Number theory Problems

CS/MATH 113 team

February 9, 2023

The questions with (*) are hard, the ones with (+) are medium level difficulty, the ones with (-) are easy level the ones (**) are very hard and not doable by students

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.

□

(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.

□

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 $dm = \gcd(a, b)\text{lcm}(a, b) = ab$.

□

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.

□

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

□

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.

□

11. (-) Explain what you must do to disprove the statement: $x^3 + 5x + 3$ has a root between $x = 0$ and $x = 1$

Solution: The statement in logical notation is

$$\exists x \text{ such that } (0 < x < 1 \land x^3 + 5x + 3 = 0)$$

Giving a counterexample is not enough. Saying that when $x = 0.5$ then $x^3 + 5x + 3 \neq 0$ is not sufficient.
To disprove this statement, we need to prove that the **negation is true** which is

$$\neg\exists x \text{ such that } 0 < x < 1 \land x^3 + 5x + 3 = 0 \equiv \forall x \text{ such that } \neg(0 < x < 1 \land x^3 + 5x + 3 = 0)$$

Or in English

For all x, it is not the case that both x is between 0 and 1 and $x^3 + 5x + 3 = 0$

12. (-) Prove that for any integer n the number $n^2 + 5n + 13$ is odd

Solution:

If n is an integer, it can either be even or odd.
Case 1: n is even. Therefore $n = 2a, a \in \mathbb{Z}$

$$\begin{aligned} &(2a)^2 + 5(2a) + 13 \\ =&4a^2 + 10a + 13 \\ =&4a^2 + 10a + 12 + 1 \\ =&2(2a^2 + 5a + 6) + 1 \end{aligned}$$

Therefore $n^2 + 5n + 13$ is odd in this case.
Case 2: n is odd. Therefore $n = 2a + 1, a \in \mathbb{Z}$

$$\begin{aligned} &(2a+1)^2 + 5(2a+1) + 13 \\ =&4a^2 + 4a + 1 + 10a + 5 + 13 \\ =&4a^2 + 14a + 19 \\ =&4a^2 + 14a + 18 + 1 \\ =&2(2a^2 + 7a + 9) + 1 \end{aligned}$$

Therefore $n^2 + 5n + 13$ is odd in this case.

Since the statement is true in all cases, it is true in general.

13. (-) State the statement of Contradiction and verify that it is a valid argument.
Hint: In contradiction we are saying that A implies B is the same as saying that A and $\neg B$ happening together is false.

Solution:
Statement is

$$(A \implies B) \equiv ((A \wedge \neg B) \;\; is \;\; \text{false})$$

We can show that one side is equivalent to the other

$$\neg(A \wedge \neg B) \equiv (\neg A \vee B) \equiv (A \implies B)$$

Therefore it is true

14. (-) Show through contraposition the following proposition is true: $x \in \mathbb{Z}$. If $7x+9$ is even, then x is odd.

Solution: Proof by Contrapositive
Let P be " $7x + 9$ is even" and Q be "x is odd"
Instead of doing a direct proof where we show $P \implies Q$, we would show that $\neg Q \implies \neg P$ since that seems easier.
Suppose x is not odd.
Thus x is even, so $x = 2a$ for some integer a.

Then

$$7x + 9 \tag{1}$$
$$= 7(2a) + 9 \tag{2}$$
$$= 14a + 8 + 1 \tag{3}$$
$$2(7a + 4) + 1 \tag{4}$$

Therefore $7x + 9 = 2b + 1$, where b is the integer $7a + 4$.
Consequently $7x + 9$ is odd.
Therefore 7x + 9 is not even
Therefore proving $\neg Q \implies \neg P$ thus logically equivalent to $P \implies Q$

15. (-) Prove that "$(a + b)^2 = a^2 + b^2$" is **not** an algebraic identity where $a, b \in \mathbb{R}$

Solution: We can disprove this by finding **specific** real numbers a and b for which the equation is false.
If an equation is **not** an identity, you can usually find a counterexample by trial and error. In this case, if $a = 1, b = 2$ then

$$(a + b)^2 = (1 + 2)^2 = 3^2 = 9 \text{ while } a^2 + b^2 = 1^2 + 2^2 = 5$$

So if $a = 1, b = 2$ then $(a + b)^2 \neq a^2 + b^2$ and hence the statement is not an identity.

