Result that $\sqrt[n]{p} \notin \mathbb{Q}$, where p is a prime...

Sachin Kumar
University of Waterloo, Faculty of Mathematics

This essay will discuss the classic result that $\sqrt[n]{p} \notin \mathbb{Q}$, ie., irrational, when p is a prime and $n \in \mathbb{Z}_{>1}$. We will mainly see the classic elaborated highschool proof, using Fermat's method of Infinite descent and our not-so-common number theoretic proof of this classic result.

The classic highschool proof that $\sqrt{2} \notin \mathbb{Q}$...

As we all know, we will use proof by contradiction. Assume, that $\sqrt{2} \in \mathbb{Q}$, ie., rational. By Definition, we can then write, $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. Since, $\sqrt{2} > 0$, we can assume that $a, b > 0$ since if $a, b < 0$, we can multiply both of them by -1 to the $a, b > 0$ and if $a = 0$, then this is a contradiction of the fact that $\sqrt{2} > 0$.

We can also assume that a and b are not both $\mathbb{Z}_{\text{even}}$, for the following reason: If $a, b \in \mathbb{Z}_{\text{even}}$, then by Definition of an even integer, there exists $c, d \in \mathbb{Z}_+$ with $a = 2c$ and $b = 2d$. Now since $c, d \in \mathbb{Z}_+$, we have $c < 2c$ and $d < 2d$, so $c < a$ and $d < b$. Also, we have $\frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}$. So, replacing $\frac{a}{b}$ by $\frac{c}{d}$. If c and d are not both $\mathbb{Z}_{\text{even}}$, then we are done. Otherwise, $c, d \in \mathbb{Z}_{\text{even}}$, in which case we repeat the above argument and make another replacement of the ratio. Since, the integer numerator in the ratio is decreased with each replacement, yet is always > 0, we can only repeat this replacement process a finite number of times until we reach the situation in which both numerator and denominator are not both even, which is what we wanted to prove.

Now multiply on both sides of the initial equation by $b \in \mathbb{Z}_+$, and square both sides, to obtain the equation, $2b^2 = a^2$. By the Definition of divisibility, we thus obtain $2 \mid a^2$, so $a^2 \in \mathbb{Z}_{\text{even}}$. Assume, for the sake of contradiction, that $a \in \mathbb{Z}_{\text{odd}}$, so by Definition of odd integer, there exists $k \in \mathbb{Z}$, with $a = 2k + 1$. Then we have,

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

and hence we can conclude that a^2 is odd, which is a contradiction. As a result, we conclude that $a \in \mathbb{Z}_{\text{even}}$. Therefore, there exists $m \in \mathbb{Z}$ such that $a = 2m$, and substituting this into $2b^2 = a^2$ and rearranging, we get $b^2 = 2m^2$. Analyzing this equation similarly, we can conclude that $b \in \mathbb{Z}_{\text{even}}$. Hence, $a, b \in \mathbb{Z}_{\text{even}}$, which is a contradiction of the assumption that a and b are not $\mathbb{Z}_{\text{even}}$. Therefore, we proved that $\sqrt{2} \notin \mathbb{Q}$. □

Fermat's proof of Infinite descent for irrationality of $\sqrt[n]{p}$

Proof. Let $\sqrt[n]{p} = \frac{x_1}{y_1}$, where $x_1, y_1 \in \mathbb{Z}_+$. By n-th powering, we get

$$x_1^n = p y_1^n$$

which is a Diophantine equation. Finding the solutions to it will give us the denominators and numerators of all the rational numbers that equal $\sqrt[n]{p}$. Since the right-hand side is even, it means the left-hand side

should be even, too. In other words, $x_1 = px_2$, where $x_2 \in \mathbb{Z}_+$ and $x_1 > x_2$. Plugging that in and simplifying gives us

$$p^{n-1}x_2^n = y_1^n$$

It is trivial to see that the left side is even. So by a similar argument, $y_1 = py_2$, where $y_2 \in \mathbb{Z}_+$ and $y_1 > y_2$. What happens when we plug this in? A little simplification gives us something like these,

