Pythagorean Triples, Sum of Squares, and Fermat's Last Theorem Proofs

Karim El Shenawy

March 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 8 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Theorems to Mark

8.4 Theorem

In any primitive Pythagorean triple, one leg is odd, one leg is even, and the hypotenuse is odd.

Proof. Let (a,b,c) is a Pythagorean triple where a is one leg, b is another leg and c is the hypotenuse. We know by Theorem 8.1 that at least one of a or b is even. Now we must prove if one leg is odd while the other is even.

- Case 1: Both a and b are even, then $a \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 2$. This also means that $2 \mid a \implies 2 \mid a^2$ and $2 \mid b \implies 2 \mid b^2$. By Theorem 1.1, $2 \mid (a^2 + b^2))$ and thus by definition of Pythagorean triple,$2 \mid c^2$. This implies that c is also even and that $gcd(a, b, c) = 2$ which contradicts the definition of Pythagorean triple where (a,b,c) must have no common factor. Thus a and b can no both be even.

- Case 2: Both a and b are odd, then $a \equiv a^2 \equiv 1 \pmod 2$ and $b \equiv b^2 \equiv 1 \pmod 2$. By definition of Pythagorean triple, $a^2 + b^2 \equiv c^2 \equiv 2 \pmod 4$. This contradicts that the square of any integer is congruent to 0 or 1 modulo 4. Thus, a and b can not both be odd.

Now suppose a is even and b is odd. Then $a \equiv a^2 \equiv 0 \pmod 2$ and $b \equiv b^2 \equiv 1 \pmod 2$. Thus $a^2 + b^2 = 1 = c$, therefore c is odd while one leg is odd and one leg is even. □

8.5 Theorem

Let s and t be any two different natural numbers with $s > t$. Then

$$(2st, (s^2 - t^2), (s^2 + t^2))$$

is a Pythagorean triple.

Proof. Let s and t be any two different natural numbers with $s > t$ and $(2st, (s^2 - t^2), (s^2 + t^2))$. Suppose that $a = 2st$, $b = (s^2 - t^2)$ and $c = (s^2 + t^2)$ where (a,b,c) is a Pythagorean triple. Now by direct proof,

$$\begin{aligned} a^2 + b^2 &= c^2 \\ (2st)^2 + (s^2 - t^2)^2 &= (s^2 + t^2)^2 \\ 4s^2t^2 + s^4 - 2s^2t^2 + t^4 &= (s^2 + t^2)^2 \\ 4s^2t^2 + s^4 - 2s^2t^2 + t^4 &= s^4 + 2s^4t^2 + t^4 \\ s^4 + 2s^2t^2 + t^4 &= s^4 + 2s^4t^2 + t^4 \end{aligned}$$

Therefore, $(2st, (s^2 - t^2), (s^2 + t^2))$ is a Pythagorean triple. □

8.14 Theorem

Let p be a prime such that $p = a^2 + b^2$ for some natural numbers a and b. Then either $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. Since all perfect squares are congruent to 0 or 1 modulo 4, the sum of two square can only be congruent to 0, 1, or 2 modulo 4. The integer 2 is the only even prime, and therefore any odd prime that is a sum of two squares must be congruent to 1 modulo 4.

Let p be a prime such that $p = a^2 + b^2$ for some natural numbers a and b. Now suppose $x \pmod 4, \exists x \in \mathbf{Z}_{\{0,1,2,3\}}$, then $x^2 \pmod 4, \exists x \in \mathbf{Z}_{\{0,1\}}$. This allows us to create 4 cases:

- Case 1: $a^2 \equiv 0 \pmod 4$, $b^2 \equiv 0 \pmod 4$ then $p \equiv 0 \pmod 4$
- Case 2: $a^2 \equiv 0 \pmod 4$, $b^2 \equiv 1 \pmod 4$ then $p \equiv 1 \pmod 4$
- Case 3: $a^2 \equiv 1 \pmod 4$, $b^2 \equiv 0 \pmod 4$ then $p \equiv 1 \pmod 4$, by contradiction, p is not prime, thus by $a \neq 0$ and $b \neq 0$.
- Case 4: $a^2 \equiv 1 \pmod 4$, $b^2 \equiv 1 \pmod 4$ then $p \equiv 2 \pmod 4$

Thus, $p = 2$ or $p \equiv 1 \pmod 4$. □

8.16 Theorem

Let p be a prime such that $p \equiv 1 \pmod 4$. Then p is equal to the sum of two squares of natural numbers.
Hint: Try applying the previous lemma to a square root of -1 modulo p.