A common mistake is to say:

"$(a + b)^2 = a^2 + 2ab + b^2$, which is not the same as $a^2 + b^2$."

In the first place, how do you know $a^2 + 2ab + b^2$ is not the same as $a^2 + b^2$? It is no answer to say that they look different - after all, $(\sin\theta)^2 + (\cos\theta)^2$ looks very different than 1 , but $(\sin\theta)^2 + (\cos\theta)^2 = 1$ is an identity.

In the second place, $a^2 + 2ab + b^2$ is the same as $a^2 + b^2$ if (for instance) $a = 17$ and $b = 0$ - and they're equal for many other values of a and b.

16. (-) Prove that for m and n integers, if 2 divides m or 10 divides n, then 4 divides m^3n^2

Solution:

$$(m \bmod 2 = 0 \lor n \bmod 10 = 0) \implies m^3n^2 \bmod 4 = 0$$

Case 1: $m \bmod 2 = 0$ is true.
This is when $m = 2x$ where $x \in \mathbb{Z}$
Then:

$$(2x)^3n^2$$
$$8x^3n^2$$
$$4(2x^3n^2)$$

The above is divisible by 4.
Proved for $m \bmod 2 = 0$.
Case 2:
$n \bmod 10 = 0$ is true:
This is when $n = 10x$ where $x \in \mathbb{Z}$
then:

$$m^3(10x)^2$$

$$m^3 100x^2$$

$$4(25m^3x^2)$$

The above is divisible by 4
Proved for $n \bmod 10 = 0$.

17. (-) Give a counterexample to the statement

"If n is an integer and n^2 is divisible by 4, then n is divisible by 4"

Solution: To give a counterexample, we need an integer n such that n^2 is divisible by 4 but n is **not** divisible by 4 - the "if" part must be true, but the "then" part must be false. For example, $n = 6$. Then $n^2 = 36$ is divisible by 4 but $n = 6$ is not divisible by 4. Thus, $n = 6$ is a counterexample to the statement.
Note that $n = 5$ is not divisible by 4, $n^2 = 25$ is also not divisible by 4. Both the "if" and "then" parts of the statement are both false. Therefore, $n = 5$ is not a counterexample to the statement.

18. (-) Show through contraposition the following proposition is true : If $x^2 - 6x + 5$ is even, then x is odd.

Solution: A direct proof seems difficult. We would begin by assuming that $x^2 - 6x + 5$ is even, so $x^2 - 6x + 5 = 2a$.

Then we would need to transform this into $x = 2b + 1$ for $b \in \mathbb{Z}$. But it is not quite clear how that could be done, for it would involve isolating an x from the quadratic expression.

However the proof becomes very simple if we use contrapositive proof.

Proposition Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd. Thus x is even, so $x = 2a$ for some integer a. So

$$x^2 - 6x + 5 \tag{5}$$

$$= (2a)^2 - 6(2a) + 5 \tag{6}$$

$$= 4a^2 - 12a + 5 \tag{7}$$

$$4a^2 - 12a + 4 + 1 \tag{8}$$

$$= 2(2a^2 - 6a + 2) + 1. \tag{9}$$

Therefore $x^2 - 6x + 5 = 2b + 1$, where b is the integer $2a^2 - 6a + 2$

Consequently $x^2 - 6x + 5$ is odd. Therefore $x^2 - 6x + 5$ is not even.

In summary, since x being not odd ($\neg Q$) resulted in $x^2 - 6x + 5$ being not even ($\neg P$), then $x^2 - 6x + 5$ being even (P) means that x is odd (Q).

Thus we have proved $P \implies Q$ by proving $\neg Q \implies \neg P$