An Existence Proof

LK

I. We will prove the following

Theorem. There exist irrational numbers α and β such that α^β is rational.

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational or it is irrational. If $\sqrt{2}^{\sqrt{2}}$ is rational, let $\alpha = \sqrt{2}$, $\beta = \sqrt{2}$ and then α^β is rational while α and β are each irrational. If $\sqrt{2}^{\sqrt{2}}$ is not rational, let $\alpha = \sqrt{2}^{\sqrt{2}}$, $\beta = \sqrt{2}$. Then, both α and β are irrational and $\alpha^\beta = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2})^2} = (\sqrt{2})^2 = 2$ is rational. Thus we have shown that in any case, there exist irrational numbers α and β such that α^β is rational.
Q.E.D.

Discussion. This proof is logically correct, but you may find it unsatisfying since it does not produce a specific example of a pair of irrational numbers such that α^β is rational. In fact, $\sqrt{2}^{\sqrt{2}}$ <u>IS</u> irrational, but this takes much more work to prove.

To find out more, look at the article on the Wikipedia about the <u>Gelfond Schneider Theorem</u>. There you will see a sketch of the proof that $\sqrt{2}^{\sqrt{2}}$ is irrational (in fact transcendental).

Another approach is to know that $\log(4)$ is irrational (using base 10 logs). Then $\sqrt{10}^{\log(4)} = 10^{\log(2)} = 2$. Since $\sqrt{10}$ is irrational, this gives an explicit example.

But back to the existence proof. Some mathematicians would not allow existence proofs. They would argue that we should not be allowed to use the tautology

$$P \vee (\sim P) = T.$$

(This is called the "law of the excluded middle.)

The paper included with these notes is a story (about a chess problem) that is designed to promote discussion about this issue.

<u>Exercise.</u> Do you think that there exists a stretch of digits, 1000 digits long in the decimal expansion of π such that all the digits are 9? $\ldots \underbrace{999\ldots9}_{1000 \text{ of these}}\ldots$?
How would you find out if this is true or false?

Vol. 62, No. 5, December 1989

The Group of Units in Z_m

DAVID J. DEVRIES
Georgia College
Milledgeville, GA 31061

A very elementary proof of part of the primitive root theorem can be given using a basic result from group theory.

THEOREM. *If m is not of the form* 2, 4, p^k, *or* $2p^k$ *where p is an odd prime, then* Z_m *has an element of multiplicative order* 2 *in addition to* $m-1$.

Proof. Case I: Suppose $m = 4h$ for some $h > 1$. Let $a = 2h + 1$. Clearly a has order 2 and $1 < a < m - 1$.

Case II: Suppose $m = p^e q^f h$, where p and q are odd primes and $(pq, h) = 1$. Let j be the least positive solution to $(p^e h)x \equiv -2 \bmod q^f$. Let $a = p^e hj + 1$. Easily $1 < a < m - 1$. Also $(a+1)(a-1) \equiv 0 \bmod m$. Thus a has order 2. □

It follows that for such m the group of units of Z_m cannot be a cyclic group since such groups have at most one element of order 2. It is interesting to show that the rest of the primitive root theorem cannot be proved using this method. In this connection, it is a nice exercise to exhibit a noncyclic group with a unique element of order 2.

Classicists and Constructivists: A Dilemma

F. ALEXANDER NORMAN
University of North Carolina
Charlotte, NC 28223

An existential dilemma (in two parts, naturally):

Conditions for existence:

a) If A is constructivist then for A a dialectic existence proof is not sufficient.
b) If B is classicist then for B a constructive proof is sufficient, but not necessary.

The proof is trivial.

An anecdotal account of a classic constructible dilemma.

I was sitting in the grass outside Cabell Hall reading from Lakatos when I spied Cohn and Klaus ambling down the lawn, as was their wont each weekday during the lunch hour. Cohn, recently converted to a constructivist philosophy, had involved Klaus in an animated discussion.

"I can no longer—I dare say I will NEVER—accept existence merely on the presumption that nonexistence is contradictory." Cohn exclaimed. "To paraphrase Bishop, if one proves that a thing exists then one should show how to find it."

To which Klaus responded, "That's ridiculous! Brouwer notwithstanding, I will NEVER require that existence is dependent upon absolute constructibility. What a notion!"

The two had gone round and round like this—Brouwerian counterexamples to the use of the principle of the excluded middle, the claim that Hilbertian formalization leads to trivialization of knowledge and loss of reference, doubts about the validity of the constructivist assumption that the integers represent universally held, indisputable knowledge, etc.—when one of the two (I could not tell which) spotted an abandoned chess game a dozen or so meters away and directed the attention of the other to it.

Cohn commented, "As the king still appears to be standing, the game most likely has been interrupted. Perhaps you would like to play it out?"

"Indeed, I would!" replied Klaus.

As they neared the board the details of the position [2] became more visible; with hardly a glance one could tell White held a tremendous advantage. Cohn, not having examined the board closely, offered, "My dear Klaus, I wager I can exhibit a mate in two for White!" "You're on!"

