

A Friendly Introduction to My Thesis  
by  
Thomas Wright

A Math Paper  
Baltimore, Maryland  
January, 2009

©Thomas Wright 2009  
All rights reserved

# Chapter 1

## In The Beginning

### 1.1 The Introduction: A Friendly Introduction to the Friendly Introduction

#### or Squares: Not Just Fifties Slang

Our story begins in 1620, at a time when pursuing mathematics for no apparent practical purpose was frowned upon<sup>1</sup> and many mathematicians had to have day jobs<sup>2</sup>. One such mathematician, Claude Gaspard Bachet de Méziriac, realizing his potential for being cited in horribly written expositions for the rest of time, noticed the following. Many times, a positive integer (sometimes called a *natural number*) can be written as the sum of two squares. For instance

$$\begin{aligned}5 &= 1^2 + 2^2, \\13 &= 2^2 + 3^2, \\16 &= 4^2 + 0^2.\end{aligned}$$

Other times it can't. For instance, 6 cannot be written as the sum of two squares. Neither can 11. 12 also has problems. If one were to ask, "How many natural numbers can be written as the sum of two squares?" the answer would be, "Not all of them."

---

<sup>1</sup>Savages.

<sup>2</sup>Can you imagine mathematicians having to get real world jobs? That would be a disaster.

Sometimes, a number can't be written as the sum of two squares, but it can be written as the sum of three squares. For instance

$$\begin{aligned}6 &= 1^2 + 1^2 + 2^2, \\11 &= 1^2 + 1^2 + 3^2, \\12 &= 2^2 + 2^2 + 2^2.\end{aligned}$$

However, this still doesn't take care of all of the numbers. 7, for instance, can't be written as the sum of three squares. 15 and 23 are still problems, too. Again, if one asked, "How many natural numbers can be written as the sum of *three* squares?" the answer would be, "Still not all of them."

What about four squares? Well, this works for 7, 15, and 23:

$$\begin{aligned}7 &= 1^2 + 1^2 + 1^2 + 2^2, \\15 &= 1^2 + 1^2 + 2^2 + 3^2, \\23 &= 1^2 + 2^2 + 2^2 + 3^2.\end{aligned}$$

Does it work in general? Well, Bachet certainly had no idea. He posed this as a question for future mathematicians:

**Bachet's Question:** *Can every positive integer be written as the sum of four squares?*

In mathematical terminology, this is the following:

**Bachet's Question (but mathier):** *For any natural number (i.e. positive integer)  $\nu$ , is there a solution to*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \nu$$

*where  $x_1, x_2, x_3,$  and  $x_4$  are be integers?*

In 1770, Lagrange came up with an answer:

**Lagrange's Answer:** *Yes.*

Lagrange proved that any natural number can indeed be written as the sum of four squares. This theorem became known, quite logically, as Lagrange's

Four Squares Theorem.

A few years later, British mathematician Edmund Waring decided that this theorem was pretty<sup>3</sup> but not nearly complicated enough. He decided that it could be expanded in scope to describe cubes, fourth powers, fifth powers, and all higher powers. For instance, every natural number can be written as the sum of nine cubes, which is to say that the equation

$$x_1^3 + x_2^3 + x_3^3 + \dots + x_9^3 = \nu$$

always has integer solutions, regardless of  $\nu$ .

What about fourth powers? Well, any natural number can be written as the sum of 19 of those:

$$x_1^4 + x_2^4 + x_3^4 + \dots + x_{19}^4 = \nu.$$

5th powers? 37 of those suffice:

$$x_1^5 + x_2^5 + x_3^5 + \dots + x_{37}^5 = \nu.$$

6th powers? 73 of those are enough:

$$x_1^6 + x_2^6 + x_3^6 + \dots + x_{73}^6 = \nu.$$

Can we keep doing this for every power? Waring certainly thought so:

**Waring's Conjecture** (1782): *We can keep doing this process for every exponent.*

To put this in mathier terms, Waring conjectured that for any exponent you pick (call this exponent  $k$ ), there should be a number  $n$  such that

$$x_1^k + x_2^k + x_3^k + \dots + x_n^k = \nu$$

is guaranteed to have integer solutions<sup>4</sup> for every  $\nu$ . This conjecture became

---

<sup>3</sup>Some mathematicians have a funny view on the word "pretty."

