9/5/2018 Fall 2018,Proofs and Problem Solving I Sitaraman

Howard University Math Department

Some problems from basic number theory

1. Prove that is x is rational and y is rational then $x+y, x-y, xy, x/y$ are rational. For the last one assume y is non-zero.

   Solution:

   Write $x = \frac{a}{b}, y = \frac{c}{d}$. Then simplify $\frac{a}{b} + \frac{c}{d}, \frac{a}{b} - \frac{c}{d}, \frac{a}{b} \times \frac{c}{d}, \frac{a}{b} / \frac{c}{d}$ into single fractions.

2. Prove by contradiction that if x is rational and y is irrational then $x+y$ is irrational.

   Solution: If $x+y$ were rational, then $(x+y)-x = y$ would also be rational because the difference of two rational numbers is also rational as we saw in 1. But y is assumed to be rational, so the contradiction means $x+y$ cannot be rational.

3. Prove that any integer can be factored into prime numbers in only one way. (Unique factorization of integers).

   Solution: The full proof of this will be given later.

   For now, just note that, if an integer is not a prime, then you can break it into factors (which *have* to be smaller than itself and bigger than 1). Then you can repeat the argument for its factors in case any of them is not a prime number. This process can be continued until you reach a factorization into prime numbers.

   You can also show that this can be done in only one way. We will prove that later as well.

4. Prove that gcd of a and b (denoted (a, b)) is least positive element in set of integers of the form of $ax + by$ where x, y are integers.

   [Note that we are assuming such a number exists. But this follows from the well-ordering principle – any non-empty subset of natural numbers will contain a gcd].

   Solution: Suppose d_0 is the smallest natural number of the form $ma + nb$, and say $d_0 = m_0 a + n_0 b$. Let d be any natural number that divides both a and b. We will first show that d also divides d_0. This means that the d_0 is bigger than any common divisor of a and b.

   Proof that d divides d_0 : By the homework problem, if d divides a and b then d divides any number of form $ma + nb$. Therefore $d | d_0$ because it is of that form.

Next we will show that d_0 would also divide a and b which means it is also itself a common divisor of a and b. But since we already showed that it is bigger than any other common divisor, this means that d_0 IS the gcd of a and b.

To show this use division algorithm again, dividing a by d_0.

$$a = qd_0 + r,\ 0 \le r < d \implies a = q(m_0a + n_0b) + r \implies (1 - qm_0)a + (-n_0)b = r.$$

So we get that $0 \le r < d$ and r is of the form $ma + nb$.

Since d_0 is least such number only possibility is $r = 0$ and $d_0|a$.

Proof that $d_0|b$ is identical.

5. Prove by contradiction: If $p|ab$, then $p|a$ or $p|b$. (This is used to prove unique factorization).

   Solution: Let $ab = pk$ since p divides ab. Since p is prime, gcd of p and a is 1 if p does not divide a. So using problem 4, we can write $px + ay = 1$ for some integers x, y. Multiplying both sides by b we get $pbx + aby = b \implies pbx + (pk)y = b \implies p(bx + ky) = b$. In other words, p divides b. So if p doesn't divide a it will divide b. Same kind of argument can be used to show that if p doesn't divide b it will divide a.

   (Assuming unique factorization): Break down both a and b into prime factors. If p is not any one of them, then writing $a \times b$ as a product of primes we get a factorization of ab into primes that does not contain p. But we know there is only one way to do it, so it must be *the way* to factorize ab and thus p is not in the factorization of ab. In other words, p does not divide ab, contrary to assumption.

6. Prove that $\sqrt{2}$ is irrational.

   Solution:

   If $\sqrt{2} = m/n$ with m and n having no common factors (we can always write any rational number like this), then

$$\sqrt{2} = \frac{m}{n} \implies 2 = \frac{m^2}{n^2} \implies 2n^2 = m^2 \implies 2|m^2(\text{ means 2 divides } m^2)$$

$$\implies 2|m \text{ (prime factors of } m \text{ and } m^2 \text{ are same)} \implies m = 2k \text{ (for some integer } k)$$

$$\implies m^2 = 4k^2 \implies 2n^2 = 4k^2 \implies n^2 = 2k^2 \implies 2|n^2 \implies 2|n.$$

   But we assumed that m, n have no common factors, so 2 *cannot* divide both!

7. Prove that n^2 is odd if n is odd.

   Solution: If n is odd we can write it as $n = 2k + 1$ for some integer k.

   Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ which is definitely odd.

PROOF BY CASES:

8. Prove that $n^2 + n$ is always even for any integer n.

   Two cases. Either the integer n is odd or it is even.

   Clearly if it is even each term is even and sum is even.

   If it is odd we proved that n^2 is odd. So both are odd and the sum of two odd numbers is always even so $n^2 + n$ is odd.

   This can also be proved directly by noting that $n^2 + n = n(n + 1)$ and n and $n + 1$ being consecutive natural numbers, one of them has to be even and thus product will be even also.

