Section 18. Sums of Two Squares

Note. In this section, we classify the integers that can be written as the sum of two squares. For example, $1 = 0^2 + 1^2$, $2 = 1^2 + 1^2$, $4 = 0^2 + 2^2$, $5 = 1^2 + 2^2$, $8 = 2^2 + 2^2$, $9 = 0^2 + 3^2$, $10 = 1^2 + 3^2$, $13 = 2^2 + 3^2$, etc. The conditions under which such a representation of n exists depends on the prime-power decomposition of n.

Note. We first prove several lemmas.

Lemma 18.A. If the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares.

Note. We can establish the next result by simply multiplying out.

Lemma 18.1. For any integers a, b, c, d, we have $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.

Note 18.A. Lemma 18.1 shows that the product of two numbers that can be written as a sum of two squares, itself can be written as a sum of two squares. By mathematical induction, we have that the product of a finite collection of numbers that can be written as a sum of squares, itself can be written as a sum of squares

Definition. Positive integer n is *representable* if it is the sum of two squares of integers.

Note. Notice that if $n = x^2 + y^2$ then for any k we have

$$k^2 n = k^2(x^2 + y^2) = (kx)^2 + (ky)^2.$$

We summarize this in the next result.

Lemma 18.2. If n is representable, the so is $k^2 n$ for an k.

Exercise 18.2. We can illustrate the use of Lemmas 18.1 and 18.2 by representing 325 as a sum of two squares. First, $325 = 5^2 \cdot 13$. So by Lemma 18.2, if we can write 13 as a sum of two squares, then we have a solution. As observed above, $13 = 2^2 + 3^2$. So we have $325 = 5^2(2^2 + 3^2) = 5^2 2^2 + 5^2 3^2 = \boxed{10^2 + 15^2}$. □

Lemma 18.3. Any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$, were k is an integer and the p's are different primes.

Exercise 18.3. If the prime-power decomposition of n contains no prime p, where $p \equiv 3 \pmod 4$, to an odd power, then $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p is congruent to 1 (mod 4).

Lemma 18.4. Every prime congruent to 1 (mod 4) can be written as a sum of two squares.

Theorem 18.1. Integer n cannot be written as the sum of two squares if and only if the prime-power decomposition of n contains a prime congruent to 3 (mod 4) to an odd power.

Note. Dudley's proof of Lemma 18.4 is based on Fermat's infinite descent, instead of the minimality assumption of k that we presented. The process is the same and we computed $k_1 < k$ in our proof as well (whereas Dudley uses $k_1 < k$ to employ Fermat's infinite descent, we used it to prove that $k = 1$). As an illustration of Dudley's proof technique, consider the expression of $145 = 5 \cdot 29$ as a sum of two squares: $1^2 + 12^2 = 145$. From this, we can find an expression of $p = 29$ as a sum of two squares. Notice that prime $p = 29 \equiv 1 \pmod 4$. So we take $k = 5$, $x = 12$, and $y = 1$. We need $r \equiv x \pmod k$ and $s \equiv y \pmod k$ such that r and s are in the interval $(-k/2, k/2]$; that is, we need $r \equiv 12 \pmod 5$ and $s \equiv 1 \pmod 5$ in $(-5/2, 5/2]$. So we take $r = 2$ and $s = 1$. Then by Lemma 18.1,

$$5^2 \cdot 29 = (2^2 + 1^2)(12^2 + 1^2) = (2 \cdot 12 + 1 \cdot 1)^2 + (2 \cdot 1 - 1 \cdot 12)^2 = 25^2 + 10^2.$$

Dividing by $k^2 = 25$ gives $29 = 5^2 + 2^2$, as sought. Here, $x_1 = (rx + sy)/k = (2 \cdot 12 + 1 \cdot 1)/5 = 5$ and $y_1 = (ry - sx)/k = (2 \cdot 1 - 1 \cdot 12)/5 = -2$, consistent with the result here.

