We recall the Fermat Conjecture: If \( n \) is an integer greater than 2, then there exists no triple \( \{x, y, z\} \), of positive integers such that

\[
x^n + y^n = z^n.
\]

This simple statement was made by Fermat in the mid-1600s as a marginal note in his copy of the work of Diophantus and accompanied by the remark that he had found a marvelous proof that was too long to be recorded on the free space on the page. It has not ceased to tantalize amateur and professional alike since it was found after Fermat’s death and made public by his son.

Since a proof for \( n = 4 \) was already known (due to Fermat himself) and since \( x^a + y^a = z^a \) implies that \( (x^a)^b + (y^a)^b = (z^a)^b \), it follows that the truth of the conjecture for \( n \) an odd prime would guarantee its truth for all \( n > 2 \). Although proofs for some of the odd primes were forthcoming during the next two centuries, these proofs were frustratingly specific to particular values of \( n \). Then in the mid-1800s new insight suggested that unity for the odd primes could be attained by viewing the set \( \mathbb{Z} \) of rational (ordinary) integers as a subset of certain sets of complex numbers, which were called cyclotomic integers, and in which \( x^n + y^n \) decomposes into \( n \) factors, all linear in \( x \) and \( y \). We look below at these “integers,” whose counterpart for \( n = 4 \) provides the setting for the theorem that we will prove. It appeared for a time that a strategy based on this new insight would finally settle the matter. It didn’t, the spoiler being that, although cyclotomic integers share many properties with \( \mathbb{Z} \), including that of being expressible as products of primes, in some cases this factorization is not unique. (The reader who is not familiar with the fascinating history of the Fermat Conjecture is assured that there is an abundance of pertinent literature and is invited in particular to consult references \([1],[3],[4],\) and \([5],\) in which many other sources are suggested.)

We begin our introduction to cyclotomic integers by considering the special case, \( n = 3 \), of the conjecture. Let \( Q \) denote the field of rational numbers and let \( \omega_3 \) denote \( (\frac{-1 + \sqrt{-3}}{2})/2 \), a primitive solution of the equation, \( x^3 - 1 = 0 \). We let \( Q(\omega_3) \) denote the field “\( Q \) adjoin \( \omega_3 \)”. The “cyclotomic integers” for \( n = 3 \) are the algebraic integers, \( I_3 \), of \( Q(\omega_3) \):

\[
Q(\omega_3) = \{a + b\omega_3 : a \text{ and } b \text{ are in } Q\}, \text{ while } I_3 = \{a + b\omega_3 : a \text{ and } b \text{ are in } \mathbb{Z}\}.
\]

Now it can be shown (for example, \([4],\) pp. 169–176, or \([5],\) pp. 191–194) that there is no triple, \( \{a, b, \gamma\} \), of nonzero members of \( I_3 \) such that \( \alpha^3 + \beta^3 = \gamma^3 \). Then, since \( \mathbb{Z} \) is included in \( I_3 \), the Fermat Conjecture is true for \( n = 3 \).

More generally, let \( p \) denote an odd prime, let

\[
\omega_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p},
\]

a primitive solution of the equation, \( x^p - 1 = 0 \), and let \( Q(\omega_p) \) denote \( Q \) adjoin \( \omega_p \). The “cyclotomic integers” for \( n = p \) are the algebraic integers, \( I_p \), of \( Q(\omega_p) \):

\[
Q(\omega_p) = \{a_0 + a_1\omega_p + a_2(\omega_p)^2 + \cdots + a_{p-2}(\omega_p)^{p-2} : \text{the } a_i \text{'s are in } Q\},
\]
while

\[ I_p = \{ a_0 + a_1 \omega_p + a_2 (\omega_p)^2 + \cdots + a_{p-2} (\omega_p)^{p-2}; \text{ the } a_i \text{'s are in } \mathbb{Z} \}. \]

Again, we should note that \( \mathbb{Z} \) is included in \( I_p \) and that it appeared for a time that the conjecture would be proven through study of the problem in \( I_p \). In fact, Kummer and others ([3], p. 172) showed that for certain odd primes called regular primes, unique factorization could be restored in \( I_p \) in a sense sufficient to prove the conjecture valid not only for \( \mathbb{Z} \)-integers but for the larger set of cyclotomic integers as well.

It is the case \( n = 4 \) that is of interest here. In elementary texts ([1], p. 291, for example), Fermat’s proof by infinite descent is given to establish the conjecture easily for \( n = 4 \) without viewing the set of positive integers as a subset of \( I_4 \) (the “integers” of \( \mathbb{Q}(\omega_4) \), where \( \omega_4 = i \) is a primitive solution of \( x^4 - 1 = 0 \)). Reflection on this point led us to think that it would be pleasing to see the \( \mathbb{Z} \)-proof of the conjecture for this case come as a corollary to an \( I_4 \)-proof, and thus we are led to offer our argument that for \( n = 4 \) the conjecture is valid in \( I_4 \), which is, of course, the set of Gaussian integers. Our exposition is, with minimal assistance from their teachers, accessible to undergraduates.

