

I remember once going to see [Ramanujan] when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavourable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."

– G.H. HARDY

Introduction

The sum is possibly the most fundamental operation in mathematics. It's what every child learns when first studying it and probably the first thing that comes to mind to a person when one mentions our subject. The study of how natural numbers relate to each other by means of sums is one as old as mathematics itself. Despite its apparent simplicity, it gives rise to a great number of surprising, difficult and profound results and has been developed by some of the most brilliant minds in the history of mathematics, from Pythagoras and Archimedes to Hardy and Ramanujan through Euler and Gauss.

"Sums of integers", however, is a fairly wide and somewhat vague description of the problem. So what do we really mean when saying this? Generally, we consider a set S of positive integers and see what we get by summing different elements of this set together while imposing certain conditions on the sums. We can, for instance, let S be the set of prime numbers, the set of even positive integers or the set of perfect numbers and ask questions such as "In how many ways can we express a number n as a sum of distinct elements of S ?" or "Which natural numbers can be written as a sum of three members of S ?"

In essence, there are two major approaches to the problem, each with a distinct flavour and take on the subject matter while still maintaining ample interplay between them. The first one is of a combinatorial nature and roughly deals with questions like our first example, where the emphasis is placed on finding the number of ways of expressing integers as sums of elements of a set. The problem of "integer partitions" is our chief interest here and indeed probably one of the most studied problems in this area of mathematics. The second approach we will consider is one of a more classical number theoretic kind and is mostly concerned with the possibility of expressing integers as sums of members of a certain set, as in our second example. The problems of decompositions of integers into sums of powers is the dominant theme here and contains some of the most elegant theorems in mathematics as well as some of the hardest of its unsolved problems.

1 A First Look at Integer Partitions

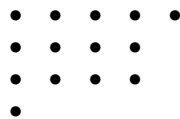
We call an *integer partition* of n any expression of the form $\lambda : n = \lambda_1 + \lambda_2 + \dots + \lambda_\ell$, with $\lambda_i \in \mathbb{N}$.¹ Of course, as discussed in the introduction, we can set a number of restrictions on the form of the sum (such as the number of summands, whether or not they should be distinct or if we shall take into

¹We set $\mathbb{N} := \{1, 2, 3, 4, \dots\}$ and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ for the remainder of this essay.

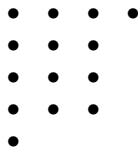
account their order) as well as on the summands themselves (for instance, we could mandate that all the summands should be even or that they should be greater than 2 — this corresponds to the set S we mentioned before).

Let us consider an easy example (from [3, Chap. 4]) to illustrate this. We shall attempt to find the number of partitions of a positive integer n into 1s and 2s, taking into account the order of the summands. This is readily done recursively: call a_k the number of such representations for a given (non-zero) number k . Now, any such partition must necessarily end by a 1 or a 2. Removing the last summand therefore gives us a partition of $k - 1$ or $k - 2$ respectively². As such, we get the recurrence relation $a_k = a_{k-1} + a_{k-2}$ which we recognise as that of the *Fibonacci numbers*³ $(F_n)_n$. We can thus conclude that $a_k = F_{k+k_0}$ where we can easily see that $k_0 = 1$ since there are $F_2 = 1$ representations of 1 and $F_3 = 2$ representations of 2 and, using a well known closed form for F_n , we have $a_n = \frac{\varphi^{n+1} - (1-\varphi)^{n+1}}{\sqrt{5}}$ (with $\varphi := \frac{1}{2}(1 + \sqrt{5})$). It is clear that the method generalises to such ordered decompositions into integers from any finite set of natural numbers by means of solving a similar linear recurrence relation.

In general, however, we shall disregard the order of the parts and add the additional convention that $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_\ell \geq 1$ to our previous notation for a partition. A useful way of representing such partitions is what is known as a *Ferrers diagram*. This corresponds to writing out a partition in a “matrix”⁴ of dots with row i of the matrix being part λ_i of our partition (five dots would represent the partition 5, for example). For instance, the Ferrers diagram of the partition $14 = 5 + 4 + 4 + 1$ is:



We also define an operation known as *conjugation* on Ferrers diagrams[6, Chap. 15], which consists of taking the “transpose” (in the sense of matrix transposition) of the diagram⁵. The conjugate of our example diagram above is thus:



which corresponds to the partition $14 = 4 + 3 + 3 + 3 + 1$. By the fact that conjugation is an involution (i.e. a self-inverse map and thus a bijection), we can immediately deduce an interesting result: the number of partitions of a positive integer into k parts is the same as the number of partitions of it for which the

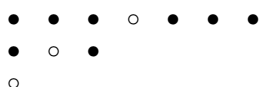
²Conversely, adding a 1 (resp. 2) to that partition of $k - 1$ (resp. $k - 2$) gives us back our initial partition — this is a simple example of a bijection between the sets of partitions of $k - 1$ (resp. $k - 2$) and the partitions of k ending with 1 (resp. 2).

