Thue's lemma in $\mathbb{Z}[i]$ and Lagrange's four-square theorem

Paul Pollack

Abstract. Without question, two of the most significant results of pre-19th century number theory are (a) Fermat's theorem that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, and (b) Lagrange's theorem that every positive integer is a sum of four squares. Today, several proofs are known for both of these theorems. Perhaps the simplest proof of Fermat's theorem uses a beautiful combinatorial lemma of Axel Thue: For any a and m, the congruence $ax \equiv y \pmod m$ has a "small" solution x, y other than the trivial solution $(0,0)$. Here "small" means that $|x|, |y| \le \sqrt{m}$. In 2010, Jameson gave a short, simple proof of Lagrange's theorem based on an extension of Thue's lemma to the Gaussian integers. Here we show how using a bit more of the arithmetic of $\mathbb{Z}[i]$ allows one to give a conceptually simpler proof based on these same ideas.

1. Introduction.

Lagrange's 1770 theorem that every positive integer is a sum of four squares seems destined to stand the test of time as one of the most beautiful results in number theory. In 2010, Jameson [**4**] gave a simple, short proof of this theorem based on the following Gaussian integer analogue of a 1902 lemma of Thue [**6**]. (A modern reference for the lemma, over $\mathbb{Z}$, is [**1**, Chapter 4], where it is used to give a "book proof" of Fermat's two-square theorem.) Recall that the *norm* $N\alpha$ of a Gaussian integer α is defined as $\alpha\bar{\alpha}$; equivalently, if $\alpha = a + bi$, then $N\alpha = a^2 + b^2$. Put $\|a + bi\| = \max\{|a|, |b|\}$.

Thue's lemma in $\mathbb{Z}[i]$. *Let μ be a nonzero Gaussian integer. For every $\alpha \in \mathbb{Z}[i]$, there are $\beta, \gamma \in \mathbb{Z}[i]$ with*

$$\alpha\beta \equiv \gamma \pmod{\mu}$$

and

$$\|\beta\|, \|\gamma\| \le \sqrt[4]{N\mu}. \tag{1}$$

Proof. We let $\tilde{\beta}$ and $\tilde{\gamma}$ range independently over all Gaussian integers $A+Bi$ and $C + Di$ with $0 \le A, B, C, D \le \sqrt[4]{N\mu}$. There are $(1 + \lfloor \sqrt[4]{N\mu} \rfloor)^4 > N\mu$ such pairs $(\tilde{\beta}, \tilde{\gamma})$. But, as is well-known, $\#\mathbb{Z}[i]/(\mu) = N\mu$ (see [**5**, Proposition 1, p. 52] for a more general statement). Hence, there are two distinct pairs $(\tilde{\beta}, \tilde{\gamma})$ for which the residue classes of $\alpha\tilde{\beta} - \tilde{\gamma}$ modulo μ coincide. If these are $(\tilde{\beta}_1, \tilde{\gamma}_1)$ and $(\tilde{\beta}_2, \tilde{\gamma}_2)$, then the conclusion of the lemma holds with $\beta = \tilde{\beta}_1 - \tilde{\beta}_2$ and $\gamma = \tilde{\gamma}_1 - \tilde{\gamma}_2$. $\square$

The aim of this note is to describe a way of deducing Lagrange's theorem from Thue's lemma that seems slightly more natural than Jameson's.

2. Jameson's proof.

In this section we give our rendition of Jameson's original argument. First, note that to prove the four-square theorem, it is enough to show all *squarefree* m are representable as a sum of four squares.[1] Indeed, if n is any positive integer, we can write $n = r^2 m$ with m squarefree; representing m as a sum of four squares and absorbing the factors of r^2 into the summands gives a corresponding representation of n. In what follows, we focus on representing squarefree m.

To prepare for the application of Thue's lemma, we need the following auxiliary result which features in essentially all of the elementary proofs of Lagrange's theorem.

