CSCI 0220 **Discrete Structures and Probability** F. Preparata

Homework 3

Solution Key

All homeworks are due at 1:00pm in the CS22 bin on the CIT second floor, opposite the elevators.

Write your full name *and the problem number on each piece of paper you hand in and then staple.*

Reading*:*

Problem 3.1

For all integers $n \geq 0$, prove $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9.

- The statement holds for the base case $n = 0$. $0^3+(0+1)^3+(0+2)^3 = 9$ Clearly, 9 divides 9.

  Next, assume the inductive hypothesis. That is for some $n = k$, $k^3 + (k+1)^3 + (k+2)^3 = 9 * a$ for some integer a.

$$k^3 + (k+1)^3 + (k+2)^3 = 9a$$
$$k^3 + (k+1)^3 + (k+2)^3 + 9(k^2 + 3k + 3) = 9a + 9(k^2 + 3k + 3)$$
$$(k+1)^3 + (k+1+1)^3 + (k+1+2)^3 = 9a + 9(k^2 + 3k + 3)$$
$$(k+1)^3 + ((k+1)+1)^3 + ((k+1)+2)^3 = 9(a + k^2 + 3k + 3)$$

  Above, it is shown that for n=k+1, $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9. From the basis and inductive steps, it follows by the principle of mathematical induction that for for all integers $n \geq 0$, $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9.

Problem 3.2

Prove that $\sqrt[3]{3}$ is irrational. (You may assume the following Lemma: "For any integer n, if n^3 is divisible by 3, then n is divisible by 3.")

Proof by contradiction. Assume that $\sqrt[3]{3}$ is rational. Then there are integers p, q such that $\sqrt[3]{3} = \frac{p}{q}$, and p and q have no common factors. Then $\sqrt[3]{3}^3 =$

$3 = \frac{p^3}{q^3}$. So $q^3 = 3p^3$, so q^3 is divisible by 3, so q is divisible by 3. That means that $q = 3k$ for some integer k. So we can say that $(3k)^3 = 27k^3 = 3p^3$, so $9k^3 = p^3$. That means p^3 is divisible by 9, so it is divisible by 3, so p is also divisible by 3. Now, both p and q are divisible by 3, but we said before that p and q had no common factors! Thus, our initial assumption must have been false, and $\sqrt[3]{3}$ is irrational. This concludes the proof.

Problem 3.3

Prove that $\forall n \in \mathbb{Z},\ n^2 + 3n - 5$ *is odd using division of cases.*

Consider two cases: n is odd and n is even.
Case 1: n is odd.

$$n = 2k + 1,\ k \in \mathbb{Z}$$

$$\begin{aligned} n^2 + 3n - 5 &= (2k+1)^2 + 3(2k+1) - 5 \\ &= (4k^2 + 4k + 1) + (6k + 3) - 5 \\ &= 4k^2 + 10k - 1 \\ &= 2(2k^2 + 5k - 1) + 1 \\ &= 2k' + 1,\ k' \in \mathbb{Z} \end{aligned}$$

Case 2: n is even.

$$n = 2k$$

$$\begin{aligned} n^2 + 3n - 5 &= (2k)^2 + 3(2k) - 5 \\ &= 4k^2 + 6k - 5 \\ &= 2(2k^2 + 3k - 3) + 1 \\ &= 2k' + 1,\ k' \in \mathbb{Z} \end{aligned}$$

Problem 3.4

Using the well-ordering principle, prove that every integer n *greater than 1 is either a prime number or a product of prime numbers.*

Claim: Every integer n greater than 1 is either a prime number or a product of prime numbers.

Proof: n must be either prime or composite.

If n is prime, the claim is true.

Suppose n is not prime. Then there exists some set of numbers $D = d_1, ..., d_k$ such that $\forall x \in D, x > 1 \wedge x|n$ and $\forall y \in \mathbb{Z} \wedge y \notin D,\ y = 1$ or $y = n$ or $y \not| n$. This set is the set of divisors of n, excluding 1 and n.

Because D by definition is a finite set of positive integers, we know by the well-ordering principle that it must have a least element. Assume that d_1 is that least element.

$d_1|n$, so $\exists c_1 \in \mathbb{Z}$ such that $n = c_1 d_1$.

Consider two cases: d_1 is prime, or d_1 is composite.

If d_1 is composite, by definition there must be two integers $a_1, a_2 \in \mathbb{Z}^{>1}$ such that $a_1, a_2 \neq d_1$ and $d_1 = a_1 a_2$. Then $n = c_1 d_1 = c_1 a_1 a_2 = c_2 a_2$. Because c_2 is a product of integers, it must also be an integer, so by definition n is divisible by a_2. We know that $1 < a_2 < d_1$, which contradicts our assumption that d_1 is the least element in the set of divisors. Because d_1 being both composite and the smallest element of D leads to a contradiction, d_1 cannot be composite and must therefore be prime.