Note. Having classified which integers can be represented as a sum of two squares, we can look to generalize this in a number of ways. We might consider (as Dudley declares "natural now to wonder" on page 146) which integers have representations as the sum of three squares. Adrien-Marie Legendre (September 18, 1752–January

9, 1833) proved that any nonnegative integer n can be represented as a sum of three squares, $n = x^2+y^2+z^2$, if and only if n is not of the form $4^e(8k+7)$ for some integers e and k. His result appears in *Essai sur la théorie des nombres*, Paris, An VI (1797-1798), pages 202 and 398-399. A more brief proof can be found in N. C. Ankeny's "Sums of Three Squares," *Proceedings of the American Mathematical Society*, **8**(2), 316–319 (1957), available on the AMS website (accessed 3/23/2022). Ankeny's proof is based on results in these notes (quadratic reciprocity which we covered in Section 12. Quadratic Reciprocity and Dirichlet's Theorem which appears as Theorem 22.B in Section 22. Formulas for Primes), plus "Minkowski's Theorem on lattice points within convex symmetric bodies." Continuing in this direction of inquiry, we could consider the integers which can be represented as a sum of four squares, $n = w^2 + x^2 + y^2 + z^2$. In the next section, Section 19. Sums of Four Squares, we show that every nonnegative integer can be represented as a sum of four squares (see Theorem 19.1).

Note. We seem to have skipped cubes. Backing up to the case of cubes, we might ask how many cubes of nonnegative integers, s, does it take to insure that every positive integer is a sum of s cubes? The correct answer is 19. This was partially shown in Arthur Wieferich's "Beweis des Satzes, daßsich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt," *Mathematische Annalen*, **66**, 95-101 (1909). Unfortunately, Wieferich made some computational errors, but these were corrected by A. J. Kempner in "Bemerkungen zum Waringschen Problem," *Mathematische Annalen*, **72**, 387-399 (1912); this history can be found in L. E. Dickson's "Simpler Proofs of Warings Theorem of Cubes, With Various General-

izations," *Transactions of the American Mathematical Society*, **30**(1), 1–18 (1928), available online on the AMS website (accessed 3/23/2022). The general problem of finding the least value s such that every nonnegative integer can be represented as a sum of no more then s kth powers is known as *Waring's Problem*. It is named for British mathematician Edward Waring (circa 1736–August 15, 1798), who stated it in his 1770 *Meditationes Algebraicae*, where he conjectured that every nonnegative integer is the sum of four squares (as we see in the next section), as the sum of nine cubes (as shown by Wieferich and Kempner) and as a sum of nineteen fourth powers. The claim for fourth powers was shown by R. Balasubramanian, J. M. Deshouillers, and F. Dress in "Problème de Waring pour les bicarrés. I. Schéma de la solution" [Waring's problem for biquadrates. I. Sketch of the solution], *Comptes Rendus de l'Académie des Sciences, Série I*, **303**(4), 85-88 (1986) and "Problème de Waring pour les bicarrés. II. Rsultats auxiliaires pour le théorème asymptotique" [Waring's problem for biquadrates. II. Auxiliary results for the asymptotic theorem], *Comptes Rendus de l'Académie des Sciences, Série I*, **303**(5), 161-163 (1986). Representing parameter s as $g(k)$, where k is the exponent, these results state that $g(2) = 4$, $g(3) = 9$, and $g(4) = 19$. Wikipedias's Waring's Problem webpage (accessed 3/23/2022) lists other values of $g(k)$ and gives references on studies of bounds which have been put on the quantity $G(k)$. This function $G(k)$ is defined as the least value of s such that every *sufficiently large* nonnegative integer can be written as a sum of no more than s kth powers. There are still unproved conjectures related to these values $g(k)$ and $G(k)$.

Note. A related conjecture deals with sums of prime numbers. Prussian mathematician Christian Goldbach (March 18, 1690–November 20, 1764) wrote a letter to Leonhard Euler on June 7, 1742 and conjectured that every even integer greater than 2 can be written as the sum of two primes. This is one of the oldest unproved conjectures in number theory (and also one of the easiest to state). This has been computationally confirmed for nonnegative integers up to 4×10^1) (according to the Goldbach Conjecture Verification website; accessed 3/23/2022). Goldbach's Weak Conjecture (also called the Ternary Goldbach Conjecture) claims that every odd number greater than 5 can be expressed as the sum of three (not necessarily distinct) primes. This conjecture has an ETSU connection. In 2013, Harald Helfgott proposed a proof that was accepted for publication in *Annals of Mathematics Studies* (in 2015), but which has apparently not yet appeared. A Google search indicates that the latest available work on this is from 2015 and is available on arXiv.org: The Ternary Goldbach Problem (this is a 327 page document; accessed 2/28/2022). The ETSU connection is that Harald Helgott is the son of former ETSU Department of Mathematics and Statistics faculty members Drs. Edith Seier and Michel Helfgott (both retired in the late 2010s). More details on Goldbach's Conjecture are in my online notes for Mathematical Reasoning (MATH 3000) on Section 6.9. Perfect Numbers, Mersenne Primes, Arithmetic Functions.

Revised: 4/20/2022