Proof. Let p be a prime such that $p \equiv 1 \pmod 4$. Then $p = 4k+1 \Longrightarrow p-1 = 4k$. We first must attempt to prove that $\exists a$ such that $a^2+1 \equiv 0 \pmod p$. Now let $b \in \mathbf{N}$ such that $(b,p) = 1$. Then by Fermat's Little Theorem,

$$\begin{aligned} b^{p-1} &\equiv 1 \pmod p \\ b^{4k} &\equiv 1 \pmod p \\ b^{4k} - 1 &\equiv 0 \pmod p \\ b^{2k\cdot 2} - 1^2 &\equiv 0 \pmod p \\ (b^{2k}-1)(b^{2k}+1) &\equiv 0 \pmod p \\ &\Longrightarrow p \mid (b^{2k}-1)(b^{2k}+1) \end{aligned}$$

Then if $p \mid (b^{2k}-1) \Longrightarrow (b^{2k}-1) \equiv 0 \pmod p \Longrightarrow b^{2k} \equiv 1 \pmod p$. However by Fermat's Little Theorem, $ord_p(b) = p-1 = 4k$ then

$$\begin{aligned} 4k &\mid 2k \\ 4 &\mid 2 \qquad \textbf{Which is a contradiction} \end{aligned}$$

Thus $p \nmid (b^{2k}-1)$ and $p \mid (b^{2k}+1) \Longrightarrow b^{2k}+1 \equiv 0 \pmod p$. Now let $a = b^k$ then $a^2+1 \equiv 0 \pmod p$ and $gcd(a,p) = 1$.
With Lemma 8.15, then there exist integers x and y such that $ax \equiv y \pmod p$ with $0 < |x|, |y| < \sqrt{p}$. Therefore,

$$\begin{aligned} a^2+1 &\equiv 0 \pmod p \\ x^2(a^2+1) &\equiv 0 \pmod p && \textbf{Multiply } x^2 \\ x^2a^2 + x^2 &\equiv 0 \pmod p \\ y^2 + x^2 &\equiv 0 \pmod p && y^2 = x^2a^2 \\ &\Longrightarrow p \mid x^2+y^2 \\ &\Longrightarrow kp = x^2+y^2 && \exists k \in \mathbf{Z} \\ &\Longrightarrow 2p > x^2+y^2 && 0 < |x|, |y| < \sqrt{p} \end{aligned}$$

Then $0 < kp = x^2+y^2 < 2p \Longrightarrow 0 < 2k < 2p \Longrightarrow 0 < k < 2 \Longrightarrow k = 1$. Therefore, $p = x^2+y^2$ when $p \equiv 1 \pmod 4$. □

8.18 Theorem

If an integer x can be written as the sum of two squares of natural numbers and an integer y can be written as the sum of two squares of natural numbers, then xy can be written as the sum of two squares of natural numbers.

Proof. Given that integers x and y can be expressed as the sum of two squares of natural number such that $x = a^2 + b^2$ and $y = c^2 + d^2$. Now suppose $x \cdot y$ then by direct proof,

$$\begin{aligned}
x \cdot y &= (a^2 + b^2) \cdot (c^2 + d^2) \\
x \cdot y &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + 0 \\
x \cdot y &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + (2abcd - 2abcd) \\
x \cdot y &= a^2c^2 + b^2d^2 + 2abcd - 2abcd + b^2c^2 + a^2d^2 \\
x \cdot y &= (ac + bd)^2 + (bc - ad)^2
\end{aligned}$$

Thus, xy can be expressed as the sum of two squares of natural numbers. □

8.22 Theorem

If (a,b,c) is a primitive Pythagorean triple, then c is a product of primes each of which is congruent to 1 modulo 4.

