The Bulletin of Society for Mathematical Services and Standards *Online: 2012-09-03*
ISSN: 2277-8020, Vol. 3, pp 67-72
doi:10.18052/www.scipress.com/BSMaSS.3.67

Primes of the form $x^2+ ny^2$

Prof. K. Raja Rama Gandhi
Department of Mathematics,BITS-Vizag
Email: rrmath28@gmail.com

Keywords: Fermat sum of two squares, quadratic reciprocity, Mersenne prime, ring of Gaussian integers, Lattice points.

Abstract. We know that, Fermat Showed a prime can be expressed as a sum of two squares if and only if it is a multiple of four plus one and its decomposition is unique. This paper will discuss the similar writings of primes as a sum of squares and multiple of another square.

1. Introduction

The reason for writing this paper is, I have seen the paper titled Primes of the form $a^2 + qb^2$ at arxiv math. This paper is published by Eugen J. Ionascu and Jeff Patterson [1] on 1 July 2012. After close look at the paper, I had some interest to develop the similar results, which is turned into the paper. Let us discuss the basic introduction.

In *1640*, Fermat [2] made a nice discovery and he realized that, $41 = 4^2 + 5^2$ as well $41 \equiv 1 \pmod{40}$. What the significance of this result? Well he was interested in which positive integers could be written as a sum of two integer squares. So far he had found that only the numbers *1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40 and 41* had this property. Out of these, Fermat noticed that the odd primes which can be written as the sum of two squares seem to be the primes which exceed a multiple of ***4*** *by* ***1***. Fermat was excited by this. He checked that the pattern held further and conjectured the following:

$$p = x^2 + y^2 \text{ if and only if } p \equiv 1 \pmod 4,$$

where p is an odd prime for *x, y* integers. In fact, this result lets us decide when any given integer can be written as a sum of squares or not by the following identity:

$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$, which says us the product of two numbers that are sum of squares is again a square in sums.

In later years Fermat found related results, claiming for $p > 3$:

$$p = x^2 + 2y^2 \text{ if and only if } p \equiv 1, 3 \pmod 8 \text{ or } p = 2$$
$$p = x^2 + 3y^2 \text{ if and only if } p \equiv 1 \pmod 3 \text{ or } p = 3$$

Unfortunately he was failed to provide proofs of any of his claims. Thereafter, it took to Euler [3] for about forty years to give complete proofs. This is outstanding, each of these results seems to classify the primes that can be written in the form $x^2 + 2y^2$ *or* $x^2 + 3y^2$ by one simple congruence condition on *p*.

One question arises in our mind that, given a positive integer n, can we find a corresponding congruence on the prime's p that can be written in the form $x^2 + ny^2$? Yes. This can be done by use of a more general identity than what we used earlier:

$$(a^2 + nb^2)(c^2 + nd^2) = (ac + nbd)^2 + n(ad - bc)^2$$

Returning to the problem, it seems that in all of the cases we have discussed, the primes p that could be written in the form $x^2 + ny^2$ were ones such that either p|n or $\left(\frac{-n}{p}\right) = 1$.

This is actually only true one way:

Theorem 1.1. $p = x^2 + ny^2 \Rightarrow p|n \left(\frac{-n}{p}\right) = 1.$

Let $p = x^2 + ny^2$, then $p = x^2 + ny^2 \equiv 0 \pmod p$. If x is not congruent 0 (mod p) then y is not congruent to 0 mod p and by rearranging, we see that $(xy^{-1})^2 \equiv -n(\text{mod } p) \Rightarrow \left(\frac{-n}{p}\right) = 1.$ If $x \equiv 0(\text{mod } p) \Rightarrow p \mid n.$

Of course the converse is not true in the case of n = 5. Now, by Quadratic reciprocity [5], $\left(\frac{-5}{p}\right) = 1$ for p ≡ 1, 3, 7, 9 mod 20, yet the primes 3 and 7 cannot be expressible in the form of $x^2 + 5y^2$. Finally, Euler conjectured:

$$p = x^2 + 5y^2 \Leftrightarrow p \equiv 1, 9 \text{ mod } 20 \text{ or } p = 5.$$

Now, this is the time to discuss some results by fixing n and leaving p, x and y values of the form $p = x^2 + ny^2$. Some of them are classical and some were found by investigation and trail-error methods.