$$x_2^n = py_2^n$$

This means if we have a solution (x_1, y_1), it is possible to find another solution (x_2, y_2) to it. By recursion, we can generate an infinite sequence of strictly decreasing positive integers $x_1 > x_2 > \cdots$, and that is not possible. This is the key to Fermat's method of infinite descent. We have to show that if one solution exists, there exist infinitely many solutions which are strictly decreasing. That way we are done. Because we can never have an infinite sequence of strictly decreasing, non-negative integers. So, there was never a solution, to begin with. In our case, the Diophantine equation $x_1^n = py_1^n$ has no solution in positive integers. So, $\sqrt[n]{p} \neq \frac{x}{y}$, where $x, y \in \mathbb{Z}_+$ and that completes our proof.

□

Not-so-common number theoretic proof...

I am trying to make this essay as self contained as possible, so I will be discussing all the definition, theorems and claims (w/ proof) in order to show the chain reaction, LOL!. So before, actually proving the statement by polynomials and number theoretic methods, we will first discuss some useful non-trivial theorems and definition.

Definition (Divisibility of $\mathbb{Z}$). Let $a, b \in \mathbb{Z}$. a divides b, ie., $a \mid b$ if and only if there exists $k \in \mathbb{Z}$ such that $b = ak$.

Divisibility of Integer Combinations. For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then for all $x, y \in \mathbb{Z}$, $a \mid (bx+cy)$.

Proof. Let a, b and c be arbitrary integers, and assume that $a \mid b$ and $a \mid c$. Since $a \mid b$, by Definition of divisibility, there exist $r \in \mathbb{Z}$ such that $b = ra$. Similarly, for $a \mid c$, there exists $s \in \mathbb{Z}$ such that $c = sa$. Let x and y be arbitrary integers. Then also $bx + cy \in \mathbb{Z}$. Using the assumption, we have,

$$bx + cy = (ra)x + (sa)y = rax + say = (rx + sy)a$$

Since, $rx + sy \in \mathbb{Z}$. It follows from the definition of divisibility that $a \mid (bx + cy)$. □

Bounds of Divisibility. For all $a, b \in \mathbb{Z}$, if $b \mid a$ and $a \neq 0$, then $b \leq |a|$.

Proof. Let a and b be arbitrary integers and assume that $b \mid a$ and $a \neq 0$. Since, $b \mid a$, from the Definition of divisibility, there exists $q \in \mathbb{Z}$ so that $a = qb$. Since $a \neq 0$, this gives $qb \neq 0$, and hence $q \neq 0$. Therefore, $q \in \mathbb{Z}\backslash\{0\}$, so $|q| \geq 1$. Then using the properties of absolute value, we have $|a| = |qb| = |q| \cdot |b| \geq 1 \cdot |b| = |b|$, which gives $|b| \leq |a|$. Now, from Proposition 1, we also have the inequality $b \leq |b|$, and putting these two inequalities together, we obtain $b \leq |b| \leq |a|$, which gives $b \leq |a|$. □

Division Algorithm. For all $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_+$, there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$, where $0 \leq r < b$.

Proof. Let a be an arbitrary integer, and b be an arbitrary positive integer. We assume that there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$, with $0 \leq r < b$. To prove that the $q, r \in \mathbb{Z}$ are unique, assume that $q_1, r_1 \in \mathbb{Z}$

such that $a = q_1 b + r_1$, with $0 \leq r_1 < b$ and that $q_2, r_2 \in \mathbb{Z}$ such that $a = q_2 b + r_2$, with $0 \leq r_2 < b$. Then, we have the pair of inequalities,

$$\begin{aligned} 0 &\leq r_1 < b \\ -b &< -r_2 \leq 0 \end{aligned}$$

where the second inequality is obtained from $0 \leq r_2 < b$ by multiplying through by -1, which therefore reverses the inequalities. Now, adding this pair of inequalities, we obtain