Proof. Let (a,b,c) be a primitive Pythagorean triple then we can suppose that $a = 2st, b = s^2 - t^2$ and $c = s^2 + t^2$ where c is odd. Now, let p be 3 congruent to modulo 4 such that $p \equiv 3 \pmod 4$ and also that $p \mid c$ but $p \nmid s$ and evidently $p \nmid t$. This implies that,

$$\begin{aligned}
c &\equiv 0 \pmod p \\
s^2 + t^2 &\equiv 0 \pmod p \\
s^2 &\equiv -t^2 \pmod p \\
s^2 \cdot t^{-2} &\equiv -1 \pmod p \\
(st^{-1})^2 &\equiv -1 \pmod p
\end{aligned}$$

Thus $(st^{-1})^2 \equiv -1 \pmod p$ suggests a contradiction since -1 is not a quadratic residue. Hence, if $k \mid s$ and $k \mid t$ then (a,b,c) is not a primitive Pythagorean triple. So there is no solution if $p \equiv 3 \pmod 4$. Therefore, $p \equiv 1 \pmod 4$ where $p \mid c$ which implies that c is a product of primes each of which is congruent to 1 modulo 4. □

Practice Theorems from Pythagorean Triples, Sum of Squares, and Fermat's Last Theorem

8.1 Theorem

If (a,b,c) is a Pythagorean triple, then at least one of a or b is even.

Proof. Let (a,b,c) is a Pythagorean triples. Suppose, by contradiction, a and b is odd then $a = 2k_1 + 1$and $b = 2k_2 + 1$ where $k_1, k_2 \in \mathbf{Z}$. Moreover,

$$a^2 \equiv (2k_1+1)^2 \equiv 4k_1^2 + 4k_1 + 1 \equiv 1 \pmod 4$$
$$b^2 \equiv (2k_2+1)^2 \equiv 4k_2^2 + 4k_2 + 1 \equiv 1 \pmod 4$$

Thus,

$a^2 + b^2 \equiv 1 + 1 \equiv 2 \equiv c \pmod 4$, since (a,b,c) is a Pythagorean triple.

This contradicts to square of any integer is either congruent to 0 or 1 modulo 4. Therefore a and b can not be both odd and thus one of them must be even. □

8.2 Exercise

Find at least seven different Pythagorean triples. Make a note of your methods.

Solution.

1. (3,4,5), multiples of (3,4,5) below
2. (6,8,10)
3. (9,12,15)
4. (12,16,20)
5. (5,12,13), multiples of (5,12,13) below
6. (10,24,26)
7. (15,36,39)

8.3 Exercise

Find at least five primitive Pythagorean triples.

1. (3,4,5)
2. (7,24,25)
3. (5,12,13)
4. (8,15,17)
5. (20,21,29)
6. (12,35,37)

8.4 Theorem

In any primitive Pythagorean triple, one leg is odd, one leg is even, and the hypotenuse is odd.

Proof. Let (a,b,c) is a Pythagorean triple where a is one leg, b is another leg and c is the hypotenuse. We know by Theorem 8.1 that at least one of a or b is even. Now we must prove if one leg is odd while the other is even.

- Case 1: Both a and b are even, then $a \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 2$. This also means that $2 \mid a \implies 2 \mid a^2$ and $2 \mid b \implies 2 \mid b^2$. By Theorem 1.1, $2 \mid (a^2 + b^2))$ and thus by definition of Pythagorean triple,$2 \mid c^2$. This implies that c is also even and that $gcd(a, b, c) = 2$ which contradicts the definition of Pythagorean triple where (a,b,c) must have no common factor. Thus a and b can no both be even.
- Case 2: Both a and b are odd, then $a \equiv a^2 \equiv 1 \pmod 2$ and $b \equiv b^2 \equiv 1 \pmod 2$. By definition of Pythagorean triple, $a^2 + b^2 \equiv c^2 \equiv 2 \pmod 4$. This contradicts that the square of any integer is congruent to 0 or 1 modulo 4. Thus, a and b can not both be odd.