Theorem1.2. For an odd prime *p*, if $p = x^2 + ny^2$ for any integers of *x* and *y*, the following are true.

(i) $p = x^2 + 6y^2$ if and only if $p \equiv 1, 7 \bmod 24$

(ii) $p = x^2 + 93y^2$ if and only if $p \equiv$ 1, 25, 49, 97, 109, 121, 133, 157, 169, 193, 205, 253, 289, 349, 361 mod 372.

(iii) $p = x^2 + 10y^2$ if and only if $p \equiv 1, 9, 11, 19 \bmod 40$

(iv) $p = x^2 + 13y^2$ if and only if $p \equiv 1, 9, 17, 25, 29, 49 \bmod 52$

(v) $p = x^2 + 14y^2$ if and only if $p \equiv$ 1, 9, 15, 23, 25, 39, mod 56

(vi) $3p = x^2 + 14y^2$ if and only if $p \equiv$ 3, 5, 13, 19,27, 45 mod 56 with $p \neq 3$

(vii) $p = x^2 + 15y^2$ if and only if $p \equiv 1, 19, 31, 49 \bmod 60$

(viii) $p = x^2 + 21y^2$ if and only if $p \equiv 1, 25, 37 \bmod 84$

(ix) $p = x^2 + 22y^2$ if and only if $p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \bmod 88$

(x) $p = x^2 + 30y^2$ if and only if $p \equiv 1, 31, 49, 79 \bmod 120$

(viii) $p = x^2 + 5y^2$ if and only if $p \equiv 1, 9 \bmod 20$

(ix) $2p = x^2 + 5y^2$ if and only if $p \equiv 3, 7 \bmod 20$

(x) $p = \begin{Bmatrix} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{Bmatrix}$ if and only if $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$

(xi) $3p = x^2 + 14y^2$ if and only if $p \equiv 3, 5, 13, 19, 27, 45 \bmod 56.$

Before proving those statements, let me discuss the Euler conjecture for odd prime's *p* and *q*. As a function of its denominator $\left(\frac{a}{p}\right)$ depends only on $\pm p(\text{mod } 4a)$.

Precisely, $\left(\frac{q}{p}\right) = 1 \Leftrightarrow p = \pm x^2 (\text{mod } 4q)$ for some x.

Of course, half the nonzero values mod *4q* take the form $\pm x^2$.

Thereafter, Legendre [4] is defined for distinct primes as below:

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\begin{cases}1\\-1\end{cases}$ if at least one of *p* and *q* is modulo *4* or if both *p* and *q* are *3* modulo *4*

2. Case (viii)

In this section, I will discuss (viii) of Theorem 1.2 ($p = x^2 + 5y^2$ if and only if $p \equiv 1, 9 \bmod 20$). Before that, let me discuss few theorems, which will conclude this section.

Theorem 2.1. *If p ≡ 1 (mod 4), then p can be written as sum of two squares.*

Proof: For expressing $p = x^2 + y^2$, write for any x and y integers, $p = (x + iy)(x - iy)$ for $p \equiv 1 \pmod 4$. We know that, ring of Gaussian integers [6] *Z[i]* is a principal ideal domain [9] and Euclidean domain as well. Now I claim that *p* is not prime in *Z[i]*. For determining the look of prime p of Z splits in *Z[i]* is same to determining the look of polynomial $x^2 + 1$splits modulo *p*. As $p \equiv 1 \pmod 4$ with *-1* as quadratic residue modulo *p* and then, there exist some $k \in Z$ such that $k^2 \equiv -1 \pmod p \Rightarrow x^2 + 1$ splits modulo *p,* and *p* not in *Z[i]*. Otherwise, if *p* in *Z[i],* we will have $p \mid (k + i)(k - i) \Rightarrow p \mid (k + i)$ or $p \mid (k - i)$. But, there is a non-unit $x + iy$ of *Z[i]* that properly divides *p*, which is nothing but norms will divide as well. In particular, $N(x + iy) = x^2 + y^2$ divides $p^2 \Rightarrow p$ or $1 \Rightarrow x^2 + y^2 = p$ for $p \equiv 1 \pmod 4$.

