, 403, 405, 407, 411, 415, 427, 429, 435, 447, 451, 455, 459, 465, 471, 475, 477, 495, 507, 511, 515, 519, 525, 527, 535, 543, 549, 551, 555, 559, 561, 575, 579, 583, 585, 591, 595, 605, 609, 611, 615, 623, 635, 637, 645, 655, 657, 663, 665, 667, 671, 675, 679, 687, 695, 699, 703, 705, 707, 715, 723, 731, 735, 741, 755, 763, 765, 767, 771, 775, 777, 779, 783, 791, 795, 799, 801, 803, 805, 807, 815, 819, 825, 831, 833, 835, 843, 851, 855, 861, 867, 871, 873, 875, 879, 885, 895, 897, 899, 909, 915, 923, 935, 939, 943, 945, 951, 955, 957, 959, 969, 975, 979, 981, 995, 999,