Now suppose a is even and b is odd. Then $a \equiv a^2 \equiv 0 \pmod 2$ and $b \equiv b^2 \equiv 1 \pmod 2$. Thus $a^2 + b^2 = 1 = c$, therefore c is odd while one leg is odd and one leg is even. □

8.5 Theorem

Let s and t be any two different natural numbers with $s > t$. Then

$$(2st, (s^2 - t^2), (s^2 + t^2))$$

is a Pythagorean triple.

Proof. Let s and t be any two different natural numbers with $s > t$ and $(2st, (s^2 - t^2), (s^2 + t^2))$. Suppose that $a = 2st$, $b = (s^2 - t^2)$ and $c = (s^2 + t^2)$ where (a,b,c) is a Pythagorean triple. Now by direct proof,

$$\begin{aligned} a^2 + b^2 &= c^2 \\ (2st)^2 + (s^2 - t^2)^2 &= (s^2 + t^2)^2 \\ 4s^2t^2 + s^4 - 2s^2t^2 + t^4 &= (s^2 + t^2)^2 \\ 4s^2t^2 + s^4 - 2s^2t^2 + t^4 &= s^4 + 2s^4t^2 + t^4 \\ s^4 + 2s^2t^2 + t^4 &= s^4 + 2s^4t^2 + t^4 \end{aligned}$$

Therefore, $(2st, (s^2 - t^2), (s^2 + t^2))$ is a Pythagorean triple. □

8.6 Lemma

Let (a,b,c) be a primitive Pythagorean triple where a is the even number. Then $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are perfect squares, say, s^2 and t^2, respectively; and s and t are relatively prime.

Proof. Let (a,b,c) be a primitive Pythagorean triple where a is the even number. Then $a^2 + b^2 = c^2 \Longrightarrow a^2 = b^2 - c^2 = (c+b)(c-b)$. Now, let s and t be any two different natural numbers with $s > t$ and $(2st, (s^2 - t^2), (s^2 + t^2))$ where $a = 2st$, $b = (s^2 - t^2)$ and $c = (s^2 + t^2)$. This implies that

$$a^2 = b^2 - c^2 = (c+b)(c-b)$$
$$(\tfrac{a}{2})^2 = \tfrac{b}{2}^2 - \tfrac{c}{2}^2 = (\tfrac{c+b}{2})(\tfrac{c-b}{2})$$

Therefore, s must be odd and t must be even which implies that they are both relatively prime □

8.7 Theorem (Pythagorean Triple Theorem)

Let (a,b,c) be a primitive Pythagorean triple with a even, b odd, and c odd. Then (a,b,c) is a primitive Pythagorean triple if and only if there exists relatively prime positive integers s and t, one even and one odd, such that $a = 2st$, $b = (s^2 - t^2)$, and $c = (s^2 + t^2)$.

Proof. Let (a,b,c) be a primitive Pythagorean triple with a even, b odd, and c odd. Then

$$a^2 = b^2 - c^2 = (c+b)(c-b)$$
$$(\tfrac{a}{2})^2 = \tfrac{b}{2}^2 - \tfrac{c}{2}^2 = (\tfrac{c+b}{2})(\tfrac{c-b}{2}).$$

Since any common divisor of $\frac{c+b}{2}$ and $\frac{c-b}{2}$ also divides $\frac{c+b}{2} + \frac{c-b}{2} = c$ and $\frac{c+b}{2} - \frac{c-b}{2} = b$, and b and c are relatively prime, then $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are also relatively prime. Since $(\frac{a}{2})^2$ is a perfect square, any prime that divides $(\frac{a}{2})^2$ must occur in its prime factorization to an even power. Since $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are also relatively prime, any prime that divides $(\frac{a}{2})^2$ appears in the factorization of exactly one of $\frac{c+b}{2}$ or $\frac{c-b}{2}$, and therefore each of these is a perfect square, say, s^2 and t^2, respectively; and s and t are relatively prime. Then,

$$a2\sqrt{\frac{c^2 - b^2}{4}} = 2\sqrt{s^2t^2} = 2st$$
$$b\frac{c^2 + b^2}{2} - \frac{c^2 - b^2}{2} = s^2 - t^2$$
$$b\frac{c^2 + b^2}{2} + \frac{c^2 - b^2}{2} = s^2 + t^2$$

