Irrational square roots

Michał Misiurewicz (mmisiure@math.iupui.edu), Indiana University - Purdue University Indianapolis, Indianapolis, IN

In the classroom. Suppose you show your students the standard proof that $\sqrt{2}$ is irrational:

Proof by contradiction. Suppose that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = m/n$ for some coprime positive integers $m$ and $n$. This means that $m^2 = 2n^2$. Thus, $m^2$ is even, and therefore $m$ is even. Hence, $m = 2v$ for some positive integer $v$. We get $4v^2 = 2n^2$, so $2v^2 = n^2$. By the same argument, this implies that $n$ is even, which contradicts the assumption that $m$ and $n$ are coprime. Therefore $\sqrt{2}$ is irrational.

Of course, the same proof works for every prime $p$. To prove that $\sqrt{p}$ is irrational, replace 2 by $p$ and “even” by “divisible by $p$.”

You wonder whether your students understand this principle. After all, it is not clear that for a student the notions of “even” and “divisible by $p$” are similar. After you prove the irrationality of $\sqrt{2}$ in class, you ask your students to prove that $\sqrt{3}$ is irrational.

One student’s proof starts by distinguishing the cases of $m$ and $n$ even or odd. This cannot be correct, you think, but before you write a big red zero on the paper, you read the rest of the proof.

Suppose that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = m/n$ for some coprime positive integers $m$ and $n$. This means that $m^2 = 3n^2$. If $n$ is even, then $m^2$ is even, so $m$ is even – a contradiction. If $m$ is even, then $3n^2$ is even, so $n$ is even – another contradiction. Thus, both $m$ and $n$ are odd, so $m = 2v + 1$ and $n = 2w + 1$ for some nonnegative integers $v, w$. We get $(2v + 1)^2 = 3(2w + 1)^2$, so $2v^2 + 2v = 6w^2 + 6w + 1$. The left-hand side is even, while the right-hand side is odd – a contradiction. Therefore $\sqrt{3}$ is irrational.
The proof is correct! Your student has earned a perfect score instead of 0, but did not learn what you wanted to teach.

Next time you are teaching this course, you do not repeat your mistake! You ask yourself: for what prime numbers does this “even-odd” proof work? You easily see that it works for all integers congruent to 3 modulo 4. It is clear what you have to do. The smallest prime number larger than 2 but not congruent to 3 modulo 4 is 5. Thus, you ask your students to prove that $\sqrt{5}$ is irrational.

One student submits this solution:

Suppose that $\sqrt{5}$ is rational. Then we can write $\sqrt{5} = m/n$ for some coprime positive integers $m$ and $n$. This means that $m^2 = 5n^2$. If $n$ is even, then $m^2$ is even, so $m$ is even – a contradiction. If $m$ is even, then $5n^2$ is even, so $n$ is even – a contradiction. Thus both $m$ and $n$ are odd, so $m = 2v + 1$ and $n = 2w + 1$ for some nonnegative integers $v, w$. We get $(2v + 1)^2 = 5(2w + 1)^2$, so $v^2 + v = 5w^2 + 5w + 1$. Now, $v^2 + v = v(v+1)$. Either $v$ or $v+1$ is even, so $v^2 + v$ is even. Similarly, $w^2 + w$ is even. Therefore the left-hand side of the equality $v^2 + v = 5w^2 + 5w + 1$ is even, while the right-hand side is odd – a contradiction. Therefore $\sqrt{5}$ is irrational.

Not again! This time, as you can again easily check, the proof works for all $k$ congruent to 5 modulo 8. You are desperate. What can you do? To check whether your students understand the idea of the proof of irrationality of $\sqrt{2}$, what can you ask them to prove?

**Problem.**

For which odd numbers $k$ can we prove that $\sqrt{k}$ is irrational using the “even-odd” method?