Theorem 2.2. *For $n \geq 1$, $p = x^2 + ny^2$, where p is some odd prime, then the following results are*

true (a) $\left(\frac{-n}{p}\right)=1$ *and* $\left(\frac{q}{p}\right)=1$ *for every odd prime* $q \mid n$

(b) $p \equiv 1 \pmod 4$ *for n = 0, 1(mod 4)*

(c) $p \equiv 1 \pmod 8$ *for* $8 \mid n$

Proof: If $\left(\frac{-n}{p}\right)=1 \Rightarrow -n \equiv x^2 \pmod p$ for some $x \in Z \Rightarrow p \mid x^2 + n = x^2 + 1.n$ and, if $p \mid x^2 + ny^2 \Rightarrow x^2 \equiv -ny^2 \pmod p$. If $y \equiv 0 \pmod p \Rightarrow x \equiv 0 \pmod p$ & $(x, y) \neq 1 \Rightarrow y \neq 0 \pmod p$ as *y* is invertible and

$\left(\frac{x}{y}\right)^2 \equiv -n \pmod p \Rightarrow \left(\frac{-n}{p}\right)=1.$

Now, for concerning *(b)* and *(c),* take a close look at the groups *Z/4Z* and *Z/8Z* and then square each element, and check the possible values of it. We can easily see that fact for odd prime *p*, the results *(b)* and *(c)* are obvious. More precisely, in the case of
(b), we know that, Z/4Z has

$$0^2 = 2^2 = 0$$
$$1^2 = 3^2 = 1$$

i.e., an even square is zero and Odd Square is one. So, for $n \equiv 0 \pmod 4 \Rightarrow ny^2 \equiv 0 \pmod 4$ for a particular ny^2 is even. As p is odd, x^2 should be odd $\Rightarrow x^2 \equiv 1$. Hence

$$\begin{aligned} p &= x^2 + ny^2 \\ &\equiv 1 + 0 \\ &\equiv 1 \end{aligned}$$

If $n \equiv 1 \pmod 4 \Rightarrow p = x^2 + y^2$. The sum of two odd numbers or two even numbers is even, since p is odd we know that, both x is odd and y is even otherwise the other way around. In all the cases, we can found that, by the inspection of squares in Z/4Z above that, $p \equiv 1 + 0 \equiv 1$ as desired.

Observe that strictly speaking I was working on modulo 2 most of the time in the last argument. Formally I could have argued that $n \equiv 1 \pmod 4 \Rightarrow n \equiv 1 \pmod 2$ and hence $p = x^2 + y^2 \pmod 2$, from which the statement of the parity of x and y follows. Then, we return to working modulo 4 again: the value of a number modulo 2 is of course not enough to determine its value modulo 4, but as we saw above, we are able to find the value of the *square* of the number modulo 4, just by knowing its value modulo 2. Since we are only interested in the values of the squares, this suffices.

For (c), we determine the squares in Z/8Z. Observe that, $5 \equiv -3 \Rightarrow 5^2 \equiv 3^2$ and similarly $7^2 \equiv (-1)^2 \equiv 1^2$, we can quickly see that all odd numbers square to one (In fact this shows that $Z/8Z^*$ is the Klein four group [11]). Now $8|n$ is a reformulation of $n \equiv 0 \pmod 8$, which certainly implies ny^2 is even, and again since p is odd we know x^2 and hence x must be odd. Putting this together we see

$$\begin{aligned} p &= x^2 + ny^2 \\ &\equiv 1 + 0 = 1 \end{aligned}$$

Modulo 8 of course, as desired. Wherever we leave out the (mod ...) notation I assume it to be clear modulo which number we work.

Remark: Theorem 2.2 is true for $n > 1$, for $t = t_n$ congruence classes $c_1, \ldots, c_t \pmod{N_n}$ have the property for an odd prime p satisfies $p = p_1, \ldots, p_t \pmod{N_n}$.

Proof of theorem 1.2 (viii).