Since b and c are odd, either s or t (but not both) mus be even. By Theorem 8.5, we know that $(2st, (s^2 - t^2), (s^2 + t^2))$ is Pythagorean triple. Moreover, since s and t have opposite parity, b and c are odd, so 2 is a divisor of only a.

if an odd prime p divides any two of a, b, or c, then it divides the third, so it divides $b + c = 2s^2$ and $b - c = 2t^2$, so it divides both s and t, which cannot happen since s and t are relatively prime. Therefore, a, b and c is a primitive Pythagorean triple. □

8.8 Exercise

Using the above formula make a lengthy list of primitive Pythagorean triples.

- (3,4,5)
- (5,12,13)
- (8,15,17)
- (7,24,25)
- (20,21,29)
- (12,35,37)
- (9,40,41)
- (28,45,53)

8.9 Exercise

Make a conjecture that describes those natural numbers that can appear as legs in a primitive Pythagorean triple.

Conjecture. *Couldn't form one.*

8.10 Theorem

In every primitive Pythagorean triple, one leg is an odd integer greater than 1 and the other is a positive multiple of 4.

Proof. Let s and t be any two different natural numbers with $s > t$ and $(2st, (s^2 - t^2), (s^2 + t^2))$. Suppose that $a = 2st$, $b = (s^2 - t^2)$ and $c = (s^2 + t^2)$ where (a,b,c) is a Pythagorean triple. By Pythagorean triple Theorem, suppose s is even. Then $a = 2st$ is a multiple of 4. This implies that the only perfect square that differ by 1 are 0 and 1, and neither s nor t can be zero. Thus $b = s^2 - t^2$ is an odd integer larger than 1. □

8.11 Theorem

Any odd number greater than 1 can occur as a leg in a primitive Pythagorean triple.

Proof. Let s and t be any two different natural numbers with $s > t$ and $(2st, (s^2 - t^2), (s^2 + t^2))$. Suppose that $a = 2st$, $b = (s^2 - t^2)$ and $c = (s^2 + t^2)$ where (a,b,c) is a Pythagorean triple. First, we need to show that an odd leg will appear by showing that $s^2 = t^2$ can represent any odd number with suitable choices of s and t. Now, let $2x + 1$ be the odd number. Now, if $s = x$ and $t = x - 1$, then $b = s^2 - t^2 = x^2 - (x-1)^2 = 2x - 1$, thus b is odd. Now let given odd number be y, $y = 2x - 1$. Therefore, $x = \frac{y+1}{2}$, $s = \frac{y+1}{2}$ and $t = \frac{y-1}{2}$.
Now, the Pythagorean triple with the odd number is $(a, b, c) = (2st, (s^2 - t^2), (s^2 + t^2)) = (\frac{y^2-1}{2}, y, \frac{y^2+1}{2})$. This implies that we can create a Pythagorean triple with any odd number. Thus, any odd number $y > 1$ can be in leg since if $y = 1$ then (0, 1, 1). Thus we cannot have a side of a triangle with 0, thus y must be greater than 1. □

8.12 Theorem

Any positive multiple of 4 can occur as a leg in a primitive Pythagorean triple.