The Gaussian integers For convenience we are going to denote \( I_4 \), the Gaussian integers, by \( G \). In fact, \( G \) is the subset of the complex numbers consisting of all \( x + yi \), where each of \( x \) and \( y \) is a rational integer. \( G \) is a unique factorization domain in which the units (members with multiplicative inverses) are 1, \( i \), \(-1 \), and \(-i \). If \( \alpha = x + yi \) is in \( G \), we define the norm of \( \alpha \), \( N(\alpha) \), to be \( x^2 + y^2 \) (a nonnegative integer). The norm of a product is the product of the norms, and \( N(\alpha) \) divides \( N(\beta) \) if \( \alpha \) divides \( \beta \).

We now give some pertinent facts about \( G \) that the reader can find discussed in more detail in [2]. The complex number \( \delta = 1 + i \) is a prime in \( G \) (and a factor of 2) that plays a role in \( G \) rather like that played by 2 in the rational integers \( \mathbb{Z} \). If we let \( \alpha \) in \( G \) be called “even” or “odd” according to whether or not \( \alpha \) is divisible by \( \delta \), then the sum of two even members of \( G \) is even, the sum of two odd members is even, the sum of an even member and an odd member is odd, the product of two odd members is odd, and the product of an even member with any member is even. The member \( x + yi \) of \( G \) is even if and only if \( x \equiv y \pmod{2} \).

If \( (\xi, \psi, \zeta) \) is a triple of nonzero members of \( G \) with \( \gcd(\xi, \psi) = 1 \) and such that \( \xi^2 + \psi^2 = \zeta^2 \), then exactly one member of the triple is even. We define a Primitive Pythagorean Triple (PPT) in \( G \) to be an ordered triple \( (\xi, \psi, \zeta) \) of nonzero members of \( G \) with \( \gcd(\xi, \psi) = 1 \), having \( \xi \) and \( \zeta \) odd while \( \psi \) is even, and such that

\[ \xi^2 + \psi^2 = \zeta^2. \]

(If \( \gcd(\xi, \psi) = 1 \), then the members of the triple are relatively prime in pairs and \( \gcd(\xi, \psi, \zeta) = 1 \).) Reminiscent of the familiar means by which Pythagorean Triples in the integers \( \mathbb{Z} \) can be generated, PPTs in \( G \) can be generated by relatively prime odd Gaussian integers (see [2], p. 108). More precisely for our purposes, let \( (\xi, \psi, \zeta) \) be a PPT in \( G \); then there exist units \( E_1, E_2, \) and \( E_3 \) in \( G \), and relatively prime odd members \( a \) and \( b \) of \( G \), with real parts odd such that

\[ E_1 \xi = \frac{a^2 + b^2}{2}, \quad E_2 \psi = \frac{a^2 - b^2}{2i}, \quad E_3 \zeta = ab. \]
Example. The triple \((\xi, \eta, \zeta) = (-4 + i, 4 + 8i, 4 + 7i)\) is a PPT. If we let \(E_1 = E_2 = E_3 = -i\), while \(a = 3 + 2i\) and \(b = 1 - 2i\), we find that \((E_1 \xi, E_2 \eta, E_3 \zeta) = (1 + 4i, 8 - 4i, 7 - 4i)\) is also a PPT and is generated by \(a\) and \(b\) in the sense that \(1 + 4i = (a^2 + b^2)/2\), \(8 - 4i = (a^2 - b^2)/2i\), and \(7 - 4i = ab\). We point out that \(a\) and \(b\) are odd and have odd real parts.

What about \(\alpha^4 + \beta^4 = \gamma^4\) in \(G\)? As we said earlier, we are going to show that there is no triple \((\alpha, \beta, \gamma)\) of nonzero members of \(G\) such that \(\alpha^4 + \beta^4 = \gamma^4\). Then, since \(Z\) is a subset of \(G\), it will follow that the Fermat Conjecture is valid for \(n = 4\). Since \((\rho \alpha)^4 + (\rho \beta)^4 = (\rho \gamma)^4\) implies \(\alpha^4 + \beta^4 = \gamma^4\), it suffices to prove that no such triple exists with \(\gcd(\alpha, \beta) = 1\). In fact, we show a bit more:

**Theorem.** There exists no triple \((\alpha, \beta, \gamma)\) of nonzero members of \(G\) with \(\gcd(\alpha, \beta) = 1\) such that \(\pm \alpha^4 \pm \beta^4 = \pm \gamma^4\).

