Wilson's Theorem:

Let p be a prime number. Then,

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof: **The theorem is clear for p=2,3.**

Assume that $p \geq 5$.

For each $a \in \mathbb{Z}$ such that $1 \leq a \leq p-1$,

There exists $\bar{a} \in \mathbb{Z}, 1 \leq \bar{a} \leq p-1$ such that

$$a\,\bar{a} \equiv 1 \bmod p \ldots.(1)$$

Further, $a=\bar{a}$ if,and only if, a=1 or a=p-1.

Note that, for $1 \leq b \leq p-1$,

$b^2 \equiv 1 \pmod{p}$ if, and only if,b=1 or b=p-1.

Pairing a and $\overline{a}$ in the product below and using(1),We have

$$\text{(p-1)!=1}\times\text{(p-1)}(\textstyle\prod_{9=2}^{P-2} j) \equiv -1 \text{ (mod p).} \qquad \blacksquare$$

<u>Theorem</u>: The quadralic congruence

$$x^2 \equiv -1(\text{mod p}),\text{-----}(1)$$

p a prime,has a solution if,and only if,p=2 or p ≡1(mod 4).

<u>Proof</u>: If p=2,then x=1 is a solution.

So,let p be odd.then,

$$-1 \equiv (p-1)! = \left(1 \ldots \frac{p_{-1}}{2}\right)\left(\frac{P+1}{2} \cdots (P-1)\right)$$

$$= \prod_{\mathbf{j=1}}^{(p_{-1})/2} \boldsymbol{j}(\boldsymbol{p}-\boldsymbol{j})$$

$$= (-1)^{(p-1)/2} \prod_{\mathbf{i=1}}^{(p_{-1})/2} \boldsymbol{j}^2 \text{ (mod p).} \qquad \blacksquare$$

So, if x = 1…. $\left(\frac{p-1}{2}\right)$ $x^2 \equiv -1 \pmod{p}$.

Thus, if $p \equiv 1 \pmod 4$, then x is a solution to the equation(1).

On the other hand , if $Y \in \mathbb{Z}$ is a solution to (1),Then

$$Y^2 \equiv -1 \pmod{p}$$

and p+y. Raising it to the power of $\frac{(p-1)}{2}$,

$$(Y^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Applying Fermat's last theorem to the left hand side, We get,

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

So, $p \equiv 1 \pmod 4$. ■

Theorem:

Let p be a prime such that

$p \equiv 1 \pmod 4$.

Then, $p=a^2+b^2$ for some integers a and b.

Proof: **Since $p \equiv 1 \pmod 4$, there exists an integer x such that**

$x^2 \equiv -1 \pmod 4$

Let k be the largest integer less than $\sqrt{p}$.

There, $k<\sqrt{p}<k+1$. Define

$A=[0,k+1] \times [0,k+1] \cap \mathbb{Z} \times \mathbb{Z}$

And $F: A \rightarrow \mathbb{Z}p$

By $f(u,v) = u+x\,v \pmod p$.

Then, $p<|A|$. So, there exist distinct elements (u_1,v_1) (u_2,v_2) in A,

Such that $f(u_1,v_1) = f(u_2,v_2) \pmod{p}$.

Let $a = u_1-u_2$ and $b= v_1-v_2$. Then

$$a \equiv -x\, b \pmod{p}.$$

So,

$$a^2 \equiv x^2 b^2 \equiv -b^2 \pmod{p}.$$

Thus, $p \mid (a^2+b^2)$-----(i)

Since $0\leq m \leq k$ and $u_2\geq 0$, $0 \leq a^2<p$.

Similarly, $0 \leq b^2 \leq p$. Further, either

a or b in non zero. So, $\blacksquare$

$$O<a^2+b^2 <2p\text{-----(ii)}$$

Now (i) and (ii) implies that $p=a^2+b^2$.

Theorem:(Fermat)

Let p be a prime, $p \equiv 3 \pmod 4$, and

$a,b \in \mathbb{Z}$ such that $a^2+b^2 \equiv 0 \pmod p$.

Then,p divides both a and b.

Proof: We show that, if p does not divide

a as well as b,then $p \equiv 1 \pmod 4$.

Since $(a,p)=1$ and $(b,p)=1$,

there exist integers a_1 and b_1 such that

$a a_1 \equiv 1 \pmod p$ and $bb_1 \equiv 1 \pmod p$.

So,

$$1 \equiv (a\ a_1) \equiv -(b\ \overline{a})^2 \pmod p,$$

because, $a^2 \equiv -b^2 \pmod p$.

Consequently, $x^2 \equiv -1 \pmod p$ has a solution.

But by theorem,

$p \equiv 1 \pmod 4$, a contradiction to the hypothesis.

So, p divides either a or b.

But since p divides a^2+b^2,

P divides both a and b. $\blacksquare$

<u>Theorem</u> (Fermat)

Let $n \in \mathbb{Z}$, $n>0$ and

$$n = 2^a \left(\prod_{i=1}^{r} p_i^{b_i}\right) \left(\prod_{i=6}^{s} q_i^{c_i}\right) \text{-------(i)}$$

be the prime factorization of n. Here

a, b_i, c_i are non negative integers,

$p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$ for each i.

Then, n is a sum of squares of integers,

if, and only if c_i is even for each

$i=1,\ldots,s$.

<u>Proof:</u> (i) 'if' part: For $a,b,c,d \in \mathbb{Z}$,

$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad-bc)^2$.

Thus, the product of two numbers,

each of which is a sum of two squares,

each of which is a sum of 2 squares.

Since $2=1^2+1^2$, p is a sum of two squares of integers,

It follows that n is a sum of squares if each c_i is even.

(Since we can write $q_i^{c_i}$ as $(q_i^{c_i/2})^2+0$).

(ii) <u>'Only if' part</u> :

Assume that n= a^2+b^2 for some integers a and b.

If q is a prime dividing n and q $\equiv 3 \pmod 4$,

Then, by Theorem, q divides both a and b.

So, q^2 divides n. Now, we apply

induction to complete the proof of the fact that

each c_i is even.