Proof. Let $4k, k \in \mathbf{Z}_+$ be positive multiples of 4. Now suppose (a,b,c) is a Pythagorean triples where $a = 2st, b = (s^2 - t^2), c = (s^2 + t^2)$ and $s = 2k, t = 1$. Then by direct proof,

$$\begin{aligned}
a^2 + b^2 &= c^2 \\
(2st)^2 + (s^2 - t^2)^2 &= (s^2 + t^2)^2 \\
4s^2t^2 + (s^2 - t^2)^2 &= (s^2 + t^2)^2 \\
4(4k^2) + (4k^2 - 1)^2 &= (4k^2 + 1)^2 \\
16k^2 + (4k^2 - 1)^2 &= (4k^2 + 1)^2 \\
(4k)^2 + (4k^2 - 1)^2 &= (4k^2 + 1)^2
\end{aligned}$$

Thus, $a = 4k, b = 4k^2 - 1$ and $c = 4k^2 + 1$ and all are relatively prime. Therefore, $4k$ can occur as a leg in a primitive Pythagorean triple. □

8.13 Question

Make a list of the first fifteen primes and write each as the sum of as few squares of natural numbers as possible. Which ones can be written as the sum of two squares? Make conjecture about which primes can be written as the sum of two squares of natural numbers.

1. $2 = 1^2 + 1^2$

2. $3 =$

3. $5 = 1^2 + 2^2$
4. 7
5. 11
6. $13 = 2^2 + 3^2$
7. $17 = 4^2 + 1^2$
8. 19
9. 23
10. $29 = 5^2 + 2^2$
11. 31
12. $37 = 6^2 + 1^2$
13. $41 = 4^2 + 5^2$
14. 43
15. 47

The numbers that can be written as sum of square are $\{2, 5, 13, 17, 29, 37, 41\}$.
Conjecture. *For a prime to be expressed on the sum of 2 squares. Then it must be either 2 or 1 modulo 4.*

8.14 Theorem

Let p be a prime such that $p = a^2 + b^2$ for some natural numbers a and b. Then either $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. Since all perfect squares are congruent to 0 or 1 modulo 4, the sum of two square can only be congruent to 0, 1, or 2 modulo 4. The integer 2 is the only even prime, and therefore any odd prime that is a sum of two squares must be congruent to 1 modulo 4.

Let p be a prime such that $p = a^2 + b^2$ for some natural numbers a and b. Now suppose $x \pmod 4), \exists x \in \mathbf{Z}_{\{0,1,2,3\}}$, then $x^2 \pmod 4), \exists x \in \mathbf{Z}_{\{0,1\}}$. This allows us to create 4 cases:

- Case 1: $a^2 \equiv 0 \pmod 4$, $b^2 \equiv 0 \pmod 4$ then $p \equiv 0 \pmod 4$
- Case 2: $a^2 \equiv 0 \pmod 4$, $b^2 \equiv 1 \pmod 4$ then $p \equiv 1 \pmod 4$
- Case 3: $a^2 \equiv 1 \pmod 4$, $b^2 \equiv 0 \pmod 4$ then $p \equiv 1 \pmod 4$, by contradiction, p is not prime, thus by $a \neq 0$ and $b \neq 0$.
- Case 4: $a^2 \equiv 1 \pmod 4$, $b^2 \equiv 1 \pmod 4$ then $p \equiv 2 \pmod 4$

Thus, $p = 2$ or $p \equiv 1 \pmod 4$. □

8.15 Lemma

Let p be a prime and let a be natural number not divisible by p. Then there exist integers x and y such that $ax \equiv y \pmod{p}$ *with* $0 < |x|, |y| < \sqrt{p}$.

Proof. Let p be a prime and let a be natural number not divisible by p. Then $gcd(a,p) = 1 \implies ax + py = 1, \exists x, y \in \mathbf{Z}$. Thus $ax \equiv y \pmod{p}$ with $0 < |x|, |y| < \sqrt{p}$. □

8.16 Theorem

Let p be a prime such that $p \equiv 1 \pmod{4}$. *Then p is equal to the sum of two squares of natural numbers.*
Hint: Try applying the previous lemma to a square root of -1 *modulo p.*

