Asymptotically Counting Primitive Pythagorean Triples

Reina Itakura

This paper seeks to observe the number of primitive Pythagorean triples bounded by a positive real number B and its behavior as B grows larger. I will generally follow the proof from the text, *A Pythagorean Introduction to Number Theory* by Professor Ramin Takloo-Bighash, with some proofs coming from Professor Elena Fuchs's number theory course MAT 115B. In particular, I will be counting the number of elements in the set

$$S(B) = \{(a, b, c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2; \gcd(a, b, c) = 1; a, b, c \leq B\}.$$

The main theorem of this paper is Theorem 8. For ease of notation, I denote $\mathcal{N}(B) = \#S(B)$.

1 Setting Up for Counting

Definition 1. A triple $(a, b, c) \in \mathbb{Z}^3$ is a primitive Pythagorean triple if $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$.

I first want to characterize the primitive Pythagorean triples.

Theorem 2. *There exists infinitely many primitive Pythagorean triples (a, b, c) where b is even. Furthermore, they are given by equations:*

$$a = x^2 - y^2, b = 2xy, c = x^2 + y^2$$

where $x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$ and exactly one of x or y is even.

The proof of this is omitted as the proof did not align with the story I wanted to paint through this paper.[1] However, intuitively see that this is true because you can check for validity by computation, and for primitivity and completeness by contradiction. Note that the pairs x, y and $-x, -y$ result in the same triple as the negatives cancel out. This will be important later on.

From Theorem 2, we have that if $(a, b, c) \in S(B)$ with $c > 0$, then there exists coprime integers x and y, where exactly one of x or y is even such that $a = x^2 - y^2$, $b = 2xy$, and $c = x^2 + y^2$. Note that I am assuming that b is the even term. Note that we also know $|a|, |b| \leq |c|$ so we just need to bound $|c| = c = x^2 + y^2 \leq B$. I would like to emphasize that constructing the triples in this way results in triples with a positive c. However we also want to count triples with negative c, so we will need to multiply a factor of 2 later on.

Now, something that is slightly easier to count is

$$h(B) = \#\{(x, y) \in \mathbb{Z}^2 : \text{exactly one of } x \text{ or } y \text{ even}, \gcd(x, y) = 1, x^2 + y^2 \leq B\}.$$

See that $\mathcal{N}(B) = 2 \cdot 2 \cdot \frac{1}{2} \cdot h(B)$ where the first factor of two comes from switching a and b, the second factor of 2 comes from including negative c's as we assumed earlier that $c > 0$, and finally the $\frac{1}{2}$ factor comes from dividing out $(-x, -y)$[2].

To make this even easier to count, we relax the conditions a bit by removing primality. Consider this new function:

$$\tilde{h}(B) = \#\{(x, y) \in \mathbb{Z}^2 : \text{exactly one of } x \text{ or } y \text{ even}, x^2 + y^2 \leq B\}.$$

Our next goal is to be able to count this function $\tilde{h}(B)$. Notice that the pairs (x, y) being counted in $\tilde{h}(B)$ approximately correspond to half the number of lattice points in a circle as $B \to \infty$.

[1] I also ran out of space, this is so Fermat-core.

[2] Recall that (x, y) and $(-x, -y)$ get us the same a, b, c.

2 Counting Lattice Points in a Circle

To count $\tilde{h}(B)$, see that matching a length $\sqrt{2}$ square to each integral point with one even, one odd coordinate allows us to associate the number of integral points within the circle with the area of the circle of radius $\sqrt{B}$.

However, note that not every $\sqrt{2}$ square will be contained within this circle of radius $\sqrt{B}$. This can be dealt with, however. Note that the diagonal of each of these squares is 2, so each integral point assigned to that $\sqrt{2}$ square strays from the circle by at most 2. Finally, see that the area of each $\sqrt{2}$ square is 2, so we need to divide that out from the area of the circle.

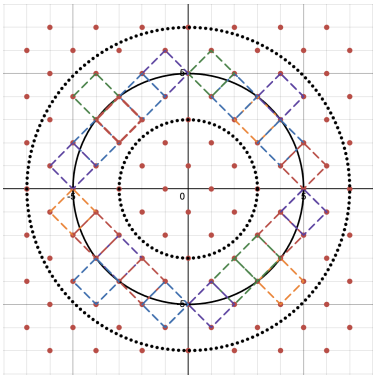

Fig. 1. The diagram for $\sqrt{B} = 5$

Thus, we have that

$$\frac{\pi}{2}(\sqrt{B}-2)^2 \leq \tilde{h}(B) \leq \frac{\pi}{2}(\sqrt{B}+2)^2$$

and writing this asymptotically, or in *big O* notation, we have that:

Lemma 3. *As* $B \to \infty$,

$$\tilde{h}(B) = \frac{\pi}{2}B + O(\sqrt{B}).$$

Now that we have an asymptotic formula for $\tilde{h}$, our next goal is to be able to express h in terms of $\tilde{h}$.

