A (Not So) Complex Solution to $a^2 + b^2 = c^n$

ARNOLD M. ADELBERG
Grinnell College
Grinnell, IA 50112
adelbe@math.grinnell.edu

ARTHUR T. BENJAMIN
Harvey Mudd College
Claremont, CA 91711
benjamin@math.hmc.edu

DAVID I. RUDEL
Dartmouth College
Hanover, NH 03755
david.rudel@dartmouth.edu

Everyone knows how easy it is to describe all solutions to the Diophantine equation $a^2 + b^2 = c^2$, and how difficult it is to prove the nonexistence of solutions to $a^n + b^n = c^n$ for $n > 2$. Mixing the easy equation with the hard one, we shall demonstrate that for $n \geq 2$, all solutions to $a^2 + b^2 = c^n$ can also be easily obtained by elementary number theory. We use only the simplest properties of the *Gaussian integers*, the complex numbers whose real and imaginary parts are both integers.

To set the stage, recall the situation when $n = 2$. The Pythagorean triples of positive integers that are primitive (that is, have no common prime factors) all have the form (a, b, c) or (b, a, c) where $a = x^2 - y^2$, $b = 2xy$, $c = x^2 + y^2$, where $x > y$ are relatively prime integers of opposite parity. This can be expressed more compactly using the Gaussian integer $z = x + yi$ and its conjugate $\overline{z} = x - yi$, whereby

$$a = \mathrm{Re}(z^2), \qquad b = \mathrm{Im}(z^2), \qquad c = \overline{z}z.$$

All solutions to $a^2 + b^2 = c^2$ are multiples of the primitive solutions.

In general, for $n \geq 2$, we demonstrate that all primitive solutions of $a^2 + b^2 = c^n$ have the form (a, b, c), where

$$\begin{aligned} &a = \mathrm{Re}(z^n), \quad &&b = \mathrm{Im}(z^n), \quad &&c = \overline{z}z \quad &&\text{when } n \text{ is odd,} \\ &a = \mathrm{Re}(z^n\omega), \quad &&b = \mathrm{Im}(z^n\omega), \quad &&c = \pm\overline{z}z \quad &&\text{when } n \text{ is even,} \end{aligned}$$

with $z = x + yi$, where x and y are relatively prime integers of opposite parity. In the even case, ω comes from the set of units $\{1, i, -1, -i\}$.

If $n > 2$, *not* all solutions to $a^2 + b^2 = c^n$ are multiples of primitive ones. The primitive solutions may be deduced by classical methods or from the following two theorems.

THEOREM 1. *When $n \geq 3$ is odd, integers a, b, and c satisfy $a^2 + b^2 = c^n$ if and only if*

$$a = \mathrm{Re}(z), \qquad b = \mathrm{Im}(z), \qquad c = \prod_{t=0}^{(n-1)/2} \overline{z}_t z_t, \tag{1}$$

where each z_t is a Gaussian integer and $z = \prod_{t=0}^{(n-1)/2} \overline{z}_t^t z_t^{n-t}$.

Proof. It is easy to see that (1) will generate solutions to $a^2 + b^2 = c^n$, since

$$a^2 + b^2 = \overline{z}z = \prod_{t=0}^{(n-1)/2} \overline{z}_t^n z_t^n = c^n.$$

To prove the other direction suppose that $a^2 + b^2 = c^n$, where n is an odd positive integer. We will use elementary number theory to prove that (1) is necessary for solutions. Let c^n have prime factorization

$$c^n = \prod_{j=1}^{k} p_j^{\alpha_j} \prod_{i=1}^{m} q_i^{\beta_i},$$

where $p_1 = 2$, $p_j \equiv 1 \pmod 4$, $j = 2 \ldots, k$, and $q_i \equiv 3 \pmod 4$, $i = 1 \ldots m$. We assume the primes are distinct, and hence $n \mid \alpha_j$ and $n \mid \beta_i$ for all i and j. Further, since c^n is the sum of two squares, it is well known [**2**] that $2 \mid \beta_i$ and since n is odd, $2n \mid \beta_i$ for all i.

Next we factor c^n into Gaussian primes, which consist of the traditional primes $q \equiv 3 \pmod 4$ and Gaussian integers $w = u + vi$ that satisfy $u^2 + v^2 = p$, where p is a prime not congruent to 3 (mod 4) [**1**]. By standard number theory [**2**], every such prime p is the sum of two squares. That is, for $j = 1 \ldots, k$, each p_j above can be written as $p_j = \overline{\rho}_j \rho_j$ where ρ_j is a Gaussian prime.