We then have $n = c_1 d_1$, where d_1 is prime and $1 < c_1, d_1 < n$. To prove that n is prime or a product of primes, we must prove that c_1 is either prime or a product of primes. If c_1 is prime, n is the product of two primes, c_1 and d_1. If c_1 is composite, we can apply similar reasoning to the above to determine that $c_1 = c_2 d_2$, where d_2 is prime (and the minimal divisor of c_1 greater than one) and $1 < c_2, d_2 < c_1$.

This can be applied repeatedly, producing a sequence $n = c_0 > c_1 > c_2 > ... > c_m > 1$ where $\forall i,\ c_i = d_{i+1} c_{i+1}$ for d_{i+1} the smallest divisor of c_i (which, as shown above, must be prime). Because each c_i is required to be a positive integer greater than 1 and the sequence is strictly decreasing, c_i must be a finite set and this process will terminate.

We have shown that each c_i is the product of c_{i+1} and a prime. To show that n is a product of primes, we must show that the final element of the sequence, c_m, is prime. If c_m were not prime, it would by definition have at least two factors, and the reasoning above could be applied again to decompose it further into a product of a prime d_{m+1} and another integer

c_{m+1}, both of which must be smaller than c_m. However, this contradicts the assumption that c_m is the smallest element of the finite set defined above, as c_{m+1} would also be a member, so c_m must be prime.

We have now shown constructively that n is either a prime or a product of primes (specifically, $n = d_1 d_2 \cdots d_m c_m$).

Problem 3.5

Given any integers a, b, c, if $a - b$ is odd and $b - c$ is even, what can you say about the parity (odd/even) of $a - c$? Support your answer with a proof.

For $a, b, c \in \mathbb{Z}$, if $a - b$ is odd and $b - c$ is even, then $a - c$ is odd.

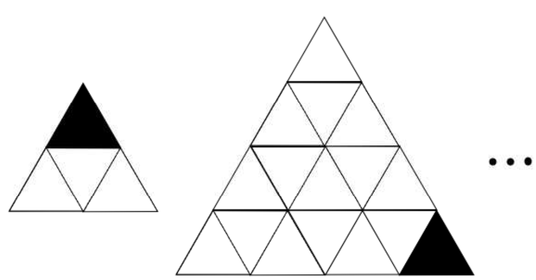
Proof. From the definitions of even and odd, $\exists m, n \in \mathbb{Z}$ such that $a - b = 2m + 1$ and $b - c = 2n$.
Then:

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= (2m + 1) + 2n \\ &= 2(m + n) + 1 \end{aligned}$$

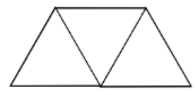
Let $p = m + n$. The set of integers is closed under addition (the sum of two integers is also an integer), so p is an integer. Therefore $a - c = 2p + 1$ is odd by the definition of odd.

Problem 3.6

Consider the set of equilateral triangles with sides of length 2^n, where $n > 0$, with one triangle $\triangle$ of side length 1 missing from any *one of the three corners of the larger triangle (see picture below).*

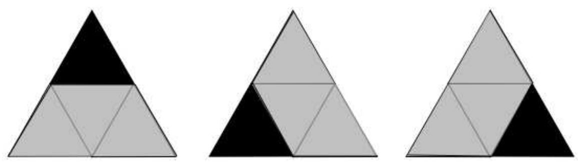


Show that each figure in the set can be covered with tiles composed of three side-length-1 triangles △ in the form:



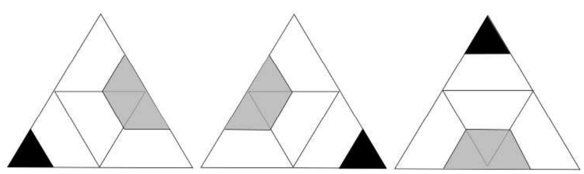
Proof by induction.

We first consider the base case in which $n = 1$, so the triangle has sides of size 2^1. We can show the solution for the three cases in which each of three corners is missing. (You can simply place one shape over the remaining part of the triangle.)



We now assume that we can tile a triangle with sides of length 2^k, and use this assumption to show that we can tile a triangle with sides of length 2^{k+1}.

In each of the three cases in which one of the three corners is missing, we can place a tile along the side of the image to create four triangles with sides of length 2^k with one 1 x 1 x 1 triangle missing. This can be accomplished as follows:



Since each of the four smaller triangles are equilateral triangles with sides of length 2^k with one square "missing," we can use the inductive hypothesis to tile the remaining area.

Since the claim is true for the base case and for the case where $n = k + 1$ assuming it is true for $n = k$, the claim is thus true by induction.