3 Möbius Inversion

See that if $x^2 + y^2 \leq B$ is a non-zero integral point, we can "make" them coprime by mapping it to $(\frac{x}{\gcd(x,y)})^2 + (\frac{y}{\gcd(x,y)})^2 \leq \frac{B}{\gcd(x,y)^2}$. Also note that since exactly one of x or y is odd, we have that $\gcd(x,y)$ is odd as well. Thus, we can establish a bijection between the set

$$\{(x,y) \in \mathbb{Z}^2 : \text{exactly one of } x \text{ or } y \text{ odd}, x^2+y^2 \leq B\}$$

and the disjoint set union

$$\bigsqcup_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \{(x,y) \in \mathbb{Z}^2 : \text{exactly one of } x \text{ or } y \text{ odd}, \gcd(x,y) = 1, x^2+y^2 \leq \frac{B}{\delta^2}\}.$$

Since we are union-ing over disjoint sets, we can just add up the cardinality of each set. Thus we have,

$$\tilde{h}(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} h\left(\frac{B}{\delta^2}\right)$$

Now, we want to be able to express h in terms of $\tilde{h}$. To help us do this, I present a well-known "tool", the Möbius function μ, and then show some of its properties.

The Möbius function, denoted μ, was first introduced by August Ferdinand Möbius in 1832. For input of $n = p_1^{r_1} \dots p_k^{r_k}$,[3] μ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } r_i = 1, \forall i \\ 0 & \text{otherwise} \end{cases}$$

[3] This is the prime factorization of n.

Proposition 4. *μ is multiplicative.*[4]

Proof. Let $m, n \in \mathbb{Z}$ such that $\gcd(m,n) = 1$. I want to write m, n in their prime factorizations, $m = p_1^{r_1} \dots p_k^{r_k}$ and $n = q_1^{s_1} \dots q_\ell^{s_\ell}$.

Note that $\gcd(m,n) = 1$ implies that $p_i \neq q_j$ for all pairs (i,j). See that if at least one of m or n has an exponent r_i or $s_i > 0$, then everything zeroes out.

In the square-free case, first note that if p is a prime, $\mu(p) = -1$. Then, we have that

$$\mu(mn) = \mu(p_1 \dots p_k \cdot q_1 \cdots q_k) = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \mu(m)\mu(n).$$

□

Proposition 5. *Let $F(n) = \sum_{d|n, d\geq 1} \mu(d)$. Then,*

$$F(n) = \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First, note that if we plug in 1 into F, we get $F(1) = 1$.

Next, see that F is multiplicative since μ is multiplicative. Let $\gcd(m,n) = 1$. Then,

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) = \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) = \left(\sum_{d_1|m} \mu(d_1)\right)\left(\sum_{d_2|n} \mu(d_2)\right) = F(m)F(n).$$[5]

Now we plug in prime powers.

$$F(p^k) = \sum_{\substack{d|p^k \\ d\geq 1}} \mu(d) = \sum_{i=0}^{k} \mu(p^i) = \mu(1) + \mu(p) + \underbrace{\mu(p^2) + \dots + \mu(p^k)}_{0} = 1 + (-1) = 0$$

Thus, for generic $n \neq 1$, $n = p_1^{r_1} \dots p_k^{r_k}$ then, $F(n) = F(p_1^{r_1}) \dots F(p_k^{r_k}) = 0$. □

Now we are ready to prove the following lemma, which will help us

Lemma 6. *Takloo-Bighash (2018) Suppose functions $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ and $G : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, for all $B > 0$, satisfy $F(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} G\left(\frac{B}{\delta^2}\right)$. Then,*

$$G(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} F\left(\frac{B}{\delta^2}\right)\mu(\delta)$$

Proof. Let functions $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ and $G : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, for all $B > 0$, satisfy $F(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} G\left(\frac{B}{\delta^2}\right)$.

Then, consider $g(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} F\left(\frac{B}{\delta^2}\right)\mu(\delta)$. See that

$$g(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} F\left(\frac{B}{\delta^2}\right)\mu(\delta) \overset{(2)}{=} \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \mu(\delta) \sum_{\substack{\eta^2 \leq \frac{B}{\delta^2} \\ \eta \text{ odd}}} G\left(\frac{B/\delta^2}{\eta^2}\right) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \sum_{\substack{\eta^2\delta^2 \leq B \\ \eta \text{ odd}}} G\left(\frac{B}{\eta^2\delta^2}\right)\mu(\delta)$$

$$\overset{(4)}{=} \sum_{\substack{n^2 \leq B \\ n \text{ odd}}} \sum_{d|n} G\left(\frac{B}{n^2}\right)\mu\left(\frac{n}{d}\right) \overset{(5)}{=} \sum_{\substack{n^2 \leq B \\ n \text{ odd}}} G\left(\frac{B}{n^2}\right) \underbrace{\sum_{d|n} \mu(d)}_{\substack{=0 \\ \text{if } n=0 \text{ (Prop. 5)}}} \overset{(6)}{=} G(B)$$

Note that we get (2) from assumption, (4) by setting $n = \eta\delta$ and rearranging terms, (5) since $\{d|n\} = \{\frac{n}{d} : d|n\}$, and (6) since by Proposition 5., $n \neq 1$ zeroes out, leaving only $G(B)$ in the summation. □

Remark 7. This Lemma holds if we remove the oddness constraint, using the same argument.

