THEORY OF NUMBERS
SUMS OF SQUARES

We wish to know which numbers are representable as sums of squares. For two squares

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$$

So the product of two numbers representable is also representable. We then ask what primes are representable.
Now the square of any even number is congruent to 0 (mod 4) and the square of any odd number is $\equiv 1$ (4). So the sum of two squares is congruent to 0 1 or 2 mod 4, so any number $4m + 3$ is not representable.

Theorem (Fermat) Every prime $p \equiv 1$ (4) is representable as the sum of two squares.

Proof 1 $\exists x_0$ such that $x_0^2 + 1 \equiv 0 \bmod p$. (-1) is a quadratic residue mod p therefore $mp = x^2 + y^2$ for some m $(x_0^2 + 1^2 - mp)$.

Let m be the least positive integer such that $mp = x^2 + y^2$. Then $1 \leq m \leq p$. R.T.P. $m = 1$

Assume $m > 1$, $\exists x_1,\ y_1$ such that $x \equiv x_1 \bmod m$ $y \equiv y_1 \bmod m$.

$|x_1| \leq \frac{1}{2}m$ $|y_1| \leq \frac{1}{2}m$
$x_1^2 + y_1^2 \equiv x^2 + y^2 = 0 \bmod m$ Therefore $lm = x_1^2 + y_1^2$ where l is an integer $l = 0 \Rightarrow x_1^2 = y_1^2 = 0 \Rightarrow x \equiv 0$ $y \equiv 0 \Rightarrow m|x$ $m|y \Rightarrow m|p$ therefore $1 \leq l < m$

For $lm \leq \left(\frac{1}{2}m\right)^2 + \left(\frac{1}{2}m\right)^2 = \frac{1}{2}m^2 < m^2$

Now $lpm^2 = (x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - x_1y)^2$

Now $xx_1 + yy_1 \equiv 0 \bmod m$ and $xy_1 - x_1y \equiv 0 \bmod m$ therefore $lp = u^2 + v^2$, v, v integers. This is a contradiction therefore $m = 1$.

Proof 2 $\exists\lambda$ such that $\lambda^2 + 1 \equiv 0 \bmod p$ S.T.P. $\exists(x, y) \neq (0, 0)$ such that $y \equiv \lambda x \bmod p$ $x^2 + y^2 < 2p$.

Lemma Suppose $\lambda \not\equiv 0 \bmod p$. Suppose $e,\ f$ are natural numbers such that $ef > p$ then $\exists$ a non-trivial solution $x,\ y$ of $y \equiv \lambda x \bmod p$ satisfying $|x| \leq e - 1$ $|y| \leq f - 1$.

Proof Consider the set S of $y - \lambda x$ as $x,\ y$ run through $0, 1, \ldots e-1;\ 0, 1, \ldots f-y$. The number of elements in s is $ef > p$ therefore $\exists$ $y' - \lambda x' \equiv y'' \lambda x''$

mod p such that $(x'-x'')^2+(y'-y'')^2 \neq 0$ Put $y = y'-y''$; $mx = x'-x'''$ then x and y are the required numbers.

Now apply the lemma with $e = f = [p^{\frac{1}{2}}]+1 > p^{\frac{1}{2}}$ then $ef > p$ and $(e-1)^2+(f-1)^2 = 2[p^{\frac{1}{2}}]^2 < 2p$.

Theorem A natural number n is representable as the sum of two squares $\Leftrightarrow$ every prime $q \equiv -1 \bmod 4$ which divides n divides it to an even power.

Proof S.C. obvious.

N.C. suppose $n = x^2+y^2$ and $q|n$ where $q = -1$ (4).

Suppose $q \not| x$
$x^2+y^2 \equiv 0 \bmod q$ and $\exists x_0$ such that $xx_0 \equiv 1 \bmod q$. Therefore $(x_0y)^2 \equiv -1 \bmod q$.

i.e. -1 is a quadratic residue mod q which is false therefore $q|x$ and $q|y$ therefore $q^2|n$ therefore $\frac{n}{q^2} = x_1^2+y_1^2$.

If $q|\frac{n}{q^2}$ we repeat the argument. We can only do so a finite number of times and so q divides n to an even power.

Considering sums of 4 squares we have the following identity

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\ &+ (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &+ (x_1y_3-x_3y_1-x_2y_4+x_4y_2)^2\\ &+ (x_1y_4-x_4y_1-x_3y_2+x_2y_3)^2\end{aligned}$$

From which it follows that the product of two representable numbers is representable.

Again if $x_i \equiv y_i \bmod m$, $i = 1,2,3,4$ and $\sum x_i^2 \equiv 0$ then each of the four expressions on the right hand sided is $\equiv 0 \bmod m$.

Theorem (Lagrange) Every natural number is representable as the sum of four squares.

Proof S.T.P. for primes by the above identity.

$2 = 1^2+1^2+0^2+0^2$
$p \equiv 1$ (4) $p^2 = x^2+y^2+0^2+0^2$

S.T.P. for $q \equiv -1$ (4)

$\exists$ an integer a such that $\left(\frac{a}{q}\right)\ \left(\frac{a+1}{q}\right) = -1$

Then since $q \equiv -1\ (4)$ we have $\left(\frac{-a-1}{q}\right) = -\left(\frac{-1}{q}\right) = +1$.

$\exists x_1$ such that $x_1^2 \equiv a\ (q)$ and $\exists x_2$ such that $x_2^2 \equiv -a-1\ (q)$.

Now $x_1^2 + x_2^2 + 1^2 + 0^2 \equiv 0 \bmod q$ so some non-zero multiple of q is representable.

Let m be the least positive integer such that $mq = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Then $1 \leq m < q$. Suppose that $m > 1$

We first prove that m is odd. Suppose that m is even. Then the number of odd x's is even, and suppose that they come first in the representation.

$$\left(\frac{1}{2}m\right)q = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

All the terms on the right hand side are integers so we have a contradiction, since $\left(\frac{1}{2}m\right)q$ is not representable.

Thus m is odd, and so for $i = 1, 2, 3, 4$ we choose y_i such that $x_i \equiv y_i\ (m)\ |y_i| < \frac{1}{2}m$ then

$lm = y_1^2 + y_2^2 + y_3^2 + y_4^2$ where $1 \leq l < m$

So $lm^2q = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = A^2 + B^2 + C^2 + D^2$ by the above identity.

$A,\ B,\ C,\ D$ are all divisible by m and so lq is representable. Thus we have a contradiction and so $m = 1$.

For 3 squares the result is $a^q(8t + 7)$ not representable, all others are.