Proof. Let p be a prime such that $p \equiv 1\ (\bmod\ 4)$. Then $p = 4k+1 \implies p-1 = 4k$. We first must attempt to prove that $\exists a$ such that $a^2+1 \equiv 0\ (\bmod\ p)$. Now let $b \in \mathbf{N}$ such that $(b,p) = 1$. Then by Fermat's Little Theorem,

$$\begin{aligned} b^{p-1} &\equiv 1 \pmod{p} \\ b^{4k} &\equiv 1 \pmod{p} \\ b^{4k} - 1 &\equiv 0 \pmod{p} \\ b^{2k\cdot 2} - 1^2 &\equiv 0 \pmod{p} \\ (b^{2k}-1)(b^{2k}+1) &\equiv 0 \pmod{p} \\ &\implies p \mid (b^{2k}-1)(b^{2k}+1) \end{aligned}$$

Then if $p \mid (b^{2k}-1) \implies (b^{2k}-1) \equiv 0 \pmod{p} \implies b^{2k} \equiv 1 \pmod{p}$. However by Fermat's Little Theorem, $ord_p(b) = p - 1 = 4k$ then

$$\begin{aligned} 4k &\mid 2k \\ 4 &\mid 2 \qquad \qquad \textbf{Which is a contradiction} \end{aligned}$$

Thus $p \nmid (b^{2k}-1)$ and $p \mid (b^{2k}+1) \implies b^{2k}+1 \equiv 0 \pmod{p}$. Now let $a = b^k$ then $a^2+1 \equiv 0 \pmod{p}$ and $gcd(a,p) = 1$.
With Lemma 8.15, then there exist integers x and y such that $ax \equiv y \pmod{p}$ with $0 < |x|, |y| < \sqrt{p}$. Therefore,

$$\begin{aligned} a^2+1 &\equiv 0 \pmod{p} \\ x^2(a^2+1) &\equiv 0 \pmod{p} \qquad \textbf{Multiply } x^2 \\ x^2a^2 + x^2 &\equiv 0 \pmod{p} \\ y^2 + x^2 &\equiv 0 \pmod{p} \qquad y^2 = x^2a^2 \\ &\implies p \mid x^2 + y^2 \\ &\implies kp = x^2 + y^2 \qquad \exists k \in \mathbf{Z} \\ &\implies 2p > x^2 + y^2 \qquad 0 < |x|, |y| < \sqrt{p} \end{aligned}$$

Then $0 < kp = x^2 + y^2 < 2p \implies 0 < 2k < 2p \implies 0 < k < 2 \implies k = 1$. Therefore, $p = x^2 + y^2$ when $p \equiv 1 \pmod 4$. □

8.17 Exercise

Check the following identity:

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

Proof.

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= (ac + bd)^2 + (bc - ad)^2 \\ a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 &= a^2c^2 + b^2d^2 + 2abcd - 2abcd + b^2c^2 + a^2d^2 \\ a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \end{aligned}$$

□

8.18 Theorem

If an integer x can be written as the sum of two squares of natural numbers and an integer y can be written as the sum of two squares of natural numbers, then xy can be written as the sum of two squares of natural numbers.

Proof. Given that integers x and y can be expressed as the sum of two squares of natural number such that $x = a^2 + b^2$ and $y = c^2 + d^2$. Now suppose $x \cdot y$ then by direct proof,

$$\begin{aligned} x \cdot y &= (a^2 + b^2) \cdot (c^2 + d^2) \\ x \cdot y &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + 0 \\ x \cdot y &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + (2abcd - 2abcd) \\ x \cdot y &= a^2c^2 + b^2d^2 + 2abcd - 2abcd + b^2c^2 + a^2d^2 \\ x \cdot y &= (ac + bd)^2 + (bc - ad)^2 \end{aligned}$$

Thus, xy can be expressed as the sum of two squares of natural numbers. □

8.19 Exercise

For each of the following numbers, (i) determine the number's prime factorization and (ii) write the number as the sum of two squares of natural numbers.