Summarizing, c^n has Gaussian prime factorization

$$(a + bi)(a - bi) = a^2 + b^2 = c^n = \prod_{j=1}^{k} (\overline{\rho}_j \rho_j)^{\alpha_j} \prod_{i=1}^{m} q_i^{\beta_i},$$

where $n \mid \alpha_j$, $j = 1 \ldots, k$, and $2n \mid \beta_i$, $i = 1 \ldots, m$. By the unique factorization of Gaussian integers (up to multiplication by units) into Gaussian primes, we must have

$$a + bi = \prod_{j=1}^{k} \overline{\rho}_j^{\gamma_j} \rho_j^{\delta_j} \prod_{i=1}^{m} q_i^{\beta_i/2} \omega, \tag{2}$$

and

$$a - bi = \prod_{j=1}^{k} \overline{\rho}_j^{\delta_j} \rho_j^{\gamma_j} \prod_{i=1}^{m} q_i^{\beta_i/2} \overline{\omega},$$

where ω is a unit, and for $j = 1 \ldots k$, we have $\gamma_j, \delta_j \geq 0$, and $\gamma_j + \delta_j = \alpha_j$.

Now define $r_j = \gamma_j \bmod n$ for $j = 1 \ldots, n$. Since $\gamma_j + \delta_j = \alpha_j$ is a multiple of n, we may write $\gamma_j = ns_j + r_j$ and $\delta_j = nt_j + (n - r_j)$, where $s_j, t_j \geq 0$ and $0 \leq r_j < n$. Hence, (2) becomes

$$a + bi = \prod_{j=1}^{k} (\overline{\rho}_j^{s_j} \rho_j^{t_j})^n \overline{\rho}_j^{r_j} \rho_j^{n-r_j} \left(\prod_{i=1}^{m} q_i^{\beta_i/2n} \right)^n \omega. \tag{3}$$

For a given exponent $0 \leq e \leq n$, the product of numbers of the form $\overline{w}^e w^{n-e}$ will still be of that form, and replacing w by $\overline{w}$ if necessary, we can assume $e \leq (n-1)/2$. Hence for $t = 0, 1, \ldots, (n-1)/2$, we let z_t denote the product of all terms in (3) of the form $\overline{w}^t w^{n-t}$. Note that terms of the form w^n have the form $\overline{w}^0 \overline{w}^n$, and that ω is itself an nth (odd) power. Hence

$$a + bi = \prod_{t=0}^{(n-1)/2} \overline{z}_t^t z_t^{n-t},$$

and (1) follows. ∎

THEOREM 2. *When $n \geq 2$ is even, integers a, b, and c satisfy $a^2 + b^2 = c^n$ if and only if*

$$a = r^{n/2}\,\mathrm{Re}(z\omega), \qquad b = r^{n/2}\,\mathrm{Im}(z\omega), \qquad c = \pm r \prod_{t=0}^{(n-2)/2} \overline{z}_t z_t \tag{4}$$

where r is a positive integer, ω is a unit, each z_t is a Gaussian integer, and $z = \prod_{t=0}^{(n-2)/2} \overline{z}_t^{\,t} z_t^{n-t}$.

Proof. The proof follows along the same lines as the previous one. The only subtlety to point out is that although 2 and n divide β_i, $2n$ might not divide β_i. However, the term $\prod_{i=1}^{m} q_i^{\beta_i/2} = (\prod_{i=1}^{m} q_i^{\beta_i/n})^{n/2}$ and the (integer) term of the form $\overline{z}_t^{\,n/2} z_t^{n/2}$ can be absorbed into the integer $r^{n/2}$. ∎

Acknowledgment. The authors gratefully acknowledge the assistance of Reba Schuller and the referees for helpful suggestions.

REFERENCES

1. David M. Burton, *Elementary Number Theory*, Allyn and Bacon, Inc., Boston, 1980.
2. R. M. Young, *Excursions in Calculus: An Interplay of the Continuous and the Discrete*, Dolciani Math. Exp. 13., MAA, Washington, D.C., 1992.

On the Two-Box Paradox

ROBERT A. AGNEW
Discover Financial Services
Riverwoods, IL 60015-3851
robertagnew@discoverfinancial.com

On a game show, you are presented with two identical boxes. Both boxes contain positive monetary prizes, one twice the other. You are allowed to pick one box and observe the prize $x > 0$, after which you can choose to trade boxes. In terms of simple expected value, it is *always* better to trade since $\frac{1}{2}(2x) + \frac{1}{2}\left(\frac{x}{2}\right) = \frac{5x}{4} > x$. That is the paradox.

Simple thought experiments suggest that a sufficiently large observed prize would cause a player not to trade, despite the mathematical computation of expected value. In individual cases, this creates some threshold, which depends on the observed prize, for ceasing to trade. A player may have in mind prior probabilities about what prizes the game show would offer, so that an observed prize of $10,000, for instance, would not yield equal *judgmental* odds of $20,000 or $5,000 in the unobserved box. The judgmental probability approach to the two-box problem seeks to develop optimal threshold strategies in terms of prior distributions on the set of possible prizes. Recent articles in this MAGAZINE have focused on the judgmental probability approach, although they have also discussed the second line of attack on this problem, expected utility [**2, 3**].

In expected utility theory, it is assumed than an individual has an underlying utility function for wealth. This utility function is increasing because it is presumed that an individual will always prefer more wealth to less wealth. In addition, the utility function is concave because it is presumed that an individual will have nonincreasing marginal utility for wealth. The utility function u is thus an increasing, concave function from the positive half line into the real line. The scaling on this function is unimportant because a positive linear transformation $a + bu$, with $b > 0$, is equivalent for individual