³We use the convention that $F_0 = 0$ and $F_1 = 1$.

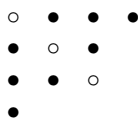
⁴Indeed, one could formally treat Ferrers diagrams as binary matrices.

⁵This operation can thus also work on partitions of a given number (since the number of dots of the conjugate partition is the same they both represent the same number), considering the one-to-one correspondence between diagrams and partitions — this is what is meant by a conjugate partition.

largest part is k . This is because, as stated before, conjugation is a bijection and taking the conjugate of a partition with $\lambda_1 = k$ gives us a partition with k parts and conversely taking a partition with k parts and conjugating it will yield a partition with $\lambda_1 = k$. Another interesting question is that of partitions which are *self-conjugate*, i.e. those with diagonally symmetrical Ferrers diagrams. It turns out that there are as many of these as partitions with odd distinct parts: taking one of the latter type of partition, simply “bend” each of the parts around its middle point (into an L shape) in the Ferrers diagram and arrange them so that the middle points lie on the diagonal (with the largest part on the exterior and the rest in decreasing order), hence obtaining a self-conjugate partition. To illustrate this with an example, here is the diagram of the partition $11 = 7 + 3 + 1$ with the middle point of each part highlighted:



Applying our transformation to the diagram, we get:



which corresponds to the self-conjugate partition $11 = 4 + 3 + 3 + 1$. Since the transformation is clearly reversible, we have a bijection and hence our desired equality. As a final proof using Ferrers diagrams, we can show that the number of partitions of $n + k$ into exactly k parts is the same as the number of partitions of n into at most k parts. In this case, starting with a partition of the former type, we can get one of the latter by deleting the first dot of each part (in the case where the part is 1, this removes it altogether). The result is clearly a partition into at most k parts of $n + k - k = n$ and it can be easily reversed by adding a column of k dots to any partition of n into at most k parts so as to obtain a partition of $n + k$ into exactly k parts (with some of them equal to 1 if the starting partition was into less than k parts). We again have a bijection yielding the result.

2 Generating Functions

In order to make some more progress in our study of integer partitions, we shall require a very powerful combinatorial tool for the study of sequences, namely the notion of a *generating function* (abbreviated GF). The GF of a sequence a_n is defined as the power series

$$G_a(x) := \sum_{n \geq 0} a_n x^n.$$

From an analytical standpoint, the manipulations we are going to make on such series would need justification on issues such as convergence and well-definedness. To avoid such problems and simplify our proofs, we shall introduce

what is known as *formal power series*⁶, which, in effect, remove any notion of convergence while still retaining the properties which we need for our study and thus make our operations rigorous. Taking the set of complex (even though we will only need integer) sequences $\mathbb{C}^{\mathbb{N}_0}$, we can set operations of addition $(a_n)_n + (b_n)_n := (a_n + b_n)_n$ and multiplication $(a_n)_n \cdot (b_n)_n := (\sum_{k=0}^n a_k b_{n-k})_n$ and obtain the ring $\mathbb{C}[[x]]$ of formal power series⁷. By setting x as the sequence $(a_n)_n$ for which $a_1 = 1$ and all the other members are 0, we see that x^k is the sequence $(b_n)_n$ with $a_k = 1$ and the rest 0, which rigorously justifies our notation⁸ $\sum_{n \geq 0} a_n x^n$ for an arbitrary sequence $(a_n)_n$. We can carry on by defining the reciprocal $G_a(x)^{-1}$ of a power series in the natural way: the unique power series such that $G_a(x)^{-1} G_a(x) = 1$, which exists if and only if $a_0 \neq 0$ (using our definition of series multiplication gives us a recurrence relation for calculating the coefficients of $G_a(x)^{-1}$). Given this definition, we can now calculate familiar identities formally, such as $\sum_{n \geq 0} x^n = \frac{1}{1-x}$. To end this brief discussion of formal power series, note that we can also define:

- Differentiation, as $G'_a(x) = \sum_{n \geq 1} n x^{n-1}$.
- Infinite sums of power series (while we avoid summing an infinite number of coefficients) which allows us to define substitution as $G_a(G_b(x)) = \sum_{n \geq 0} a_n G_b(x)^n$ as long as $b_0 = 0$ so that $G_b(x)^n$ only involves powers of x greater than n — as such, only a finite number of terms contribute to x^k for every k and the substitution makes sense.
- Infinite products of power series of the form $G_k(x) = 1 + f_k(x)$ where f_k is a member of a sequence of formal power series and has the first k terms equal to 0. In this case, we evaluate the product $\prod_{k \geq 1} G_k(x) = \prod_{k \geq 1} (1 + f_k(x))$ by choosing either 1 or a term from $f_k(x)$ from each bracket and counting up the contribution to x^n in the final product (for this to make sense, we specify that we chose 1 from all brackets except a finite subset and because of the restriction on the first terms of $f_k(x)$ we will only have to deal with finite sums contributing to a fixed x^n).

3 Applying Generating Functions to Partitions

Now that we have shown what generating functions are, let us start using them to study integer partitions. Let $p(n)$ denote the number of *unrestricted partitions* of n , i.e. partitions where the parts can be any positive integer⁹. This is the most general type of integer partition and possibly also the most important and

⁶We loosely follow the exposition in [3] and [6] for our explanation.

⁷Note that it contains a subring isomorphic to the ring of complex polynomials $\mathbb{C}[x]$.

⁸We call this the generating function of $(a_n)_n$ but in our formal definition it is actually equal to it.

⁹We set $p(0) = 1$, the “empty partition”.

challenging. As an example, the unrestricted partitions of 6 are:

$$\begin{array}{ll}
 6 = 6 & 6 = 3 + 2 + 1 \\
 6 = 5 + 1 & 6 = 3 + 1 + 1 + 1 \\
 6 = 4 + 2 & 6 = 2 + 2 + 2 \\
 6 = 4 + 1 + 1 & 6 = 2 + 2 + 1 + 1 \\
 6 = 3 + 3 & 6 = 2 + 1 + 1 + 1 + 1 \\
 6 = 1 + 1 + 1 + 1 + 1 + 1 &
 \end{array}$$

and hence $p(6) = 11$. There is no known simple closed formula for $p(n)$ (which gives a hint of how complicated the general problem can be) but Hardy and Ramanujan have found the beautiful asymptotic estimate $p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$ by using a complex analytical technique known as the *circle method*.

The key observation we need to make here is¹⁰:

$$\sum_{n \geq 0} p(x) = \prod_{k \geq 1} (1 + x^k + x^{2k} + x^{3k} + \dots),$$

which we can write as

$$\sum_{n \geq 0} p(x) = \prod_{k \geq 1} \frac{1}{1 - x^k}$$

by summing the (formal) geometric series.

Let us pause for a moment and see why this is true: according to the rule we have specified above for computing infinite products for generating functions (note that the series of GFs does fit the criteria we have set), we're picking a member out of each bracket. We must hence evaluate the contribution to x^n from each possible choice of terms from the brackets: if we see the k^{th} bracket as containing the possible choices of k as a part in the partition (and choosing $x^m k$ out of the bracket if we want m parts equal to k), we see that every possible choice of brackets corresponds to a partition of n and contributes 1 to the coefficient of x^n in the series on the left-hand side. As an example, if we want to represent the partition $6 = 4 + 1 + 1$ above, we would take x^2 from the first bracket (corresponding to having the summand 1 twice), x^4 from the fourth bracket (corresponding to once the summand 4) and 1 from all the others (for a product of $x^2 x^4 = x^6$). As there is one product for every such partition and each of them contributes 1 to the coefficient of x^n , we get that this coefficient is none other than $p(n)$.