[4] Note that μ is just multiplicative, and not completely multiplicative.

[5] Note that this argument can be used more generally for any multiplicative function, and not just μ.

4 Combining Everything

From Lemma 3. and Lemma 6. we have

$$h(B) = \sum_{\substack{\delta^2 \le B \\ \delta \text{ odd}}} \tilde{h}\left(\frac{B}{\delta^2}\right)\mu(\delta) = \sum_{\substack{\delta^2 \le B \\ \delta \text{ odd}}} \left(\frac{\pi}{2}\cdot\frac{B}{\delta^2} + O(\sqrt{B/\delta^2})\right)\mu(\delta) = \frac{\pi}{2}B\sum_{\substack{\delta^2 \le B \\ \delta \text{ odd}}}\frac{\mu(\delta)}{\delta^2} + O\left(\sqrt{B}\sum_{\delta^2\le B}\frac{1}{\delta}\right)$$

Note that we can replace $\mu(\delta)$ with $O(1)$ in the last summation since the one function upper bounds μ (we use this trick again). Continuing, we have,

$$= \frac{\pi}{2}B\sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty}\frac{\mu(\delta)}{\delta^2} - \frac{\pi}{2}B\sum_{\substack{\delta^2 > B \\ \delta \text{ odd}}}^{\infty}\frac{\mu(\delta)}{\delta^2} + O\left(\sqrt{B}\sum_{\delta^2\le B}\frac{1}{\delta}\right) = \frac{\pi}{2}B\sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty}\frac{\mu(\delta)}{\delta^2} + O\left(B\sum_{\delta^2>B}^{\infty}\frac{1}{\delta^2}\right) + O\left(\sqrt{B}\sum_{\delta^2\le B}\frac{1}{\delta}\right).$$

Breaking down the last formula, intuitively observe that the sum in the first term is convergent by comparison with the series $\sum_{n\ge 1}\frac{1}{n^2}$. We call this sum C_2, and derive it at the very end.
See that for the second term,

$$\sum_{\delta^2>B}\frac{1}{\delta^2} \le \int_{\sqrt{B}}^{\infty}\frac{1}{t^2}dt \ll \frac{1}{\sqrt{B}}$$

and for the third term,

$$\sum_{\delta^2\le B}\frac{1}{\delta} \le \int_1^{\sqrt{B}}\frac{1}{t}dt \ll \log B.$$

Thus, we currently have,

$$h(B) = \frac{\pi}{2}C_2\cdot B + O(\sqrt{B}) + O(\sqrt{B}\log B) = \frac{\pi}{2}C_2 B + O(\sqrt{B}\log B).$$

4.1 Computing C_2

Recall from your calculus class that the series $\sum_{n=1}\frac{1}{n^2}$ converges absolutely, so it makes sense to compare C_2 to this series. We claim that

$$\frac{3}{4}C_2\cdot\sum_{n=1}\frac{1}{n^2} = 1^{6}.$$

Proof. Recall that $C_2 = \sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty}\frac{\mu(\delta)}{\delta^2}$. We want to get rid of this "oddness" constraint. An intuitive way to do this is to take the sum of all δ regardless of parity, then subtracting out the sum of δs of even parity. Thus, we get that

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2} = \sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty}\frac{\mu(\delta)}{\delta^2} + \sum_{\substack{\delta=1 \\ \delta \text{ even}}}^{\infty}\frac{\mu(\delta)}{\delta^2} \overset{(2)}{=} C_2 + \sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty}\frac{\mu(2\delta)}{2^2\delta^2} \overset{(3)}{=} C_2 + \frac{\mu(2)}{4}\sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty}\frac{\mu(\delta)}{\delta^2} = C_2 - \frac{1}{4}C_2.$$