<sup>4</sup>Note here that  $n$  depends on  $k$ . In fact,  $n$  is sometimes denoted  $n(k)$  to emphasize this. What, did you expect all of the footnotes to be jokes? Geez.

known as Waring's Problem and therefore deserves not only capitalization but also bold letters:

**Waring's Problem (Waring's Conjecture with Fancier Words) (1782):**

*Prove that for any  $k$ , there exists an  $n$  such that*

$$x_1^k + x_2^k + x_3^k + \dots + x_n^k = \nu$$

*has a solution for any natural number  $\nu$ .*

Incumbent in this problem are two actual questions:

- 1.) Does such an  $n$  exist regardless of the power  $k$  that I've chosen?
- 2.) For a given power  $k$ , what is  $n$ ?

Question 1 was answered in the affirmative by David Hilbert<sup>5</sup> in 1908. For the second question, however, Hilbert's method was ineffective; for instance, if  $k = 3$ , Hilbert's method merely said that  $n \leq 53$ , a far cry from the  $n = 9$  that we know to be true.

For question 2, piecemeal results trickled for several years after Hilbert's discovery. Then, in 1919, G.H. Hardy and J.E. Littlewood discovered a new method which would become the standard approach not just for Waring's problem but all related problems as well. This method was called the *circle method*, named as a facetious reference to Hardy's mother's considerable girth<sup>6</sup>.

The circle method has solved Waring's Problem for many powers and has given good bounds for what the solution will be in many others. Naturally, that means that Waring's problem is too easy.

---

<sup>5</sup>Hilbert is my mathematical great-great grandfather (my advisor's advisor's advisor's advisor). This has no relevance to anything, but I felt the need to throw this in.

<sup>6</sup>Okay, that's not true, but there aren't enough mother jokes in mathematics, so I'm leaving this in here. Also, Hardy and Littlewood did decide on the name before they actually came up with the method, which is kind of odd.

## 1.2 Friends of Waring's Problem: A Friendly Introduction to the Friends of the Friendly Introduction to the Friendly Introduction

If the previous section had been the end of the story, I would be unemployed<sup>7</sup>. Therefore, in an attempt at self-preservation and possibly government grants, we will make this problem slightly more interesting by adding constraints.

In particular, let's write

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \nu.$$

We know the above has a solution. LaGrange told us so, and he's dead, so you can't question him. However, what if we added another equation that we want to be solved simultaneously

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= \nu_1, \\ x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 &= \nu_2? \end{aligned}$$

Is four variables always enough to guarantee a solution to *both* equations? Well, no. How many variables do we need to guarantee a solution? I'm glad you asked. I have a fifty-page paper in hand that gets about halfway to a solution to that question. It seems like the answer is 6, provided the  $\nu_1$  and  $\nu_2$  aren't too far apart from one another.

## 1.3 The Circle Method: Yo Mamma's So Fat, She Has a Mathematical Method Named After Her

Hardy and Littlewood's new method relied on an important mathematical identity. Let  $a$  be an integer. Then

$$\int_0^1 e^{2\pi i a y} dy = \begin{cases} 1 & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

---

<sup>7</sup>Of course, the way the market looks, I may soon be unemployed anyway.

This is known as Euler's Formula, possibly named after someone named Euler. It tells us whether or not  $a$  is zero.