What makes this identity even more remarkable is that, given our way of obtaining it, it's extremely easy to generalise it to functions counting partitions with some restrictions. For instance, let $p_e(n)$ and $p_o(n)$ represent the number of partitions into even and odd parts respectively, then their generating functions are clearly $\prod_{k \geq 1} \frac{1}{1 - x^{2k}}$ and $\prod_{k \geq 1} \frac{1}{1 - x^{2k-1}}$: since $\frac{1}{1 - x^k} = (1 + x^k + x^{2k} + x^{3k} + \dots)$ accounts for the appearances of the summand k in a potential partition, removing it from the product removes the contributions from those given partitions to the coefficient of x^n on the left-hand side. Thus, in general, if we want to

¹⁰See [2, Chap 29] and [4, Chap XIX] for example — this appears in almost all of our sources however.

consider only partitions from a given set $S \subseteq \mathbb{N}$ and letting $p_S(n)$ be the number of such partitions of n , we have:

$$\sum_{n \geq 0} p_S(x) = \prod_{k \in S} (1 + x^k + x^{2k} + x^{3k} + \dots) = \prod_{k \in S} \frac{1}{1 - x^k}.$$

It's also very easy to restrict the number of parts in the partition: since the powers higher than k in the k^{th} bracket represent taking the part k multiple times, removing the power x^{mk} disallows partitions which feature the summand k m times. For instance, letting $p_d(n)$ represent the number of partitions into distinct parts (i.e. none of which are equal to one another), we have $\sum_{n \geq 0} p_d(n) = \prod_{k \geq 1} (1 + x^k)$ (each term means that we can either chose to include the part k either once or not at all).

To provide a first example of the power of these techniques, we can use them to prove the uniqueness of the base b expansion in an easy and elegant way.

Theorem. *The base b expansion $n = \sum_{k=0}^N a_k b^k$ with $a_k \in \{1, 2, \dots, b-1\}$ of a natural number n is unique.*

Proof. We need to consider the partitions into powers of b while allowing at most $b-1$ repetitions of every power (naming $p_b(n)$ the number of such partitions of a number n), hence the generating function will be given by

$$\sum_{n \geq 1} p_b(x) = x^n \prod_{k \geq 0} (1 + x^{b^k} + x^{2b^k} + \dots + x^{(b-1)b^k}).$$

But, summing up the finite geometric sum, we get:

$$\sum_{n \geq 1} p_b(x) = \prod_{k \geq 0} \frac{1 - (x^{b^k})^b}{1 - x^{b^k}} = \prod_{k \geq 0} \frac{1 - x^{b^{k+1}}}{1 - x^{b^k}} = \frac{1}{1 - x},$$

since every $1 - x^{b^k}$ denominator cancels out with a $1 - x^{b^{k+1}}$ numerator except for the $k = 0$ one. Equating coefficients, we get $p_b(n) = 1$ for all n and we are done. \square

Let us try to use a similar technique on the number of distinct partitions of a number and see what we obtain. We have:

$$\sum_{n \geq 0} p_d(n) = \prod_{k \geq 1} (1 + x^k) = \prod_{k \geq 1} \frac{1 - x^{2k}}{1 - x^k} = \prod_{k \geq 1} \frac{1}{1 - x^{2k-1}},$$

where we have again summed up the (two term) finite geometric sum and canceled out the numerators when possible. Recalling the generating function for the number of partitions into odd parts, we see that we have just proven that $p_d(n) = p_o(n)$ by proving that their generating functions are equal! It is interesting to see a proof by bijection of this result as well and we have taken the very elegant one by J.W.L. Glaisher from [2]¹¹:

Proof. Consider a partition of n into odd parts

$$\lambda : n = \underbrace{\lambda_1 + \dots + \lambda_1}_{n_1} + \underbrace{\lambda_2 + \dots + \lambda_2}_{n_2} + \dots + \underbrace{\lambda_\ell + \dots + \lambda_\ell}_{n_\ell}$$

¹¹Also available in [4].

and write the n_i in their binary representation as $n_i = 2^{m_{i,1}} + 2^{m_{i,2}} + \dots + 2^{m_{i,r}}$. We can now write another partition

$$\lambda' : 2^{m_{1,1}} \lambda_1 + 2^{m_{1,2}} \lambda_1 + \dots + 2^{m_{1,r}} \lambda_1 + 2^{m_{2,1}} \lambda_2 + \dots + 2^{m_{\ell,r}} \lambda_\ell$$

as if we were expanding the binary sums.