We have seen the theorems **2.1** and **2.2**. From these theorems, we see that, $\left(\frac{p}{5}\right) = 1$ and $p \equiv 1 \pmod t \Rightarrow p \equiv 1,9 \bmod(20)$. again, by these theorems, we have, $\left(\frac{-5}{p}\right) = 1$ and there exist some integer k such that $k^2 \equiv -5 \pmod p$. Now, by taking the Lattice [7] $L \subset R^2$ and define

$$L = \{(x, y) \in Z^2 \mid x \equiv ky \pmod p\}$$

Where L is generated by the vertices $M = (p, 0)$ & $N = (u, 1)$ and has index $\begin{vmatrix} p & 0 \\ u & 1 \end{vmatrix} = p$ in Z^2.

Finally, consider region R is the area of an ellipse $x^2 + 5y^2 = s$ and area of region R is $\frac{\pi k}{\sqrt{5}} > 1.4s$.

Now by taking $s = 2.84p$, then the area $R > 4p$ and $R \cap L$ contains a non-zero point (x, y).

$$\begin{aligned} i.e., x^2 + 5y^2 &\equiv (uy)^2 + 5y^2 \\ &\equiv -5y^2 + 5y^2 \\ &= 0 \pmod p \\ &\Rightarrow p \mid x^2 + 5y^2. \end{aligned}$$

3. Case (vi)

In this section, I will discuss the case (vi) of theorem 1.2. i.e., $3p = x^2 + 14y^2$ if and only if $p \equiv 3$, 5, 13, 19, 27, 45 mod 56, where p > 3.

Proof of theorem 1.2 (vi).

If we assume p ≠ 3 (even ≠2 and 7), then any solution of form $(x, y) = 1 \Rightarrow \left(\frac{-14}{p}\right) = \left(\frac{3p}{7}\right) = 1.$

The quadratic reciprocity gives us $p \equiv 3,5 (\mathrm{mod}\, 8)$ and $p \equiv 3,5,6 (\mathrm{mod}\, 7) \Rightarrow \left(\frac{-14}{p}\right) = 1 \Rightarrow \exists$

Solution (x, y) with $dp = x^2 + 14y^2$ for some d = 1, 2, 3, 4. For d = 1, 2 and 4 $\Rightarrow x^2 \equiv dp (\mathrm{mod}\, 7)$.

Also, $\left(\frac{p}{7}\right) = 1$ which contradicts the congruence conditions on p $\Rightarrow 3p = x^2 + 14y^2$.

Theorem 2.3. For an odd prime $p > 17,\ p = x^2 + 17y^2 \Leftrightarrow \left\{\frac{-17}{p} = 1 \,\&\, x^4 - x^2 \equiv 4 (\mathrm{mod}\, p)\right.$ has an integer solution. I am leaving the proof for the readers and researchers.

4. In the case of Mersenne Prime (Mp)

In this section, I would like to discuss the conjecture and an interesting theorem of the form $p = x^2 + ny^2$. However, I will take M_p in the place of p. Okay! Let me state the conjecture.

Conjecture 4.1. *Every Mersenne Prime number [8] (M_p) can be expressible in the form of $x^2 + 3y^2$ for (x, y) =1 with x, y ≥ 0.*

Mersenne prime *(M_p)* is an odd prime $\Rightarrow M_p \equiv 1 \ (mod\ 2)$. By Fermat little theorem [10], we see that, $2^p \equiv 2 \ (mod\ p) \Rightarrow 2^p - 1 \equiv 1 \ (mod\ p) \Rightarrow M_p \equiv 1 (mod\ p)$. Also, $2 \equiv -1 (mod\ 3) \Rightarrow 2^p \equiv (-1)^p \ (mod\ 3) \Rightarrow 2^p - 1 \equiv -2 \ (mod\ 3) \Rightarrow M_p \equiv 1 \ (mod\ 3)$. i.e., we have $M_p \equiv 1 \ (mod\ 2)$, $M_p \equiv 1 \ (mod\ 3)$ and $M_p \equiv 1 \ (mod\ p)$ as equivalence classes. So, for $p > 3$, we can found that $M_p \equiv 1 \ (mod\ 6p)$. Now, for $x^2 + 3y^2$ is prime with $(x, y) = 1$ and $x, y \geq 0 \Rightarrow x^2 + 3y^2 > 5 \Rightarrow x^2 + 3y^2 \equiv 1 \ (mod\ 6)$.