LEMMA 1. *Let m be a squarefree integer. There is an $\alpha \in \mathbb{Z}[i]$ for which*

$$N\alpha \equiv -1 \pmod{m}.$$

PROOF. Recalling that $N(a+bi) = a^2 + b^2$, our task is that of proving -1 is a sum of two squares in the ring $\mathbb{Z}/m\mathbb{Z}$. By the Chinese remainder theorem, it is enough to show this when $m = p$ is prime. The case $p = 2$ is clear, so we suppose p is odd. Over any field of odd characteristic, $x \mapsto x^2$ is a 2-to-1 map on nonzero elements. Hence, the number of nonzero squares in $\mathbb{Z}/p\mathbb{Z}$ is $\frac{p-1}{2}$, and the total number of squares in $\mathbb{Z}/p\mathbb{Z}$ is $\frac{p+1}{2}$. So if we put

$$\mathcal{S} = \{a^2 : a \in \mathbb{Z}/p\mathbb{Z}\} \quad \text{and} \quad \mathcal{T} = \{-1 - b^2 : b \in \mathbb{Z}/p\mathbb{Z}\},$$

then $\#\mathcal{S} = \#\mathcal{T} = \frac{p+1}{2}$. Since $\#\mathcal{S} + \#\mathcal{T} > \#\mathbb{Z}/p\mathbb{Z}$, the sets $\mathcal{S}$ and $\mathcal{T}$ are not disjoint. Thus, there are $a, b \in \mathbb{Z}/p\mathbb{Z}$ with $a^2 = -1 - b^2$, i.e., $a^2 + b^2 = -1$. $\square$

We are now able to deduce the following.

PROPOSITION 2. *Let m be a squarefree integer. At least one of m, $2m$, and $3m$ is a sum of four squares.*

PROOF. We can assume that $m > 1$. Using Lemma 1, choose $\alpha \in \mathbb{Z}[i]$ with $N\alpha \equiv -1 \pmod{m}$. By Thue's lemma, there are $\beta, \gamma \in \mathbb{Z}[i]$, not both 0, with

$$\alpha\beta \equiv \gamma \pmod{m} \tag{2}$$

and

$$\|\beta\|, \|\gamma\| \le m^{1/2}. \tag{3}$$

Applying complex conjugation to (2) shows that

$$\bar{\alpha}\bar{\beta} \equiv \bar{\gamma} \pmod{m}. \tag{4}$$

Multiplying (2) and (4) and rearranging yields

$$N\beta + N\gamma \equiv 0 \pmod{m}.$$

We claim that $N\beta + N\gamma = m$, $2m$, or $3m$. From the above, it is clear that the integer $N\beta + N\gamma$ is positive (since β and γ do not both vanish) and a multiple of m. Moreover, since m is not a square, the inequalities in (3) are necessarily strict, so that

$$N\beta + N\gamma < 4(m^{1/2})^2 = 4m.$$

Thus, $N\beta + N\gamma = m, 2m$, or $3m$, as claimed. $\square$

[1] Recall that m is said to be *squarefree* when it is a product of distinct prime numbers.

Disappointingly, the conclusion of Proposition 2 is not the representability of m, but the representability of at least one of m, $2m$, and $3m$. When m is represented, we are home free. The case when $2m$ is represented is also OK, in view of the following easy lemma.

LEMMA 3 (2-removal and insertion). *For every positive integer n, we have that n is a sum of four squares $\Longleftrightarrow$ $2n$ is a sum of four squares.*

PROOF. Applying the observation that $(a+b)^2+(a-b)^2 = 2a^2+2b^2$ twice, one arrives at the duplication identity

$$2(x^2+y^2+z^2+w^2) = (x+y)^2+(x-y)^2+(z+w)^2+(z-w)^2. \tag{5}$$

This makes the forward implication of the lemma obvious. For the backward direction, suppose that $2n = X^2+Y^2+Z^2+W^2$ with X, Y, Z, W integers. If x, y, z, w solve the system