We claim that the function $f : \lambda \mapsto \lambda'$ is a bijection from the set of partitions into odd parts onto the set of partitions into distinct parts. We need to first check that λ' is indeed a partition of the latter type and this is easy since $2^a \lambda_i = 2^b \lambda_j$ implies $a = b$ (as the λ are odd) and thus $\lambda_i = \lambda_j$, which proves that the parts are distinct. To prove that this is a bijection we need only specify a way of reversing it: considering a partition into distinct parts $\mu : n = \mu_1 + \mu_2 + \dots + \mu_s$, write each part as a power of 2 times an odd number and group together the parts with the same odd component. Now, these odd components will be our odd parts for the partition into odd numbers and summing up the powers of two we obtain the multiplicity of each: we have found an inverse for f which proves that it is indeed a bijection and we are done! \square

4 Euler's Pentagonal Number Theorem

One of the most strikingly beautiful identities relating to partitions is known as *Euler's pentagonal number theorem*. Before coming to the statement of the theorem, let us start by considering what happens if we include a second variable in the generating function for the number of distinct partitions as follows:

$$\prod_{k \geq 1} (1 + yx^k) = \sum_{n \geq 0} p_d^{(m)}(n) x^n y^m,$$

where $p_d^{(m)}(n)$ denotes the number of partitions of n into m distinct parts. We thus see that the variable y serves as a counter for the number of parts of the partition. Letting¹² $y = -1$ we get the identity:

$$\prod_{k \geq 1} (1 - x^k) = \sum_{n \geq 0} (p_{d,e}(n) - p_{d,o}(n)) x^n,$$

where $p_{d,e}(n)$ and $p_{d,o}(n)$ are the number of partitions into distinct even, resp. distinct odd, parts of n . As such, if we were to find an expression for the coefficients of the first product, we could see the relationship between the number of distinct odd and even parts of a given non-negative integer. Computing the first few terms of the expansion, we get:

$$\prod_{k \geq 1} (1 - x^k) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + x^{57} + \dots$$

We can see that the coefficients are either 0, 1 or -1 and that the non-zero ones come in pairs of two negatives and two positives (except for x^0). Taking the first exponent in each such pair gives us a well known sequence: that of

¹²Although we are assigning a numerical value to a variable here, the identity remains a formal one since the formal variable was x and since we are not summing over m there are no convergence issues to worry about.

the pentagonal numbers (which are obtained in a way analogous to the more well-known triangular numbers). The formula for the n^{th} pentagonal number is $f(n) = \frac{1}{2}(3n^2 - n)$ while the second number in every pair is $\bar{f}(n) = \frac{1}{2}(3n^2 + n)$. We are now ready to state and prove¹³ *Euler's pentagonal number theorem*:

Theorem.
$$\prod_{k \geq 1} (1 - x^k) = 1 + \sum_{n \geq 1} (-1)^n (x^{f(n)} + x^{\bar{f}(n)})$$

Proof. We will carefully set up another bijection between sets of partitions which will yield our desired identity. Notice that the product on the left side is the exact multiplicative inverse of our generating function for unrestricted partitions. Thus, letting $a(n)$ be the coefficient of x^n for our product when expanding it as a formal power series, we have:

$$\left(\sum_{n \geq 1} a(n)x^n \right) \cdot \left(\sum_{n \geq 1} p(n)x^n \right) = 1$$

which, according to the formula for multiplication of formal power series, means that $a(0) = 1$ and

$$\sum_{k=0}^n a(k)p(n-k) = 0 \quad \text{for } n \geq 1. \quad (1)$$

Now, looking at our right-hand side expression in Euler's identity, we would need to prove that:

$$a(k) := \begin{cases} 1 & \text{if } k = \bar{f}(i) = \frac{1}{2}(3i^2 + i) \text{ with } i \in \mathbb{Z} \text{ even,} \\ -1 & \text{if } k = \bar{f}(i) = \frac{1}{2}(3i^2 + i) \text{ with } i \in \mathbb{Z} \text{ odd,} \\ 0 & \text{otherwise,} \end{cases}$$

where we let $i \in \mathbb{Z}$ so that $\bar{f}(i)$ can encompass both the $f(i)$ exponents and the $\bar{f}(i)$ ones. Hence, substituting these values for $a(n)$ and k in (1), we have that Euler's identity is equivalent to:

$$\sum_{i \text{ even}} p(n - \bar{f}(i)) = \sum_{i \text{ odd}} p(n - \bar{f}(i))$$

where $i \in \mathbb{Z}$ ranges over even or odd values such that $\bar{f}(i) \leq n$. Setting $\mathcal{P}(n)$ as the set of partitions of n , we see that all we require in order to prove the theorem is to find a bijection φ from $\bigcup_{i \text{ even}} \mathcal{P}(n - \bar{f}(i))$ to $\bigcup_{i \text{ odd}} \mathcal{P}(n - \bar{f}(i))$ and for this $\varphi : \lambda \mapsto \lambda'$, where we have $\lambda : n - \bar{f}(i) = \lambda_1 + \lambda_2 + \cdots + \lambda_\ell$ and

$$\lambda' : \begin{cases} n - \bar{f}(i-1) = (\ell + 3i - 1) + (\lambda_1 - 1) + \cdots + (\lambda_\ell - 1) & \text{if } \ell + 3i \geq \lambda_1, \\ n - \bar{f}(i+1) = (\lambda_2 + 1) + \cdots + (\lambda_\ell + 1) + \underbrace{1 + \cdots + 1}_{\lambda_1 - \ell - 3i - 1} & \text{if } \ell + 3i < \lambda_1 \end{cases}$$