1. 205

$$\begin{aligned}
&\implies 5(41)\\
&\implies (4+1)(25+16)\\
&\implies (2^2+1^2)(5^2+4^2)\\
&\implies 2^2(5^2)+2^2(4^2)+5^2+4^2\\
&\implies 10^2+8^2+5^2+4^2\\
&\implies (10+4)^2+(5-8)^2\\
&\implies (14)^2+(3)^2
\end{aligned}$$

2. 6409

$$\begin{aligned}
&\implies 13(17)(29)\\
&\implies (221)(29)\\
&\implies (11^2+10^2)(5^2+2^2)\\
&\implies 11^2(5^2)+11^2(2^2)+10^2(5^2)+10^2(2^2)\\
&\implies (55+20)^2+(50-22)^2\\
&\implies (75)^2+(28)^2
\end{aligned}$$

3. 722, no solution

4. 11745

$$\begin{aligned}
&\implies (45)(261)\\
&\implies (6^2+3^2)(6^2+15^2)\\
&\implies 6^2(6^2)+6^2(15^2)+3^2(6^2)+3^2(15^2)\\
&\implies (6(6)+3(15))^2+(3(6)-6(15))^2\\
&\implies (36+45)^2+(18-90)^2\\
&\implies (81)^2+(72)^2
\end{aligned}$$

8.20 Question

Which natural numbers can be written as the sum of two squares of natural numbers? State and prove the most general theorem possible about which natural numbers can be written as the sum of two squares of natural numbers, and prove it.

We can observe the natural numbers that can be written as the sum of squares have 1 common characteristics. Suppose n is the natural number and it can be express, by the Fundamental Theorem of Arithmetic, as $n = p_1^{r_1}p_2^{r_2}...p_m^{r_m}$. Then each prime can be expressed as the sum of squares which has its own theorem, Theorem 8.14.

8.21 Theorem

A natural number n can be written as a sum of two squares of natural numbers if and only if every prime congruent to 3 modulo 4 in the unique prime factorization of n occurs to an even power.

Proof. Incomplete. □

8.22 Theorem

If (a,b,c) is a primitive Pythagorean triple, then c is a product of primes each of which is congruent to 1 modulo 4.

Proof. Let (a,b,c) be a primitive Pythagorean triple then we can suppose that $a = 2st, b = s^2 - t^2$ and $c = s^2 + t^2$ where c is odd. Now, let p be 3 congruent to modulo 4 such that $p \equiv 3 \pmod 4$ and also that $p \mid c$ but $p \nmid s$ and evidently $p \nmid t$. This implies that,

$$\begin{aligned} c &\equiv 0 \pmod p \\ s^2 + t^2 &\equiv 0 \pmod p \\ s^2 &\equiv -t^2 \pmod p \\ s^2 \cdot t^{-2} &\equiv -1 \pmod p \\ (st^{-1})^2 &\equiv -1 \pmod p \end{aligned}$$

Thus $(st^{-1})^2 \equiv -1 \pmod p$ suggests a contradiction since -1 is not a quadratic residue. Hence, if $k \mid s$ and $k \mid t$ then (a,b,c) is not a primitive Pythagorean triple. So there is no solution if $p \equiv 3 \pmod 4$. Therefore, $p \equiv 1 \pmod 4$ where $p \mid c$ which implies that c is a product of primes each of which is congruent to 1 modulo 4. □

8.23 Theorem

If the natural number c is a product of primes each of which is congruent to 1 modulo 4, then there exist integers a and b such that (a,b,c) is a primitive Pythagorean triple.

Proof. To begin with, we can see that for a Pythagorean triple (a,b,c), then

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

By Theorem 8.22, we know that $p \equiv 1 \pmod 4$ is a sum of two squares and that the product of sum of two squares is also the sum of two squares. Thus, if each of the primes in the prime factorization of natural number c is congruent to 1 modulo 4, then c is also sum of two squares and thus there exist integers a and b such that (a,b,c) is a primitive Pythagorean triple. □

8.24 Theorem

There are no natural numbers x, y, and z such that $x^4 + y^4 = z^2$.

Proof. Incomplete. □

8.25 Blank Paper Exercise

- Pythagorean triple
- Sum of Squares of natural numbers
- Sum of Squares of primes
- Fermat's Last Theorem
- Sum of cubes
- Taxicabs
- Proof 8.23 was heavily researched.
- Proof 8.21 & 8.24 seemed impossible.