Hardy and Littlewood realized that they could do the following. Say we have the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \nu.$$

Let's do something tricky to it. See if you can spot the trick:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu = 0.$$

Take a look at the left side there

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu$$

What do we want to know about this left side? We want to know if it's zero. Now, Euler's formula told us whether  $a$  is zero. Could it tell us whether  $x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu$  is ever zero? I don't see why not. There's nothing special about the letter  $a$  except that some dead ancient guy decided it should be at the beginning of the alphabet<sup>8</sup>. If we just put  $x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu$  in everywhere we see  $a$ , we'd get

$$\int_0^1 e^{2\pi i(x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y} dy = \begin{cases} 1 & \text{if } x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu = 0, \\ 0 & \text{if } x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu \neq 0. \end{cases}$$

Let's call this thing  $M[x_1, x_2, x_3, x_4]$ , i.e.

$$M[x_1, x_2, x_3, x_4] = \int_0^1 e^{2\pi i(x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y} dy.$$

How can we use this? Let's try plugging *every* possible value for  $x_1$ ,  $x_2$ ,  $x_3$ , and  $x_4$  into  $M[x_1, x_2, x_3, x_4]$ .  $M[x_1, x_2, x_3, x_4]$  will spit out a 0 or a 1 depending on whether or not the  $x_1$ ,  $x_2$ ,  $x_3$ , and  $x_4$  we've plugged in are solutions to the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu = 0.$$

---

<sup>8</sup>As a person whose last name begins with "W", I am wholeheartedly opposed to alphabetical order.

Add up all these 0's and 1's. That's the total number of solutions to the equation!

Now, because mathematicians like to write things with cool looking Greek symbols, we use the universal symbol for "sum", which is  $\sum$ . This adding up of the zeroes and ones is written mathematically as

$$\text{number of solutions} = \sum_{x_1, x_2, x_3, x_4 \in \mathbb{Z}} M[x_1, x_2, x_3, x_4],$$

which just means "plug all possible integer  $x_1$ 's,  $x_2$ 's,  $x_3$ 's, and  $x_4$ 's ( $\mathbb{Z}$  means "integers" for some reason) into  $M[x_1, x_2, x_3, x_4]$  and then add up the results."

Do you remember what  $M[x_1, x_2, x_3, x_4]$  stood for? Good. Let's plug that into the equation above:

**Important Equation:**

$$\text{number of solutions} = \sum_{x_1, x_2, x_3, x_4 \in \mathbb{Z}} \int_0^1 e^{2\pi i(x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y} dy.$$

## 1.4 Goofy notation

Sometimes, instead of writing  $e^{2\pi ix}$ , we write  $\chi(x)$ . Why? Because the exponents get kind of annoying. Compare:

$$\int_0^1 e^{2\pi i(x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y} dy,$$

$$\int_0^1 \chi((x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y) dy.$$

It's no contest.

Also, instead of writing out "number of solutions" every time, we abbreviate this as  $N(\nu)$ . It's the same idea, but it saves paper, and who isn't all about the environment these days?

Combining these two facts, we can rewrite the Important Equation as

**Important Equation (reprise):**

$$N(\nu) = \sum_{x_1, x_2, x_3, x_4 \in \mathbb{Z}} \int_0^1 \chi((x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y) dy.$$

## 1.5 Addendum

What do you think we'd do if, instead of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \nu,$$

we had, as promised earlier,

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= \nu_1, \\ x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 &= \nu_2? \end{aligned}$$

Well, instead of one integral, we would have two:

$$\begin{aligned} N(\nu) &= \sum_{x_1, x_2, x_3, x_4 \in \mathbb{Z}} \int_0^1 \chi((x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu_1)y_1) dy_1 \\ &\quad \times \int_0^1 \chi((x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 - \nu_2)y_2) dy_2. \end{aligned}$$

That's it. Now, we have the ability to tackle any equation or system of equations. Pretty neat trick, huh?