After a few moments of analysis Cohn announced, "You are done in, my friend. I can prove there is a mate in two."

"Indeed, I imagine so," grinned Klaus mischievously. "Be so kind as to show me."

"Well, I move Ke6, and if you don't castle then g8 provides the mate."

"So it would. In which case, I should castle, don't you think?" replied Klaus.

"Of course, but if you can castle that means that neither your King nor Rook has moved, so you must have moved the Black pawn from e7 to e5. If so, then as a first move I would capture the pawn *en passant* and, if you then castled, b7 would provide the mate; if you did not castle, g8 mates."

"Very clever. But of course, you, of all people, see the 'obvious' fallacy."

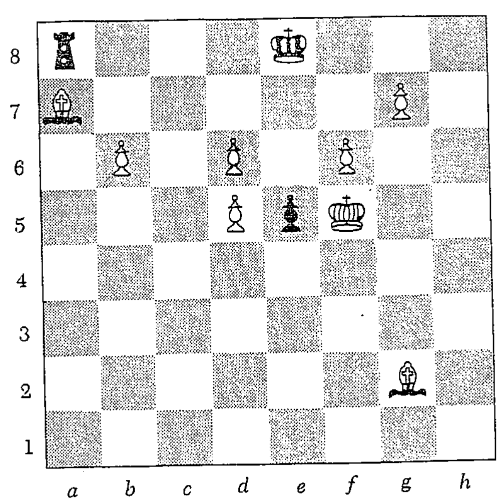
"What?—Either you can castle or you can't. If you can then White can mate. If you can't then White can mate. What's the big deal?" queried Cohn, not a little put out at this offhanded dismissal of his brilliant—well, ingenious—analysis.

"Such liberal use of non-constructivist principles—the excluded middle, dialectic existence... ."

"Now wait a minute, Klaus! You are the one who said you'd NEVER make constructivity a prerequisite for existence."

"And it was you, Cohn, who swore NEVER to accept an argument which... ."

It was getting late and I had a class to teach. Tucking *Proofs and Refutations* [1] under my arm I headed toward the nearest building. I could not help smiling. As the door closed quietly behind, I could hear the muted, yet lively, voices of Cohn and Klaus still engaged in their absurd debate.



Admittedly this dialogue is an imperfect presentation of the philosophical prejudices of constructivists and classicists. The implication here is that the working mathematician does not let philosophical considerations deprive him or her of results.

However, a more compelling theme emerges; one that has been eloquently articulated by Lakatos and others. As one colleague wrote: "... the current chess position is not the whole story of the game, similarly no formal axiomatic presentation of a branch of mathematics is the whole story of the objects with which it deals."

REFERENCES

1. Imre Lakatos, *Proofs and Refutations: The Logic of Mathematical Discovery*, Cambridge University Press, Cambridge, 1986.
2. This position, in which it can be *proved* that White can play and mate in two but the mate can not be exhibited, is the creation of Raymond Smullyan, and can be found in his delightful *The Chess Mysteries of Sherlock Holmes*, Alfred A. Knopf, New York, 1982, p. 103.

Solutions of $x^n + y^n = z^{n+1}$

LARRY HOEHN
Austin Peay State University
Clarksville, TN 37044

In students' first introduction to Fermat's Last Theorem (i.e, there are no nontrivial integral solutions to $x^n + y^n = z^n$ for $n > 2$), they frequently encounter several related diophantine equations. Some of these, such as $x^4 + y^4 = z^2$ (in most texts), $x^4 + 4y^4 = z^2$ [3], and $x^4 - y^4 = z^2$ [1], have no nontrivial solutions; whereas others, such as $x^2 + y^2 = z^2$ (Pythagorean triplets), $x^4 + 3y^4 = z^4$ [3], and $x^2 + y^2 = z^3$ [1], [3], have an infinite number of integral solutions.

There is, however, another equation, $x^n + y^n = z^{n+1}$, that is almost identical to Fermat's and which is very easy to deal with. To show that this equation has an infinite number of solutions, for any positive integers a and b define $z_0 = a^n + b^n$, $x_0 = az_0$, and $y_0 = bz_0$. By elementary algebra x_0, y_0, z_0 is a solution of $x^n + y^n = z^{n+1}$.

It may be noted also that $x = a(a^{n+1} + b^{n+1})$ and $y = b(a^{n+1} + b^{n+1})$ provide one solution in integers to $ax^n + by^n = z^{n+1}$.

One of the referees has pointed out that work on the equation $x^n + y^n = z^{n+1}$ goes back to at least 1908. In 1914, L. Aubry [2] gave the following more general result: If $\gcd(m, n) = 1$, then $x^m + y^m = z^n$ has the solution $x = a(a^m + b^m)^u$, $y = b(a^m + b^m)^u$, $z = (a^m + b^m)^v$, where $nv - mu = 1$.

REFERENCES

1. David M. Burton, *Elementary Number Theory*, Allyn and Bacon, Inc., Boston, 1980.
2. Leonard Eugene Dickson, *History of the Theory of Numbers*, vol. II, Chelsea Publishing Company, New York, 1952.
3. Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1984.