¹³The standard proof of the theorem which appears in [1] [3], [4] and [6] relies on Ferrers diagrams and is an excellent proof in its own right but we have chosen to use the one in [2] instead which is slightly less direct but even shorter and more elegant in the opinion of the author.

will do the job! One can easily check that this function is not only a bijection but an involution (in the case where we apply the function again to the first case, using the second case on it as required, we get our original partition back and vice-versa in the other case). \square

Reinterpreting this result in terms of partitions into distinct odd and even parts again, we have just proved the very elegant result that there are as many partitions into distinct odd parts of n as there are into distinct even parts, unless $n = \bar{f}(i)$ with $i \in \mathbb{Z}$, in which case there will be one more partition into distinct even parts if i is even and one more partition into odd parts if i is odd!

5 Sums of Integer Powers

We now turn for the remainder of this essay to some classical problems in additive number theory. Up to this point, the existence of the different representations into sums of integers was always a trivial fact. The questions which we shall study now are less concerned with the exact number of representations as before (though this is still an interesting problem) as they are with guaranteeing the existence of at least one such representation. A classical conjecture in number theory, the famous *Goldbach Conjecture*, can be seen as an example of this type of problem: we are looking for the existence of a representation of the form $n = p + q$ for every even positive integer n greater than 4, where p and q are odd primes. While this kind of problem is extremely interesting, it is also among the hardest unsolved problems in mathematics: the closest we have gotten to it are two theorems known as Vinogradov's theorem and Chen's theorem, the former stating that any sufficiently large odd integer is a sum of at most 3 odd primes and the latter that every sufficiently large integer is a sum of a prime and a prime or a product of two primes; both of these theorems relying on fairly advanced number theoretic results [1, Chap. 14].

The first problem which we shall consider is a much easier one but no less elegant: which numbers can be written as sums of squares? Starting with sums of two squares, we first prove a famous result known as *Fermat's two squares theorem*:

Theorem. *Every odd prime $p \equiv 1 \pmod{4}$ can be written as a sum of two squares*

It is easy to see that this theorem is the best possible: odd primes p are either $1 \pmod{4}$ or $3 \pmod{4}$ and since a square is necessarily 0 or $1 \pmod{4}$, a sum of two squares can never be congruent to $3 \pmod{4}$. Our proof of this theorem is taken from [2, Chap. 4] and is delightfully simple and surprising at the same time:

Proof. Consider the set \mathcal{S} of solutions $(x, y, z) \in \mathbb{Z}^3$ to the Diophantine equation $4xy + z^2 = p$ with $x, y \geq 1$ and p a fixed odd prime with $p \equiv 1 \pmod{4}$. This set is finite since we have $z^2 \geq 0$ and $x, y \geq 1$, which implies that $x, y \leq p/4$ and given a choice of x and y there are at most two possible choices for z . The proof relies on 3 different linear involutions on \mathcal{S} , each of which will give us a bit of information needed to prove our theorem.

The first involution is defined as $\varphi : \mathcal{S} \rightarrow \mathcal{S}$, $(x, y, z) \mapsto (y, x, -z)$. Note that this map has no fixed points, as one such fixed point would require $z = 0$ which

would imply $p = 4xy$, a contradiction given that p is prime. Defining subsets \mathcal{T} and \mathcal{U} of \mathcal{S} as $\mathcal{T} := \{(x, y, z) \in \mathcal{S} : z > 0\}$ and $\mathcal{U} := \{(x, y, z) \in \mathcal{S} : x - y + z > 0\}$, we see that φ maps these subsets to their complements in \mathcal{S} . But then φ also maps $\mathcal{T} \setminus \mathcal{U}$ to $\mathcal{U} \setminus \mathcal{T}$ bijectively, which means that $|\mathcal{T}| = |\mathcal{U}|$.