In the second equality (2), you might be concerned that we "missed" some evens that have more than one power of 2 in its prime factorization. But note that by definition of the Möbius function μ, any input that has a prime square in its prime factorization will zero out. Also note that in the third equality (3) we can factor out the $\mu(2)$ because $\gcd(2,\delta) = 1$ when δ is odd and μ is multiplicative. Then,

$$\begin{aligned}\frac{3}{4}C_2\sum_{m=1}\frac{1}{m^2} &= \sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}\sum_{m=1}^{\infty}\frac{1}{m^2} = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{\mu(n)}{n^2m^2} = \sum_{\delta=1}^{\infty}\sum_{mn=\delta}^{\infty}\frac{\mu(n)}{n^2m^2} \\ &= \sum_{\delta=1}^{\infty}\frac{1}{\delta^2}\sum_{mn=\delta}^{\infty}\mu(n) = \sum_{\delta=1}^{\infty}\frac{1}{\delta^2}\sum_{n|\delta}^{\infty}\mu(n) = 1.\end{aligned}$$

[6] Note that the text I am referencing proves a more general result.

By Proposition 5, note that $\sum_{n|\delta}^{\infty} \mu(n) = 0$ unless $\delta = 1$, so the only term that survives is $\delta = 1$, getting us that the entire terms equals to 1. □

Now it remains to find the constant $\sum_{n=1} \frac{1}{n^2}$. This problem, known as the *Basel Problem*, was solved by Euler in 1735, and this value is known to be $\sum_{n=1} \frac{1}{n^2} = \frac{\pi^2}{6}$. I omit the proof as the result is well-known and the proof is not specific to this problem.

Thus, we get that $C_2 = \frac{8}{\pi^2}$.

4.2 Asymptotic Formula for Primitive Pythagorean Triples

Recall that by plugging in C_2, we now have

$$h(B) = \frac{4}{\pi}B + O(\sqrt{B}\log B).$$

Finally, plugging in $h(B) = \mathcal{N}_1(B)$ into the original equation $\mathcal{N}(B)$, we have

Theorem 8. *Takloo-Bighash (2018) As $B \to \infty$,*

$$\mathcal{N}(B) = 2 \cdot h(B) = \frac{8}{\pi}B + O(\sqrt{B}\log B).$$

Remark 9. As of when I am writing this paper, the text has a coefficient of $\frac{4}{\pi}$ instead of $\frac{8}{\pi}$, but I believe that $\frac{8}{\pi}$ is the correct coefficient, and that $\frac{4}{\pi}$ is a result of arithmetic error. In addition, this result with a coefficient of $\frac{8}{\pi}$ matches Lehmer's corollary from 1900, which is in support of my claim that $\frac{8}{\pi}$ is the correct coefficient..

Corollary 10. *Lehmer (1900). As $B \to \infty$, the number of primitive right triangles with hypotenuse bounded by B is*

$$\frac{1}{2\pi}B + O(\sqrt{B}\log B).$$

Note that we count primitive Pythagorean triples, both positive and negative, and we also count both $a^2 + b^2 = c^2$ and $b^2 + a^2 = c^2$ as separate triples. When counting the primitive right triangles, Lehmer fixes one of the sides to be even, in other words, does not distinguish between the triples $a^2 + b^2 = c^2$ and $b^2 + a^2 = c^2$. Finally, triangles cannot have negative length sides, so we must divide those out. See that there are three variables that can be negative, and we also divide out another factor of 2 for the swapping of a and b, getting us that from our derivation of $\mathcal{N}$, the number of primitive right triangles is $\frac{1}{2^4}\mathcal{N}(B) = \frac{1}{2\pi}B + O(\sqrt{B}\log B)$ as $B \to \infty$ as desired.

Reflection. Overall I think that I understand the argument pretty well. Since I like counting, all of the counting arguments made sense to me, and the Möbius function part of the proof made sense to me since we walked through a similar proof during class. I was already comfortable with the use of asymptotics and big-O notation from my computer science classes. The one part of the proof that I am not the most comfortable with is the Basel Problem proof because I decided not to focus on it and the proof was not as attractive to me than the other ones. I omitted the proof for theorem 1 because we did it in class and it is lengthy. In general I feel pretty confident in my understanding of the chapter, especially because I went through all of the counting and calculations for why I was getting $\frac{8}{\pi}$ instead of $\frac{4}{\pi}$. I think it also helped that I counted the lattice points slightly differently, proved Lemma 6 but without the oddness constraint (not in this paper), and counted the PPTs using our (MAT 115B's) characterization of them instead of the textbook's (they used odd x, y). My favorite part of the proof is section 3, where we deal with the primitivity which is hard to count using Möbius Inversion. I think it was also great that I chose to read the textbook as I found it extremely intuitive and easy to read and understand. I think I learned a lot from this experience.

References

Lehmer, D. N. (1900). Asymptotic evaluation of certain totient sums. *American Journal of Mathematics*, *22*(4), 293–335. Retrieved 2025-03-14, from http://www.jstor.org/stable/2369728

Takloo-Bighash, R. (2018). *A pythagorean introduction to number theory.* Springer Cham. DOI: 0.1007/978-3-030-02604-2