$$-b < r_1 - r_2 < b \tag{0.1}$$

However, we also have $0 = a - a = (q_1 b + r_1) - (q_2 b + r_2) = (q_1 - q_2)b + (r_1 + r_2)$ and rearranging the equation $0 = (q_1 - q_2)b + (r_1 - r_2)$ gives $(q_2 - q_1)b = r_1 - r_2$. This means that $b \mid (r_1 - r_2)$, so $r_1 - r_2 = kb$, for some $k \in \mathbb{Z}$. Now substituting for $r_1 - r_2$ in (0.1) gives $-b < kb < b$, and dividing through this inequality by b, which is positive, gives $-1 < k < 1$. Since $k \in \mathbb{Z}$, we can conclude that $k = 0$. Now $k = 0$ gives $r_1 - r_2 = kb = 0b = 0$, so we have $r_1 = r_2$. Finally, substituting $r_1 = r_2$, we get $(q_2 - q_1)b = r_1 - r_2 = 0$ and since $b \neq 0$, we have $q_2 - q_1 = 0$ and hence $q_1 = q_2$. We have proved that $r_1 = r_2$ and $q_1 = q_2$, and therefore conclude that the $q, r \in \mathbb{Z}$ are unique. □

GCD With Remainders Theorem. For all $a, b, q, r \in \mathbb{Z}$, if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let a, b, q and r be arbitrary integers, and assume that $a = qb + r$. Now either a and b are not both zero, or they are both zero, and we consider these possibilities as two cases.

Case 1. When a and b are not both zero, let $d = \gcd(a, b)$. Note that in this case we also have that b and r are not both zero. From the definition of gcd we have $d \mid a$ and $d \mid b$, and by the Divisibility of Integer Combinations, this implies that $d \mid (a(1) + b(-q)) \implies d \mid (a - qb)$. But rearranging $a = qb + r$, we get $a - qb = r$, so $d \mid r$, and hence d is a common divisor of b and r. Now, let c be an arbitrary common divisor of b and r. Since, $c \mid b$ and $c \mid r$, then we have $c \mid qb + r$. Now, $a = qb + r$, so $c \mid a$. Since, $d = \gcd(a, b)$ and $c \mid a$ and $c \mid b$, then from the definition of gcd we have $c \leq d$. Hence, $\gcd(b, r) = d = \gcd(a, b)$ in this case.

Case 2. When are $a = b = 0$, then $a = qb + r$ becomes $0 = 0 + r$, so we have $r = 0$. We thus have $\gcd(a, b) = \gcd(0, 0) = 0$ and $\gcd(b, r) = \gcd(0, 0) = 0$, giving $\gcd(a, b) = \gcd(b, r)$ in this case. □

GCD Characterization Theorem. For all $a, b \in \mathbb{Z}$, and $d \in \mathbb{Z}_{\geq 0}$, if

1. d is a common divisor of a and b.
2. There exists integers s and t such that $as + bt = d$

then $d = \gcd(a, b)$.

Proof. Let a and b be arbitrary integers, and let d be an arbitrary non-negative integer. Assume that d is a common divisor of a and b, and that there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$. We consider the two cases a and b no both zero, and $a = b = 0$.

Case 1. Suppose that a and b are not both zero. Since d is a common divisor of a and b, that means that $d \neq 0$, so $d > 0$. Now, let c be an arbitrary common divisor of a and b. Hence, $c \mid a$ and $c \mid b$, so by divisibility of integer Combinations, we have that $c \mid (ax + by)$, for all $x, y \in \mathbb{Z}$. Therefore, $c \mid (as + bt)$, and since $as + bt = d$, we obtain $c \mid d$. Then from Bounds by Divisibility we obtain $c \leq |d|$, so by the positivity of d we get $c \leq d$. Hence from the definition of gcd, we have $d = \gcd(a, b)$.

Case 2. Suppose that $a = b = 0$. From the assumption that there exists $s, t \in \mathbb{Z}$ such that $as + bt = d$, we must have $d = 0$, since $0s + 0t = 0$, for all $s, t \in \mathbb{Z}$. Also, $0 \mid 0$, so $d = 0$ is a common divisor of $a = 0$ and $b = 0$. Since $\gcd(0, 0) = 0$, then $d = \gcd(a, b)$. □

Bézout's Lemma (Coprimeness Characterization Theorem). For all $a, b \in \mathbb{Z}$. $\gcd(a, b) = 1$ if and only if there exists $s, t \in \mathbb{Z}$ such that $as + bt = 1$.