## Chapter 2

# Prime Numbers: The Greatest Discovery in the History of the Universe

### 2.1 Modular Arithmetic: Why Number Theorists Wear Watches

Imagine you had a clock. Or else look at the one you have. Right now, it's about 3 o'clock<sup>1</sup>. In 6 hours, what time will it be? You guessed it: 9 o'clock.

$$3 + 6 = 9.$$

Say it were now 9 o'clock. In 6 hours, what time would it be? You guessed it: 15 o'clock.

$$9 + 6 = 15.$$

Wait, that can't be right. My clock only goes up to 12 and then goes back to 1. In 6 hours, then, it would be 3 o'clock.

This defines a new kind of addition; we can call it "clock arithmetic," though number theorists often call it "modular arithmetic." To indicate that this is modular arithmetic instead of regular arithmetic, we often write " $\equiv$ "

---

<sup>1</sup>If it's not 3 around o'clock, you should assume that you are reading this paper in the wrong time zone. Shame on you.

instead of "=", and we write  $(\text{mod } 12)$  to indicate that twelve is where the clock resets. Thus,

$$3 + 6 \equiv 9 \pmod{12},$$

but

$$9 + 6 \equiv 3 \pmod{12}.$$

By convention, instead of 12, we say 0, so picture a clock where the 12 has been replaced by a 0 and you're good:

$$4 + 8 \equiv 0 \pmod{12}.$$

This works for subtraction as well. For example, if we start at 2 o'clock and go back 4 hours, we get not -2 o'clock but instead 10 o'clock:

$$2 - 4 \equiv 10 \pmod{12}.$$

Multiplication strays from the analogy a little bit, but it still works: if we start at 0 and go forward  $3 \cdot 10 (=30)$  hours, we end up at 6 o'clock, so

$$3 * 10 \equiv 6 \pmod{12}.$$

You know what's awesome about this? This "mod 12" thing means we only have to deal with the numbers from 0 to 11; since we'll never have, say, a 22 o'clock, all the other numbers don't matter.

What if we lived in a country<sup>2</sup> where clocks were 7 hours instead of 12? A clock go from 0 to 6, and after 6, it would go back to 0 and start again. Here, our clock arithmetic would look a little different. Let's say it's 3 o'clock now. In 1 hour, it would be four o'clock:

$$3 + 1 \equiv 4 \pmod{7}.$$

In 4 hours, though, the clock would reach 0:

---

<sup>2</sup>No, no such country exists. Bear with me anyway.

$$3 + 4 \equiv 0 \pmod{7}.$$

In 6 hours, then, it would be 2 o'clock:

$$3 + 6 \equiv 2 \pmod{7}.$$

Likewise, if we started at 3 o'clock and subtracted off 4 hours, we would end up at 6 o'clock:

$$3 - 4 \equiv 6 \pmod{7}.$$

This sort of arithmetic works not just with mod 7 or mod 12 but mod any positive integer.

Mathematically, what does it mean to be "mod 12"?<sup>3</sup> To find out, let's go back to our example. We said that the 15th hour was actually 3 (mod 12). What relationship do 3 and 15 have? This one:

$$15 = 3 + 12.$$

What if we went forward 12 more hours? Well, it would still be 3 o'clock, but now it would actually be the 27th hour. What's the relationship here? This:

$$27 = 3 + 12 \cdot 2.$$

12 hours later, it would still be 3 o'clock, but now we have

$$39 = 3 + 12 \cdot 3.$$

Noticing a pattern? Good! I had faith in you. A number is considered 3 (mod 12) if it can be written as  $3 + 12k$  for some integer  $k$ .

What if it were 5 (mod 12)? Well, then it could be written as  $5 + 12k$ . Examples of this include

---

<sup>3</sup>This sounds like one of those pseudo-deep questions that mathematicians always get asked at bars. You know, the ones where, after you tell them you're a mathematician, they try to ask to make them sound deep and intellectual, like, "How do we know 2 doesn't equal 1?" or "Do you think everything in the universe can be explained by numbers?" Yeah. I hate those questions.

$$\begin{aligned}53 &= 5 + 12 \cdot 4, \\89 &= 5 + 12 \cdot 7, \\5 &= 5 + 12 \cdot 0, \\-7 &= 5 + 12(-1).\end{aligned}$$

All of these numbers would be 5 (mod 12).