9. Prove that $2m + 5n^2 = 20$ has no solution in positive integers.

   Solution: Note that 0 is NOT a positive integer. Try cases: If $m = 1$ we need $5n^2 = 18$. If $m = 2$ we need $5n^2 = 16$. If $m = 3$ we need $5n^2 = 14$. If $m = 4$ we need $5n^2 = 12$. None of these are possible because 4 does not divide 18, 16, 14 or 12.

   If $m = 5$ we need $5n^2 = 10 \implies n^2 = 2$. But $\sqrt{2}$ is not an integer.

   If $m = 6$ we need $5n^2 = 8$. if $m = 7$ we need $5n^2 = 6$. If $m = 8$ we need $5n^2 = 4$. If $m = 9$ we need $5n^2 = 2$. Again, none of these are possible because 5 does not divide 8,6,4 or 2.

   But that is all because if $m \geq 9$ we would need $5n^2$ to be 0 or negative, in other words, n cannot be a positive integer.

   An easier proof would wrap up all the cases in which we get m equals something that is not a multiple of 5, into one line. Equivalently, we would show that m has to be a multiple of 5 in order for solution to exist:

   $$2m+5n^2 = 20 \implies 5n^2 = 20-2m = 2(10-m) \implies 5|10-m \implies 5|m \implies m = 5, 10, 15, ...$$

   From here you can eliminate 5 as above and $m = 10, 15$, etc., would make $5n^2$ equal to 0 or negative.

HOMEWORK 3 (due on wed, 6/12; no late hw).

10. Prove if true or prove that it is false using counterexample:

    If $n|ab$ then $n|a$ or $n|b$.

    HINT: This is true only for prime numbers. Give a counterexample by taking n that is not a prime and divides product of two numbers without dividing either.

    Solution:

11. Prove that $m^3 + 2n^2 = 36$ has no solutions in positive integers.

    HINT: Start with $m = 0$. What are the possibilities for n ? Then try $m = 1, m = -1, m = 2, m = -2$ etc., and show there is no n that will satisfy the equation in each case.

    Solution:

$$m = 1 \implies 1 + 2n^2 = 36 \implies 2n^2 = 35 \implies n = \sqrt{17.5}$$
$$m = 3 \implies 27 + 2n^2 = 36 \implies 2n^2 = 9 \implies n = \sqrt{9.5}$$

    None of these are integers.

    You can also say that if m is odd then m^3 is odd and then we get that $36 - m^3$ is odd while $36 - m^3 = 2n^2$, an even number.

    If $m \geq 4$ we get $36 - m^3 < 0$ so it cannot equal $2n^2$ which is always positive.

    When $m = 2$ we get $8 + 2n^2 = 36 \implies 2n^2 = 28 \implies n = \sqrt{14}$ which is also not an integer.

    NOTE: This equation actually does not have solutions for all integers!

    The proof for all odd integers is the same: If m is odd you get that $36 - m^3$ is odd regardless of whether m is positive or negative. So it cannot equal $2n^2$.

    If m is even then letting $m = 2k$ we get $36 + m^3 = 36 + 8k^3 = 4(9 + 2k^3)$.

    This is 4 times an odd number whereas $2n^2$ can never equal 4 times an odd number: if n were odd then we get that $2n^2$ is 2 times an odd number and if n were even we get $2n^2$ equals 8 times an odd number. Neither can equal 4 times an odd number.

12. Prove that $\sqrt[3]{2}$ is irrational.

    [Proof similar to that of $\sqrt{2}$ being irrational].

    Solution:

    If $\sqrt[3]{2} = m/n$ with m and n having no common factors (we can always write any rational number like this), then

$$\sqrt[3]{2} = \frac{m}{n} \implies 2 = \frac{m^3}{n^3} \implies 2n^3 = m^3 \implies 2|m^3 (\text{ means 2 divides } m^3)$$

$$\implies 2|m \text{ (prime factors of } m \text{ and } m^3 \text{ are same)} \implies m = 2k \text{ (for some integer } k)$$
$$\implies m^3 = 8k^3 \implies 2n^3 = 8k^3 \implies n^3 = 4k^3 \implies 2|n^3 \implies 2|n.$$

But we assumed that m, n have no common factors, so 2 *cannot* divide both!

13. Prove or disprove: If x is nonzero and rational and y is irrational then xy is irrational.

    Solution: Proof by contrapositive:

    Assume xy is rational. Then we would get $xy/x = y$ is rational because we showed that quotient of two rational numbers is rational.

    This contradicts the fact that y is irrational.

14. Prove that if $d|a$ and $d|b$ then $d|ma + nb$.

    Solution: Write $a = dk, b = dl$ because we know d divides them.

    Then $ma + nb = mdk + ndl = d(mk + nl)$.

    This shows that d divides $ma + nb$.