Proof. Let a and b be arbitrary integers. We will prove both implications.

Claim. For $a, b \in \mathbb{Z}$ be nonzero, let $\gcd(a, b) = d$. Then, there exists $x, y \in \mathbb{Z}$ such that $ax + by = d$.

The proof of this claim uses the property that for non-zero integers a and b, dividing a by b leaves a remainder of r_1 strictly less than b and $\gcd(a, b) = \gcd(r_1, b)$ by GCD With Remainders. Then by repeated computation of the Euclidean division algorithm, we have

$$\begin{aligned} a &= bx_1 + r_1 && 0 < r_1 < |b| \\ b &= r_1x_2 + r_2 && 0 < r_2 < r_1 \\ &\vdots \\ r_{n-1} &= r_nx_{n+1} + r_{n+1} && 0 < r_{n+1} < r_n \\ r_n &= r_{n+1}x_{n+2} \end{aligned}$$

where the r_{n+1} is the last nonzero remainder in the division process. Now, we can use the second to last equation to solve for r_{n+1} as a combination of r_n and r_{n-1}. Unfolding this, we can solve for r_n as a combination of r_{n-1} and r_{n-2}, ...
Untill, we eventually write r_{n+1} as a linear combination of a and b. Since, r_{n+1} is the last nonzero remainder in the division process, it is the gcd of a and b, which proves our claim.

($\Longrightarrow$:) Assume that $\gcd(a, b) = 1$. Applying the above claim, there exists $s, t \in \mathbb{Z}$ so that $as + bt = 1$.

($\Longleftarrow$:) Assume that there exists $s, t \in \mathbb{Z}$ such that $as + bt = 1$. Now, $1 \mid a$ and $1 \mid b$ for all $a, b \in \mathbb{Z}$, so from GCD Characterization theorem, we have $\gcd(a, b) = 1$. □

Comprimness and Divisibility Theorem. For all $a, b, c \in \mathbb{Z}$, if $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$

Proof. Let a, b and c be arbitrary integers, and assume that $c \mid ab$ and $\gcd(a, c) = 1$. Since $\gcd(a, c) = 1$, by Coprimeness Characterization Theorem (or by Bézout's Lemma) there exists $s, t \in \mathbb{Z}$ such that $as + ct = 1$. Multiplying the equation by b gives,

$$abs + cbt = b$$

Now, we have $c \mid ab$ from the hypothesis, and $c \mid c$ from the Definition of divisibility, so by the Divisibility of integer combination, we have $c \mid ((ab)s + c(bt))$. Hence from (6.8) we obtain $c \mid b$. □

Rational Roots Theorem. For all $f(x) \in \mathbb{Z}[x]$ with $n \geq 1$. If $\frac{p}{q}$ is a rational root of $f(x)$, where $p, q \in \mathbb{Z}$ and $q \neq 0$, with $\gcd(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.

Proof. Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$, be an arbitrary polynomials, and assume $\frac{p}{q}$ is a root of $f(x)$. Then $f\left(\frac{p}{q}\right) = 0$, so we have

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_2\left(\frac{p}{q}\right)^2 + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

multiplying on both sides by q^n gives,

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n = 0$$

and rearranging, we obtain

$$a_n p^n = -q(a_{n-1} p^{n-1} + \cdots + a_2 p^2 q^{n-3} + a_1 p q^{n-2} + a_0 q^{n-1})$$

where $q, a_i, p^i \in \mathbb{Z}$, $0 \leq i \leq n$, so from the Definition of divisibility we have, $q \mid a_n p^n$.

Claim: for all $n \in \mathbb{N}$, if $\gcd(p, q) = 1$, then $\gcd(p, q^n) = 1$.

