Number theory Problems

CS/MATH 113 team

January 6, 2023

1. Prove that for all natural numbers $n > 1$, $\sqrt[n]{n}$ is irrational

Solution: Suppose $\sqrt[n]{n}$ is rational for some $n \in \mathbb{N}$
Then there exists integers a and b, such that $\sqrt[n]{n} = \frac{a}{b}$, where $b \neq 0$ and $gcd(a, b) = 1$

$$\sqrt[n]{n} = \frac{a}{b} \Rightarrow n = \frac{a^n}{b^n}$$

$$gcd(a, b) = 1 \Rightarrow gcd(a^n, b^n) = 1$$

As $n \in \mathbb{N}$, then $b^n = 1$, which means $n = a^n$
As $n > 0$ and $b^n = 1$, then $a^n > 0$, which means that $a > 0$
$a \neq 1$, as if $a = 1$ then $n = \frac{a^n}{b^n} = \frac{1}{1} = 1$, but $n > 1$, so $a \geq 2$
We know for all natural numbers n $2^n > n$ (this result is trivial and can be easily proved by mathematical induction.
So $a^n \geq 2^n > n$, which means $n \neq a^n$, there we have a contradiction with out orignal claim that $n = a^n$
Therefore for all natural numbers $n > 1$, $\sqrt[n]{n}$ is irrational

$\square$

2. Given that p is a prime and $p|a^n$, prove that $p^n|a^n$.

Solution: As $p|a^n$ then $a^n = kp$ for some integer k.
Case 1: $p \neq a$
Then a is not a prime, then $a = p_1 \times p_2 \times ...p_m$
$a^n = p_1^n \times p_2^n \times ...p_m^n = kp$
As $p|a^n$ and $a^n = p_1^n \times p_2^n \times ...p_m^n$ then there must be some p_i from $1 \leq i \leq m$ such that $p|p_i$
As p_i is prime for all $i \leq i \leq m$, then if $p|p_i$ then $p_i = p$ which means $p|a$
Then $a = pq$ so $a^n = p^n q^n$ therefore $p^n|a^n$.
Case 2: $p = a$
If $p = a$ and $p|a^n$ then as $a^n|a^n$ and $a^n = p^n$ then $p^n|a^n$.

$\square$

3. Show that any composite three-digit number must have a prime factor less than or equal to 31.

Solution: The next prime after 31 is 37, then the smallest composite number not containing a prime factor less than or equal to 31 would be $37^2 = 1369$ which is 4 digits.

$\square$

4. Show that $\sqrt{p}$ is irrational for any prime number p.

Solution: Suppose $\sqrt{p}$ is rational then $\sqrt{p} = \frac{r}{q}$ where $q \neq 0$ and $gcd(q, r) = 1$
Then $p = \frac{r^2}{q^2}$, so $pq^2 = r^2$
Now as $r^2 = r \times r$ then any number in prime factorization of r^2 would appear an even number of times.
Similiary any number in prime factorization on q^2 appear and even number of times.
So take $q^2 = p_1 \times p_2 \times ...p_n \times p_1 \times p_2 \times ...p_n$
As $p|r^2$ and $q^2|r^2$ then $r^2 = p \times p_1 \times p_2 \times ...p_n \times p_1 \times p_2 \times ...p_n$
Now p is a number that appears in prime factorization of r^2 an odd number of times.
Here we have a contradiction, therefore $\sqrt{p}$ is irrational.

$\square$

5. Show that if a is a positive integer and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.

Solution: Let $a \in \mathbb{Z}^+$, suppose $\sqrt[n]{a}$ is rational, we show that then $\sqrt[n]{a}$ must be an interger.
Let $\sqrt[n]{a} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ where $q \neq 0$ and $\gcd(p, q) = 1$.

$$\sqrt[n]{a} = \frac{p}{q} \Leftrightarrow a = \frac{p^n}{q^n} \Leftrightarrow aq^n = p^n$$

Now we have that $q^n|p^n$, but as $\gcd(p, q) = 1$ then $\gcd(p^n, q^n) = 1$.
So as only common divider of p^n and q^n is 1 and $q^n|p^n$ then $q^n = 1$
Therefore $a = \frac{p^n}{q^n} = p^n$, so $\sqrt[n]{a} = p$.
Which means $sqrt[n]a$ is an integer.

$\square$

6. In this question we will prove Euclid's Lemma that if p is a prime number that divides ab then p divides a or p divides b.
We shall prove this by proving a lemma and using a corollary from that lemma.
Well ordering principle: Every non empty set of positive integers have a smallest element.
Division algorithm: if $a, b \in \mathbb{Z}$, where $b > 0$, then there exists unique $q, r \in \mathbb{Z}$, $a = bq + r$ where, $0 \leq r < b$
   (a) **Bezout's lemma:** for all integers a and b there exist integers s and t such that $gcd(a, b) = as + bt$

   Solution:

Let $S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$
Due to well ordering principle S has a smallest element d

$$d = as + bt$$

We claim that $d = gcd(a, b)$
Using the division algorithm $a = dq + r$, where $0 \leq r < d$
We assume $r > 0$, and reach a contradiction, from which we can conclude that $r = 0$ thus d would divide a
If $r > 0$

$$r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$$

r is in the form that it belongs to our set S, but as said above $r < d$ thus it contradicts the fact that d is the smallest element in S
Thus $r = 0$, which means d divides a
Same argument can be constructed for b and used to show that d divides b as well.
Now assume there exist d' that is also a divisor of a and b.
Let $a = d'h$ and $b = d'k$
Then $d = as + bt = (d'h)s + (d'k)t = d'(sh + kt)$, then d' is also a divisor of d
Thus $d > d'$, so by universal generalization we can conclude that d is the greatest of all divisors of a and b. Thus contradiction with the fact that d is the smallest element.