$$X = x+y, \quad Y = x-y, \quad Z = z+w, \quad W = z+w,$$

then (5) implies that $x^2+y^2+z^2+w^2 = n$. So n will be a sum of four squares as long as $x, y, z, w \in \mathbb{Z}$. Solving for x, y, z, w explicitly, we see that this last condition is satisifed precisely when $X \equiv Y \pmod 2$ and $Z \equiv W \pmod 2$. Since we may permute X, Y, Z, W, the lemma will be proved if we show that X, Y, Z, W can be put in pairs of the same parity. Now all of X^2, Y^2, Z^2, W^2 are 0 or 1 modulo 4, and their sum is $2n$, which is $\equiv 0$ or 2 modulo 4. If $2n \equiv 0 \pmod 4$, then all of X^2, Y^2, Z^2, W^2 must coincide modulo 4, and so all of X, Y, Z, W are even or all are odd. If $2n \equiv 2 \pmod 4$, then exactly two of X, Y, Z, W are odd. In either case, we can pair X, Y, Z, W as desired. □

Jameson completes his proof by also showing the "3-removal lemma", viz.

$$3n \text{ is a sum of four squares} \Longrightarrow n \text{ is a sum of four squares.}$$

This result has been known for more than 250 years; the simple and short proof Jameson gives appears already in a July 26, 1749 letter from Euler to Goldbach [**3**, pp. 1000–1006]. In fact, the corresponding p-removal lemma is proved in Euler's letter for each of $p = 2, 3, 5$, and 7.

Unfortunately (in the opinion of the author) the proof of the 3-removal lemma rests on the triplication identity

$$3(x^2+y^2+z^2+w^2) = (y+z+w)^2+(z-w+x)^2+(w-y+x)^2+(y-z+x)^2,$$

which cannot be considered obvious to mathematical mortals.[2] This is our primary motivation for staking out a different path.

3. A way around 3-removal.

We now restrict attention to *odd* squarefree m. Rather than show m is representable directly, we will aim at proving the representability of $2m$; we know from Lemma 3 that the two are in fact equivalent.

The essential new idea is to use a wee bit more about the arithmetic of $\mathbb{Z}[i]$. This facilitates application of Thus's lemma with $\mu = (1+i)m$ rather than the more obvious choice $\mu = 2m$. We need the following two facts:

---

[2]This identity seems most naturally explained in terms of quaternions. (Of course, the same holds for Euler's more general identity expressing a product of two sums of four squares as a sum of four squares, which we have taken pains to avoid here.)

(i) The integer multiples of $1+i$ are exactly the even integers.
(ii) $1+i$ is a unit multiple of its complex conjugate.

Both (i) and (ii) are straightforward to check. Indeed, let r be an integer. Then $\frac{r}{1+i} = \frac{r}{2} - \frac{r}{2}i$, and this belongs to $\mathbb{Z}[i]$ precisely when r is even. This proves (i). The proof of (ii) is easier: $1+i = i(1-i)$, and i is a unit as $i^4 = 1$.

The following result now replaces Proposition 2.

Proposition 4. *Let m be an odd, squarefree integer. Then at least one of $2m$ and $4m$ is a sum of four squares.*

Proof. By Lemma 1, we may select $\alpha \in \mathbb{Z}[i]$ with $N\alpha \equiv -1 \pmod{2m}$. By Thue's lemma, there are $\beta, \gamma \in \mathbb{Z}[i]$, not both 0, with

$$\alpha\beta \equiv \gamma \pmod{(1+i)m} \tag{6}$$

and

$$\|\beta\|, \|\gamma\| \le 2^{1/4} m^{1/2}. \tag{7}$$

Applying complex conjugation to (6) shows that $\bar{\alpha}\bar{\beta} \equiv \bar{\gamma} \pmod{(1-i)m}$. Since $1+i$ and $1-i$ differ by a unit (fact (ii)), this last congruence is equivalent to the same congruence modulo $(1+i)m$:

$$\bar{\alpha}\bar{\beta} \equiv \bar{\gamma} \pmod{(1+i)m}. \tag{8}$$

Since $N\alpha \equiv -1 \pmod{2m}$, and 2 is a multiple of $1+i$, we have

$$N\alpha \equiv -1 \pmod{(1+i)m}.$$

Multiplying (6) and (8) and rearranging yields

$$N\beta + N\gamma \equiv 0 \pmod{(1+i)m}.$$

The left-hand side is a sum of four squares of integers, not all of which are zero, and so is a positive integer. It follows (keeping fact (i) in mind) that $N\beta + N\gamma$ is a multiple of both 2 and m, and so a multiple of $2m$. The inequalities (7) imply that

$$N\beta + N\gamma \le 4 \cdot (2^{1/4} m^{1/2})^2 = 2m \cdot 2\sqrt{2}.$$

Since $2\sqrt{2} = 2.828\ldots < 3$, either $N\beta + N\gamma = 2m$ or $4m$. $\square$