Note that, as pointed out before, this means we only have to worry about the numbers 0-11 in mod 12. Similarly, we would only have to worry about the numbers 0-6 in mod 7, or 0-2 in mod 3, or 0-28 in mod 29, or 0-112 in mod 113, or...well, you get the point.

## 2.2 All Mathematics Is Local

Let's flip this "mod" business around. Imagine<sup>4</sup> that we're given the equation

$$x^3 \equiv 1 \pmod{7}.$$

What's  $x$ ? One option is obviously 1:

$$1^3 \equiv 1 \pmod{7}.$$

There's another option, though. If we tried  $x = 2$  instead, we see that

$$2^3 = 8 = 1 + 7 \cdot 1,$$

which means that

$$2^3 \equiv 1 \pmod{7}.$$

But wait, there's even a third solution:

$$4^3 = 64 = 1 + 7 \cdot 9,$$

---

<sup>4</sup>I'm not really sure why you'd need to imagine this. I am, in fact, giving you that equation.

which means that

$$4^3 \equiv 1 \pmod{7}.$$

So  $x$  is 1, 2, or 4 (mod 7).

Well, that's just great. We've taken a problem that's really easy ( $x^3 = 1$ ), and, thanks to our brilliant "modular arithmetic," we've made the problem harder. Thanks a lot, math.

Fortunately, this doesn't always happen; sometimes, if you can believe it, problems get easier. For instance, take the following equation. We'll call it "Freddie's Equation" for obvious reasons<sup>5</sup>:

$$x^6 + x^4 - 3x^2 + x^2 = 2.$$

Quick, find an integer solution.

Still looking? Yeah, you'll be doing that for a while.

What if we tried this equation mod 3? It would look like this:

$$x^6 + x^4 - 3x^3 + x^2 \equiv 2 \pmod{3}.$$

As I pointed out at the end of the last section<sup>6</sup>, this reduces the arithmetic to the numbers 0, 1, and 2. Let's plug in 0, 1, and 2 for  $x$ :

$$\begin{aligned} 0^6 + 0^4 - 3(0^3) + 0^2 &= 0, \\ 1^6 + 1^4 - 3(1^3) + 1^2 &= 0, \\ 2^6 + 2^4 - 3(2^3) + 2^2 &= 60 = 0 + 3 \cdot 20. \end{aligned}$$

None of these are 2 (mod 3). So there are no solutions mod 3.

Now, you would hope that this would have a relationship to Freddie's Equation, or else I just wasted a bunch of your time. In fact, there is:

**Mod 3 Theorem:** *If there are no solutions mod 3, there are no solutions to the original (Freddie's) equation.*

---

<sup>5</sup>I can't actually think of a good reason. But hey, why not?

<sup>6</sup>You were paying attention, weren't you?

Do you know what's special about 3? Nothing! This mod 3 theorem works for mod 5, or mod 2, or mod 113, or mod any other number you can think of:

**Mod  $p$  Theorem:** *If there are no solutions mod  $p$  for any positive integer  $p$ , there are no solutions to the original problem.*

Now, we talked for a while about mod 12, and we know that  $12 = 2^2 \cdot 3$ . As it turns out, if anything interesting happens mod 12 then it happens mod 2, mod 3, or both. This actually works in general: if a number  $p$  is not prime, we can look mod its prime factors instead of mod  $p$ , and we'll get the same information.

Because of this, we can amend the theorem above to ignore every number that isn't prime:

**Better Mod  $p$  Theorem:** *If there are no solutions mod  $p$  for any prime number  $p$ , there are no solutions to the original problem.*

The information about an equation mod  $p$ 's is known as the "local" data. That's the point of the section title.