Theorem 4.1. *If $x^2 + 3y^2 > p$ $(p > 5) \Rightarrow x^2 + 3y^2 \equiv 1 \ (mod\ 6)$.*

Proof: We know that $x^2 + 3y^2 = p > 3$ will be in the form of either $6k + 1$ or $6k - 1$. *If* $x^2 + 3y^2$ is in the form of $6k - 1 \Rightarrow x^2 + 3y^2 + 1 = 6k \Rightarrow 6|(x^2 + 3y^2 + 1) \Rightarrow 6|\ x^2 + 1$ and $6|3y^2$. *If* $6|x^2 + 1 \Rightarrow 2|x^2 + 1$ as well as $3|x^2 + 1$. But, $x^2 \neq -1 \ (mod\ 3) \Rightarrow 3$ does not divides $x^2 + 1 \Rightarrow 6$ does not divides $x^2 + 1 \Rightarrow 6$ does not divides $x^2 + 3y^2 + 1$. Obviously, $x^2 + 3y^2$ should be in the form of $6k + 1$. Therefore, $x^2 + 3y^2 \equiv 1 \ (mod\ 6)$.

Theorem 4.2. *If $p \equiv 1 \ (mod\ 6) \exists$ only one positive solution of $x^2 + 3y^2 = p$.*

Proof: Consider the Gaussian integers for $p \equiv 1 \ (mod\ 4)$, then $x^2 + y^2 = p$ has an integer solution. Here we can observe that, there is some a such that $a^2 + 1$ is divisible by p. By quadratic

reciprocity, we know that $p \equiv 1 \pmod 6$ is a prime iff $a^2 \equiv -3 \pmod p$ has a solution. i.e., $p|a^2 + 3$. By unique factorization on $Z[\sqrt{-3}]$, we will have a common prime factor p and $a + \sqrt{-3}$, which will have norm p. Since we do not have unique factorization on $Z[\sqrt{-3}]$, we consider the ring R of algebraic integer in $Q[\sqrt{-3}]$ of the form $\frac{a+b\sqrt{-3}}{2}$ with $a \equiv b \pmod 2$ This will happen as any element $r \in R$ there exist some unit $u \in R$ with an element $z \in Z[\sqrt{-3}]$ such that $r = uz$. Also, for any $r \in R$, the norm $N(r) = z_1^2 + 3z_2^2$ for some integers $z_1, z_2 \in Z$.

Acknowledgement

I am heartily thankful to Mathematician Prof. J. Gopala Krishna and my well-wishers Dr. C.V. Gopinath, Sri N. Nanda Kumar and external supporters *Thomas Andrews, Georg Joachim* whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

References

[1] http://arxiv.org/pdf/1207.0172v1.pdf

[2] http://en.wikipedia.org/wiki/Fermat%27s_theorem_on_sums_of_two_squares

[3] C. Edward Sandifer, *"How Euler did it"* The Mathematical Association of America, 2007.

[4] Hans Riesel, *"Prime Numbers and Computer Methods for Factorization"* Birkhauser, second edition, Springer Sciences + Business media. Sweden.

[5] Franz Lemmermeyer, *"Reciprocity Laws: From Euler to Eisenstein"* Springer Verlag.

[6] Richard Dedekind, *"Theory of Algebraic Integers"* Cambridge Mathematical Library, 1996.

[7] Sergiu Rudeanu, *"Lattice Functions and Equations"* Springer Verlag, 2001.

[8] Martin Aigner, Günter M. Ziegler, "Proofs from The Book" Springer Verlag.

[9] Bhubaneswar Mishra, "Algorithmic Algebra" Springer Verlag, New York, 1993.

[10] James J. Tattersall, *"Elementary Number Theory in Nine Chapters"* Second edition, CUP.

[11] M.R. Adhikari, A. Adhikari, "Groups, Rings And Modules With Applications" University Press (India) Limited, 2003.