Let us translate the “even-odd” method into the rigorous language of mathematics. Assume that $\sqrt{k} = m/n$ with $(m, n) = 1$. Then

$$m^2 = kn^2. \quad (1)$$
Depending on whether $m$ is even or odd, we write $m = 2v$ or $m = 2v + 1$; depending on whether $n$ is even or odd, we write $n = 2w$ or $n = 2w + 1$ We substitute those expressions in (1). This gives us 4 possibilities. Some of them lead immediately to a contradiction (an even number equals an odd number), some of them may require further analysis. “Further analysis” means that we continue the same procedure with $v, w$ instead of $m, n$, that is, $v$ may be even or odd and $w$ may be even or odd. Repeating this procedure $\ell$ times amounts to considering $2^{2\ell}$ possibilities (although some may be ruled out earlier in the process): $m \equiv r \pmod{2^\ell}$ for some $r \in \{0, 1, \ldots, 2^\ell - 1\}$, and $n \equiv s \pmod{2^\ell}$ for some $s \in \{0, 1, \ldots, 2^\ell - 1\}$. In fact, many cases are ruled out because $r$ and $s$ are odd.

Thus, our proof is successful if, for some $\ell \geq 1$, all possibilities are ruled out, that is, the equation

$$r^2 \equiv ks^2 \pmod{2^\ell} \tag{2}$$

has no solutions in odd $r, s$. When solutions exist, we continue to $\ell + 1$.

Since $s$ is odd, it has an inverse modulo $2^\ell$. Multiplying both sides of (2) by the square of this inverse, we get $t^2 \equiv k \pmod{2^\ell}$. We see that our problem is equivalent to the following:

For which odd $k$ is there an $\ell \geq 1$, such that for every $t$ we have $t^2 \not\equiv k \pmod{2^\ell}$?

**Solution.** As we have noticed already, the “even-odd” method works if $k \equiv 3, 5, 7 \pmod{8}$. We can also see this by observing that $t^2 \equiv 1 \pmod{8}$ for all odd $t$. We will show that it does not work if $k \equiv 1 \pmod{8}$. That is, we show that if $k \equiv 1 \pmod{8}$ then for every $\ell \geq 1$ there is $t$ such that $t^2 \equiv k \pmod{2^\ell}$, and the “even-odd” proof will never terminate.

Let $k \equiv 1 \pmod{8}$. Then for $t = 1$ we get $k \equiv t^2 \pmod{2^\ell}$ for $\ell = 1, 2, 3$. Now we apply induction. Namely, we show that if $\ell \geq 3$ and $k \equiv t^2 \pmod{2^\ell}$ then either $k \equiv t^2 \pmod{2^{\ell+1}}$ or $k \equiv (t + 2^\ell)^2 \pmod{2^{\ell+1}}$. Indeed, if $k \equiv t^2 \pmod{2^\ell}$ then either $k \equiv t^2 \pmod{2^{\ell+1}}$ (and we are done), or $k \equiv t^2 + 2^\ell \pmod{2^{\ell+1}}$. In the latter
case, since $2\ell - 2 \geq \ell + 1$ and $t$ is odd,

$$(t + 2^{\ell - 1})^2 \equiv t^2 + 2^\ell t + 2^{2\ell - 2} \equiv t^2 + 2^\ell t \equiv t^2 + 2^\ell (t - 1) \equiv t^2 + 2^\ell \equiv k \pmod{2^{\ell + 1}}.$$ 

Thus, by induction we prove that for every $\ell \geq 1$ there is $t$ such that $k \equiv t^2 \pmod{2^\ell}$. This solves our problem.

**Theorem.** The “even-odd” method of proving that $\sqrt{k}$ is irrational works for an odd $k$ if and only if $k \equiv 3, 5, 7 \pmod{8}$.

**Conclusion.** To check whether your students understand the proof of irrationality of $\sqrt{2}$, ask them to prove that $\sqrt{17}$ is irrational.