## Chapter 3

# Using Prime Numbers to Solve Equations: It *Might* Work

### 3.1 Hasse Principle: An Anagram for "Preach Less in Pi"<sup>7</sup>

That Mod  $p$  Theorem was pretty awesome, no? It's pretty powerful, too; if we can find any prime number  $p$  where the equation has no solutions mod  $p$ , then we're done. What if we wanted to prove the equation *did* have solutions, though? After all, that's what the whole Hardy-Littlewood thing was about.

Hasse had a thought, which he called a "principle" because he often confused ethics with mathematics. The thought was this:

- 1.) Check to see that the equation has solutions mod  $p$  for all prime numbers  $p$ .
- 2.) If it does, the original equation must have solutions by the mod  $p$  theorem! Right?

Does the Hasse Principle work? In a word, no. In four words, sometimes but not always. In twenty-three words and two slightly lewd gestures...eh, I'm tired of counting words. Here's an example where it does work:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \nu.$$

---

<sup>7</sup>Also, "A Rich Pepsi Lens" and "I, Nipple Chaser".

The equation has solutions mod  $p$  for all  $p$ , and it also has solutions in general. So far, so good.

Unfortunately, here's an example (called Selmer's equation) where it doesn't work:

$$3x^3 + 4y^3 + 5z^3 = 0.$$

This has a solution mod  $p$  for every  $p$ , but it doesn't have a general solution where  $x$ ,  $y$ , and  $z$  are integers.

If the Hasse Principle works, we mathematicians say, "The Hasse Principle holds." If it doesn't work, we say, "The Hasse Principle doesn't hold." If it's tough to tell, we say, "@%\$& #%@!," and then we break things<sup>8</sup>.

What we get, then, is a new two-pronged way of figuring out where equations hold

- 1.) Check to see that the equation has solutions mod  $p$  for all  $p$ .
- 2.) Use complicated algebraic methods to figure out whether the Hasse Principle holds.

In my thesis, I use exactly this method to try to figure out whether there are solutions to the equations

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + \dots + x_6^2 &= \nu_1, \\ \lambda_1 x_1^2 + \lambda_2 x_2^2 + \lambda_3 x_3^2 + \dots + \lambda_6 x_6^2 &= \nu_2, \end{aligned}$$

where the  $\lambda$ 's are just any old integers (though we'll assume that no two of the  $\lambda$ 's are equal to one another).

For part 1, I use a clever method that looks like the integration from the first installment but is much easier. I'll explain this a little more in the upcoming section.

For the second part, I actually use two methods. The first is called, "Let's Hope Somebody Else Already Proved It," and if the first fails, the second is called, "Let's Pretend It's True." I don't think I have to explain these.

---

<sup>8</sup>When the Hasse Principle comes up, it's best to stay out of the way.

### 3.2 $p$ -adics: Taking What We Already Know and Putting Goofy Notation On It

Remember how we could find the number of solutions to an equation in the last installment? We had this method where we took this integral

$$\int_0^1 \chi((x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y)dy,$$

or, if we had multiple equations (like the ones above),

$$\int_0^1 \chi((x_1^2 + x_2^2 + x_3^2 + \dots + x_6^2 - \nu_1)y)dy \cdot \int_0^1 \chi((\lambda_1 x_1^2 + \lambda_2 x_2^2 \dots + \lambda_6 x_6^2 - \nu_2)y)dy,$$

and we took the sum over all various integers? Well, there's an analogous integral method to find the number of solutions mod  $p$ . The integral has a funny-looking notation:

$$\int_{\mathbb{Q}_p} \chi((x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)\xi)d\xi,$$

or, for two equations,

$$\int_{\mathbb{Q}_p} \chi((x_1^2 + x_2^2 + x_3^2 + \dots + x_6^2 - \nu_1)\xi_1)d\xi_1 \cdot \int_{\mathbb{Q}_p} \chi((\lambda_1 x_1^2 + \lambda_2 x_2^2 \dots + \lambda_6 x_6^2 - \nu_2)\xi_2)d\xi_2,$$

What this equation means specifically is beyond the scope of this paper, but it suffices to think of it as a mod  $p$  analogy to the Important Equation from the first installment.