The second map which we consider is $\psi : \mathcal{U} \rightarrow \mathcal{U}$, $(x, y, z) \mapsto (x - y + z, y, 2y - z)$. We have that $4(x - y + z)y + (2y - z)^2 = 4xy + z^2 = p$, so this is indeed a map from \mathcal{S} to \mathcal{S} and since $(x - y + z) - y + (2y - z) = x > 0$ it is, as claimed, from \mathcal{U} to \mathcal{U} . Also, we can easily check it's an involution as well, since $(\psi \circ \psi)(x, y, z) = ((x - y + z) - y + (2y - z), y, 2y - (2y - z)) = (x, y, z)$. Lastly, the map has exactly one fixed point: $\psi(x, y, z) = (x, y, z)$ implies $(x - y + z, y, 2y - z) = (x, y, z)$, for which we need $y = z$; but then we have $p = 4xy + y^2 = y(4x + y)$ and since p is a prime we get require $y = 1$. As such, we get the lone fixed point $(\frac{p-1}{4}, 1, 1)$ and this tells us that $|\mathcal{U}|$ is odd: the involution maps every point to a different one (and back, since it is an involution) except the fixed point, resulting in a partition of \mathcal{U} into a number of pairs and a single point.

Finally, the third involution we shall call upon is $\theta : \mathcal{T} \rightarrow \mathcal{T}$, $(x, y, z) \mapsto (y, x, z)$. Knowing from the two other maps that $|\mathcal{T}| = |\mathcal{U}|$ and that $|\mathcal{U}|$ is odd, we can conclude that $|\mathcal{T}|$ itself is odd and thus θ has at least one fixed point (if not, we would be able to partition \mathcal{T} into pairs of elements). But a fixed point of θ implies a solution $(x, y, z) \in \mathcal{S}$ with $x = y$ which means that $p = 4x \cdot x + z^2 = (2x)^2 + z^2$, which ends the proof. \square

Once we have proven this, it is rather easy to see that the natural numbers which are representable by a sum of two squares are exactly those for which every prime factor p congruent to $3 \pmod{4}$ appears with an even exponent in their prime factorisation. Indeed, knowing that $1 = 0^2 + 1^2$, $2 = 1^2 + 1^2$ and every prime $p \equiv 1 \pmod{4}$ are representable as sums, combined with the facts that:

- for every number $n = x^2 + y^2$ that is representable as a sum of two squares and a given integer m , $m^2 \cdot n = (mx)^2 + (my)^2$ is also representable,
- given any two representable numbers $n = x^2 + y^2$ and $m = w^2 + z^2$, their product $nm = (xw + yz)^2 + (xz - yw)^2$ is also representable,

yield that every number satisfying our condition is representable as a sum of two squares. To prove that these are the only such numbers, we can use the fact that if a prime $p \equiv 3 \pmod{4}$ divides a representable number $n = x^2 + y^2$, then p divides both x and y and hence $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ is still representable. To see this, note that if we don't have¹⁴ $x \equiv 0 \pmod{p}$, then we can find x^{-1} such that $xx^{-1} \equiv 1 \pmod{p}$ (as \mathbb{Z}_p is field for prime p) and hence multiply $x^2 + y^2 \equiv 0 \pmod{p}$ by x^{-2} to get $y^2x^{-2} \equiv -1 \pmod{p}$ which is impossible since -1 is not a quadratic residue mod p for primes $p \equiv 3 \pmod{4}$ [5, p. 126]. This is of course a contradiction if p appears with an odd exponent in the prime factorisation of n since we would be able to keep dividing by p^2 ad infinitum and still get representable integers.

We could now ask ourselves, as we did for the integer partitions in the previous sections, how many representations into such sums of two squares we can find. It turns out, as C. G. Jacobi proved,[1] that if we let $r_2(n)$ be the

¹⁴The same reasoning applies for y .

number of such representations (taking the order into account and allowing negative integers), then we have:

$$r_2(n) = 4(\tau_1(n) - \tau_3(n)),$$

where $\tau_k(n)$ denotes the number of divisors of n that are congruent to $k \pmod 4$. Of course, this result has Fermat's two squares theorem as a corollary: if p is a prime of the form $4k + 1$ we get $r_2(p) = 8$ and if it is of the form $4k - 1$ we get $r_2(p) = 0$.