**Proof.** (Our proof is a version of Fermat’s method of infinite descent.) Suppose such a triple does exist. It is easy to see that exactly one of \(\alpha, \beta, \gamma\) is even. Then it is possible to rename and write

\[
\pm \alpha^4 \pm \beta^4 = \gamma^2. \tag{1}
\]

where \(\alpha\) and \(\gamma\) are odd while \(\beta\) is even and \(\gcd(\alpha, \beta) = 1\). In the set of all such triples \((\alpha, \beta, \gamma)\), there is one in which \(N(\gamma)\) is minimal. We assume that the triple under consideration is one such. Now \(\alpha^4 = (\alpha^2)^2\) and \(-\alpha^4 = (i \alpha^2)^2\); similarly \(\beta^4 = (\beta^2)^2\) and \(-\beta^4 = (i \beta^2)^2\). Thus there exist units, \(u_1\) and \(u_2\), such that \((u_1 \alpha^2, u_2 \beta^2, \gamma)\) is a PPT. Then we let \(E_1, E_2,\) and \(E_3\) be units and \(\alpha\) and \(\beta\) be relatively prime odd Gaussian integers with odd real parts such that

\[
E_1 \alpha^2 = \frac{a^2 + b^2}{2}, \quad E_2 \beta^2 = \frac{a^2 - b^2}{2i}, \quad E_3 \gamma = ab. \tag{2}
\]

(Here we have used the fact that the units in \(G\) form a multiplicative group so that, for example, any unit times \(u_1 \alpha^2\) can be written as \(E_1 \alpha^2\).) Now one can check that if \(\alpha\) is an odd Gaussian integer, then \(\alpha^2\) has odd real part and (by considering \(\alpha^2\) and \(b^2 \mod 4\)) that if each of \(a\) and \(b\) is odd with odd real part, then so is \((a^2 + b^2)/2\).

These observations imply that the unit \(E_1\) is either 1 or \(-1\). Now we divide the middle equality of (2) by \(-2i:\)

\[
-\frac{E_2 \beta^2}{2i} = -E_2 \left(\frac{\beta}{i}\right)^2 = \frac{a^2 - b^2}{4} = \frac{a - b}{2} \frac{a + b}{2}. \tag{3}
\]

Each of \(a\) and \(b\) has odd real part and even imaginary part, so that \((a - b)/2\) and \((a + b)/2\) are members of \(G\). Moreover they are relatively prime, for if \(\pi\) is a common prime factor, then it divides their sum and difference; that is, it divides each of \(a\) and \(b\), which is impossible. Then since their product is a unit times a square, each of \((a - b)/2\) and \((a + b)/2\) is a unit times a square:

\[
\frac{a - b}{2} = U_1 s^2 \quad \text{and} \quad \frac{a + b}{2} = U_2 t^2, \quad \text{where} \quad U_1 \text{ and } U_2 \text{ are units.}
\]

Any common divisor of \(s\) and \(t\) would divide \((a - b)/2\) and \((a + b)/2\); then \(s\) and \(t\) are relatively prime. Now

\[
\left(\frac{a - b}{2}\right)^2 + \left(\frac{a + b}{2}\right)^2 = (U_1 s^2)^2 + (U_2 t^2)^2 = \frac{a^2 + b^2}{2} = E_1 \alpha^2 = \pm \alpha^2.
\]
Then, multiplying through by $-1$, if necessary, and noting that the square of any unit is either 1 or $-1$, we can write

$$\pm s^4 \pm t^4 = \alpha^2. \quad (3)$$

Here $\alpha$ is odd, so that exactly one of $s$ and $t$ is even. Without loss of generality, we assume that $s$ is odd. We compare (1) and (3) and observe that if we can show that $N(\alpha) < N(\gamma)$, then we will have proven our theorem. To this end we recall that $E_1 \alpha^2 = (a^2 + b^2)/2$ and $E_3 \gamma = ab$. Since the norm of a unit is 1, we have

$$N(\alpha^2) = N(a^2 + b^2) \quad \text{and} \quad N(\gamma^2) = N(a^2b^2) = N(a^2)N(b^2).$$

Hence $N(a^2 + b^2) < N(a^2) + N(b^2)$, which is less than $4N(a^2)N(b^2)$, since for positive integers $m$ and $n$, $m + n < 4mn$. Then $N(\alpha^2) < N(\gamma^2)$, which implies that $N(\alpha) < N(\gamma)$. This contradiction completes the proof of the theorem.

A question for the reader Have we used the fact that factorization into primes in $G$ is unique, and if so, then where?

Thanks. I am grateful to my student, Danny K. McIntyre, whose interest in this problem was an inspiration to me. I also wish to thank my colleague, Professor Clay Ross, for his reading of the manuscript and to thank the referees for their valuable suggestions.

REFERENCES