Remember how the next step was to plug in all integers and add up the results? That's what we do here, too. Again, the notation looks a little funny:

$$\int_{\mathbb{Z}_p^n} \int_{\mathbb{Q}_p} \chi((x_1^2 + x_2^2 + x_3^2 + \dots + x_6^2 - \nu_1)\xi_1)d\xi_1 \cdot \int_{\mathbb{Q}_p} \chi((\lambda_1 x_1^2 + \lambda_2 x_2^2 \dots + \lambda_6 x_6^2 - \nu_2)\xi_2)d\xi_2 dx,$$

but that  $\mathbb{Z}_p^n$  thingy on the front works like the summation symbol ( $\sum$ ) did in the last installment. This expression means just what was said above: evaluate the integral at each point mod  $p$ , then add up all of the evaluations.

Sometimes, just to clean everything up, we pull all of the integrals out front and write  $f(x)$  for the pair of equations and  $\nu$  for  $\nu_1, \nu_2$ :

$$\int_{\mathbb{Q}_p^2} \int_{\mathbb{Z}_p^n} \chi(\langle f(x) - \nu, \xi \rangle) dx d\xi.$$

Basically, this is just a nice way to write the integral so that it doesn't take up as much space<sup>9</sup>.

We call this thing  $S_p(\nu)$ , or the *p-adic singular series*. For those people that can't understand things unless they're written as equations, the previous sentence says,

$$S_p(\nu) = \int_{\mathbb{Q}_p^2} \int_{\mathbb{Z}_p^n} \chi(f(x) - \nu, \xi) dx d\xi.$$

It turns out that this integral doesn't work quite as nicely as the one from the previous chapter. In the previous case, we had

$$\int_0^1 e^{2\pi i(x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y} dy = \begin{cases} 0 & \text{if } x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu \neq 0, \\ 1 & \text{if } x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu = 0. \end{cases}$$

which made it really easy to figure out the number of solutions. In this case, we basically have

$$\int_{\mathbb{Q}_p} \chi((x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu)y) dy = \begin{cases} 0 & \text{if } x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu \not\equiv 0 \pmod{p}, \\ ? & \text{if } x_1^2 + x_2^2 + x_3^2 + x_4^2 - \nu \equiv 0 \pmod{p}. \end{cases}$$

You can see why this wouldn't be quite as helpful. However, it still works in a narrower way: if the integral is *not* zero, the equation has a solution. This warrants bold letters:

**Theorem:** *If  $S_p(\nu) \neq 0$  then there are solutions mod  $p$ .*

So there's that, which is nice. If we figure out  $S_p(\nu)$  for every  $p$ , we can completely finish the first half of the two-pronged Hasse Principle business. Combined with our foolproof methods of hoping and pretending for the second part, this solves the problem.

---

<sup>9</sup>Often, we will write this as  $\int_{\mathbb{Q}_p^2} \int_{\mathbb{Z}_p^n} \chi(\langle f(x), \xi \rangle) \bar{\chi}(\langle \nu, \xi \rangle) dx d\xi$ . It means the same thing.

### 3.3 Massively Important Conjecture

While the above was a good use of the Hasse Principle, we actually expect these  $S_p(\nu)$ 's to give us more info.

Take all of the  $S_p(\nu)$ 's for all of the various prime  $p$ 's and multiply them together. We call this product  $S(\nu)$ . Here's an outrageous claim about  $S(\nu)$ :

**Outrageous Claim:** *Numerically,  $S(\nu)$  and the actual number of solutions are very close to one another. In fact, as the  $\nu_1$ 's and  $\nu_2$ 's get larger,  $S(\nu)$  and the number of solutions get closer and closer.*

**Proof:** ?

There's evidence that the claim is true, and we *expect* it to be true, but there's nothing close to a proof.

In my thesis, I calculate  $S(\nu)$ . I have no idea if it shows the number of solutions. That'll be someone else's job.