$\square$

(b) **Corollary of bezout's lemma:** If a and b are relatively prime then $as + bt = 1$

(c) Using the above corollary prove Euclid's lemma.

Solution: Let p be a prime that divides ab but does not divide a
We need to show that p must divide b
As $p \nmid a$ and p is a prime then $\gcd(a, p) = 1$
Then there exist $s, t \in \mathbb{Z}$ such that $1 = as + pt$

$$b = abs + pbt$$

as p divides right hand side then p would divide b as well.

$\square$

7. For all positive integers a and b show that $\gcd(a,b)\text{lcm}(a,b) = ab$.

Solution: Let $d = \gcd$ for $a, b \in \mathbb{Z}$. Then $\exists p, q \in \mathbb{Z}$ s.t. $a = pd$ and $b = qd$.
Let $m = \frac{ab}{d}$ then $m = aq = pb$. Which means $a|m$ and $b|m$ which mean m is a common multiple of a and b.
Now we need to show that m is indeed the least common multiple of a and b.
Let c be a common multiple of a and b, then $c = at = sb$.
From bezout's lemma we know that $\exists x, y \in \mathbb{Z}$ s.t. $d = ax + by$.
We show that $m|c$ which would imply that $m \leq c$.

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{cax}{ab} + \frac{cby}{ab}$$

$$\frac{cax}{ab} + \frac{cby}{ab} = \frac{cx}{b} + \frac{cy}{a} = \frac{c}{b}x + \frac{c}{a}y$$

$$\frac{c}{m} = \frac{c}{b}x + \frac{c}{a}y = sx + ty$$

As $s, x, t, y \in \mathbb{Z}$ then $sx + ty \in \mathbb{Z}$, which means $m|c$ theefore $m \leq c$.
Which means m is the least common multiple of a and b.
So we have that $dm = \gcd(a,b)\text{lcm}(a,b) = ab$.

$\square$

8. Show that there are infinitely many primes, in other words the set containing all prime numbers is infinite.
Definition: A prime number is a Natural number that is only divisible by 1 and itself, and has to be divisible by 2 different numbers.
Fundamental Theorem of Arithmetic: Every integer $N > 1$ has a prime factorization, meaning either N is itself prime or can be written as a product of prime numbers.

Solution: Let $s = \{p_0, p_1, p_2, ..., p_n\}$ be set of all primes.
Let $P = p_0 \times p_1 \times p_2 \times ... \times p_n$
Let $q = P + 1$
Case 1:
q is prime, which is not in our set s
Case 2:
if q is not prime, then there exits a prime factor decomposition of q.
Let f be a prime that divides q, then f would be in our set s thus f would divide P too.
As f divides q and P then f divides $q - P$, which is 1
Then f divides 1.
As $f \geq 2$ f cannot divide 1, thus we have a contradiction.

$\square$

9. Prove the following claim: There exists irrational numbers a and b such that a^b is rational.

Solution: Take $a = \sqrt{2}$ and $b = \sqrt{2}$

$$c = a^b$$

Case 1:
If $\sqrt{2}^{\sqrt{2}}$ is rational then we already have our irrational numbers a and b such that a^b is rational
Case 2:
If $\sqrt{2}^{\sqrt{2}}$ is irrational then, let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$

$$c = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$$

and 2 is rational

$\square$

10. Show that $\sqrt{2}$ is irrational. In other words, $\sqrt{2}$ cannot be written in the form $\frac{p}{q}$ where $p, q \in \mathbb{Z}$ and $q \neq 0$

Solution: Assume $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.
And $\frac{p}{q}$ is the lowest form it can be.

$$\left(\frac{p}{q}\right)^2 = 2$$

$$p^2 = 2q^2$$

This implies p is even which means $p = 2k$, for some $k \in \mathbb{Z}$

$$4k^2 = 2q^2$$

$$2k^2 = q^2$$

This implies q is even.
But p and q can't both be even as they are in the lowest form possible thus the 2 would be canceled.
Here we have a contradiction.
Thus $\sqrt{2}$ cannot be written in form $\frac{p}{q}$ where $p, q \in \mathbb{Z}$
Thus $\sqrt{2}$ is irrational.

$\square$

11. Show that $x^n + y^n = z^n$ has no solutions where $x, y, z \in \mathbb{Z}$ with and $x \neq 0, \quad y \neq 0, \quad z \neq 0$ whenever $n \in \mathbb{Z}$ and $n > 2$

Solution: I've found a remarkable proof of this fact, but there is not enough space in the margin to write it.

$\square$