We will prove a claim by applying induction on n, where $P(n)$ is the open sentence that if $\gcd(p, q) = 1$, then $\gcd(p, q^n) = 1$.

Base Case. Let $n = 1$. We can see that if $\gcd(p, q) = 1$, then $\gcd(p, q) = 1$.

Inductive Case. Let k be an arbitrary natural number. Assume the inudctive hypothesis, $P(k)$. That is, we assume if $\gcd(p, q) = 1$, then $\gcd(p, q^k) = 1$. We wish to prove $P(k + 1)$, ie., if $\gcd(p, q) = 1$, then $\gcd(p, q^{k+1}) = 1$. Hence, assume $\gcd(p, q) = 1$. Hence assume $\gcd(p, q) = 1$, then by Bézout's Lemma (Coprimeness Characterization Theorem), there exists $s, t \in \mathbb{Z}$ such that $ps + qt = 1$. Since $\gcd(p, q^k) = 1$ from the inductive hypothesis, we can also use the Bézout's Lemma again, to give that there exists $u, v \in \mathbb{Z}$ such that $pu + q^k v = 1$, Multiplying these two equations together gives, $p^2 su + pq^k sv + pqtu + q^{k+1} tv = 1$, which we can rewrite as, $p(psu + q^k sv + qtu) + q^{k+1}(tv) = 1$. Let $e = psu + q^k sv + qtu$ and $f = tv$. Then from the previous equation $e, f \in \mathbb{Z}$ such that $pe + q^{k+1} f = 1$, and hence we deduce from the Bézout's Lemma that $\gcd(p, q^{k+1}) = 1$. The result us true for $n = k + 1$, and hence holds for all integers $n \geq 1$ by the Principle of Mathematical Induction.

So applying Coprimess and Divisibility theorem, we get that $q \mid a_n$. Now, the proof of $p \mid a_0$ is trivial using the same technique. □

Now, we will prove our original result that $\sqrt[n]{p} \notin \mathbb{Q}$, when p is a prime and $n \in \mathbb{Z}_{>1}$, using the rational roots theorem.

Proof. Since, we will be proving using rational roots theorem, we need to constuct a polynomial, $f(x) \in \mathbb{Z}[x]$ such that $\sqrt[n]{p}$ is a root of $f(x)$, ie., $f(\sqrt[n]{p}) = 0$. So let $x = \sqrt[n]{p}$, powering to the n-th on both sides we get $x^n = p$, so we get $f(x) = x^n - p \in \mathbb{Z}[x]$. Since, $f(\sqrt[n]{p}) = p - p = 0$, $\sqrt[n]{p}$ is a root of $f(x)$. Now, applying the rational roots theorem to $f(x)$. Since the divisors of 1 are ± 1 and p are ± 1 and $\pm p$. So, the candidates for rational roots of $f(x)$ are ± 1 and $\pm p$. We will see in two different cases: when $n \in \mathbb{Z}_{\text{even}}$ and when $n \in \mathbb{Z}_{\text{odd}}$. Using the fact that 1 is neither a prime nor composite the following holds,

When $n \in \mathbb{Z}_{even}$. $f(1) = f(-1) = 1 - p \neq 0$ and $f(p) = f(-p) = p^n - p = p(p^{n-1} - 1) \neq 0$, which means that $f(x)$ has no rational roots. Since, $\sqrt[n]{p}$ is a root of $f(x)$ but $f(x)$ has no rational roots, we proved that $\sqrt[n]{p}$ is irrational.

When $n \in \mathbb{Z}_{odd}$. $f(1) = 1 - p \neq 0$, $f(-1) = -1 - p = -(1 + p) \neq 0$, $f(p) = p^n - p = p(p^{n-1} - 1) \neq 0$ and $f(-p) = -p^n - p = -p(p^{n-1} + 1) \neq 0$, which means that $f(x)$ has no rational roots. Since, $\sqrt[n]{p}$ is a root of $f(x)$ but $f(x)$ has no rational roots, we proved that $\sqrt[n]{p}$ is irrational.

Therefore, we proved that $\sqrt[n]{p}$ is irrational when p is a prime and $n > 1$ □