The advantage of Proposition 4 over Proposition 2 is that 2 and 4 are both powers of 2 ! So whichever case of Proposition 4 we find ourselves in, (the backward direction of) Lemma 3 implies the representability of m of as a sum of four squares. We assumed m was odd and squarefree, but another application of Lemma 3 (the forward direction this time) shows that all squarefree m are representable. As explained above, the four-square theorem follows.

Concluding remarks.

(i) The deepest fact used in our argument is that $N\mu = \#\mathbb{Z}[i]/(\mu)$ for all nonzero Gaussian integers μ. For our application this is only needed when $\mu = (1+i)m$, where m is an odd integer. In fact, all we really use is that $N\mu$ is an upper bound on $\#\mathbb{Z}[i]/(\mu)$ for these μ. As we now explain, this much has a simple proof. Since $N((1+i)m) = 2m^2$, it suffices to show the following.

Claim: Every Gaussian integer is congruent, modulo $(1+i)m$, to $a+bi$ for some integers a and b with $0 \le a < 2m$ and $0 \le b < m$.

To see this, note that given any Gaussian integer, subtracting a suitable integer multiple of $(1+i)m$ will force the imaginary component into the interval $[0, m)$ without changing the congruence class modulo $(1+i)m$. We may then subtract a multiple of $2m = (1+i)m \cdot (1-i)$ to place the real component in $[0, 2m)$.

(ii) Jameson recognizes the desirability of avoiding the 3-removal lemma and, in the same paper [**4**], gives an intriguing alternative argument serving this purpose. Bringing in an asymptotic estimate for the number of lattice points within a 4-dimensional ball, Jameson shows (essentially) that the conclusion (1) of Thue's lemma can be replaced with

$$N\beta + N\gamma \le \left(\frac{4\sqrt{2}}{\pi} + \epsilon\right)\sqrt{N\mu},$$

for any $\epsilon > 0$ and all μ with $N\mu$ sufficiently large in terms of ϵ. Since $4\sqrt{2}/\pi < 2$, one deduces from the proof of Proposition 2 that all large squarefree m are sums of four squares. Explicit estimates imply that $m > 764$ is large enough; of course, smaller m can be checked on a pocket computer (read: smartphone).[3] This argument is quite similar in spirit to the well-known proof of Lagrange's theorem based on Minkowski's geometry of numbers (see, e.g., [**2**]).

Acknowledgments.

The author thanks Enrique Treviño for useful feedback. Research of the author is supported by NSF award DMS-1402268.

References

1. M. Aigner and G. M. Ziegler, *Proofs from The Book*, fifth ed., Springer-Verlag, Berlin, 2014.
2. H. Davenport, *The geometry of numbers*, Math. Gazette **31** (1947), 206–210.
3. L. Euler, *Leonhardi Euleri—Opera omnia. Series 4 A. Commercium epistolicum. Vol. 4.2. Leonhardi Euleri commercium epistolicum cum Christiano Goldbach. Pars II/Correspondence of Leonhard Euler with Christian Goldbach. Part II*, Springer, Basel, 2015.
4. G. J. O. Jameson, *Two squares and four squares: the simplest proof of all?*, Math. Gazette **94** (2010), 119–123.
5. P. Samuel, *Algebraic theory of numbers*, Houghton Mifflin Co., Boston, Mass., 1970.
6. A. Thue, *Et par antydninger til en taltheoretisk metode*, Kra. Vidensk. Selsk. Forh. **7** (1902), 57–75.

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30601

E-mail address: pollack@uga.edu

[3]The details are arranged somewhat differently in [**4**]. For instance, the version of the argument presented there still relies on the 2-removal lemma (but requires less mopping up of small cases).