The problem of sums of three squares is less well known and somewhat harder. We shall not explore the subject in detail but Gauss proved that an integer is a sum of three squares if and only if it is not of the form $4^n(8m - 1)$ for integers n and m . Interestingly, this is linked to another theorem of Gauss showing that every natural number can be expressed as a sum of three triangular numbers, which in fact settles a case of another conjecture of Fermat, which states that every number is a sum of at most k k -gonal numbers¹⁵. As Fermat's conjecture suggests, it is indeed true that all natural numbers can be written as sums of at most four squares: this is *Legendre's four square theorem*.

The next step would be seeing if we can find similar results for higher powers. This is in fact a fairly large area of partly unsolved mathematics all relating to what is known as Waring's Problem, which generalises Legendre's theorem for higher powers[4][1]:

Theorem. *There exists a number $g(k)$ such that any natural number n is expressible as a sum $n = x_1^k + x_2^k + \dots + x_{g(k)}^k$ of $g(k)$ k^{th} powers.*

This was conjectured by Waring in 1770, who had empirically noted that every positive integer seems to be the sum of at most 4 squares, 9 cubes, 19 fourth powers and so on. Of course, Lagrange's four square theorem provides the affirmative answer $g(2) = 4$ but it was not until 1909 that Hilbert proved the existence of $g(k)$ for every k . The values of $g(k)$ have since been found for a wide variety of numbers (indeed, those which Waring initially conjectured do hold) and recent developments[7] have shown that in fact $g(k) = 2^k + \left\lfloor \frac{3^k}{2^k} \right\rfloor - 2$ for a large number of values¹⁶ of k and, in fact, this holds for all large enough k .

A harder and more fundamental problem, which has been first put forth in the work of Hardy and Littlewood, is the asymptotic one[4]: finding the related quantity $G(k)$ such that all but a finite number of positive integers can be expressed as a sum of at most $G(k)$ k^{th} powers. This is because very often only a few small numbers require more powers than the rest: as an example, in the case of $k = 3$, it is known that only two numbers require 9 cubes and only 15 more require 8, while the actual value of $G(3)$ is smaller or equal to 7. As such, these small numbers can be seen as rather meaningless special cases, making the problem of finding $G(k)$ a more interesting one than that of finding $g(k)$. Unfortunately, the exact value of $G(k)$ is not known for any k except 2 (it is clear by the previous paragraph that $G(2) = g(2) = 4$) and 4 (for which $G(4) = 16$). We do, however, have a number of bounds on $G(k)$, both in general

¹⁵We can generalise the triangular, square and pentagonal numbers to sequences depicting "polygons" of any number of vertices. The full conjecture was later proven by Cauchy.

¹⁶This has been verified for $3 \leq k \leq 47160000$.

and for specific values of k . The best currently known bounds for $k = 5, \dots, 16$ are 17, 21, 33, 42, 50, 59, 67, 76, 84, 92, 100, 109 while the known values of $g(k)$ for these k are 37, 73, 143, 279, 548, 1079, 2132, 4223, 8384, 16673, 33203, 66190, showing how small $G(k)$ is in comparison to $g(k)$ for these values and illustrating our earlier claim that finding $G(k)$ is the more fundamental problem. Hardy and Littlewood themselves have established that $G(k) \leq 2^{k-1}k - 2^k + 5$ and, building upon their methods, Vinogradov later showed that $G(k) \leq 3k \log(k) + 11k$. Even so, we are still very far away from finding the values of $G(k)$ both in general and in these examples.

This concludes our rather brief overview of these fascinating topics in additive number theory. We hope that it has been possible to show in these few pages not only how enjoyable and surprising the theory and results can be but also how open and active this area remains.

References

- [1] T. APOSTOL: *An Introduction to Analytic Number Theory*, Springer-Verlag (1976).
- [2] M. AIGNER & G. M. ZIEGLER: *Proofs from THE BOOK*, Third edition, Springer-Verlag (2004).
- [3] P. J. CAMERON: *Combinatorics: Topics, Techniques and Algorithms*, Cambridge University Press (1994).
- [4] G. H. HARDY & E. M. WRIGHT: *An Introduction to the Theory of Numbers*, Fifth edition, Oxford University Press (1979).
- [5] G. A. JONES & J. M. JONES: *Elementary Number Theory*, Springer-Verlag (1998).
- [6] J. H. VAN LINT & R.M. WILSON: *A Course in Combinatorics*, Second Edition, Cambridge University Press (2001).
- [7] M. WALDSCHMIDT: *Open Diophantine Problems*, arXiv.org (2004), <http://arxiv.org/abs/math/0312440v2>.