

MATH 8: ASSIGNMENT 22

MARCH 31, 2019

1. PRIME FACTORIZATION

Here is a useful fact about prime numbers:

Theorem. *If p is a prime number and a, b are integers such that ab is divisible by p , then at least one of a or b is divisible by p .*

Proof. To prove this, we will use the fact that the gcd of two numbers is always a factor of both numbers.

First, because p is prime, its only factors are p and 1; since $\gcd(p, a)$ is a factor of p , we get therefore that $\gcd(p, a) = p$ or $\gcd(p, a) = 1$.

In the case where $\gcd(p, a) = p$, then p must be a factor of a by the fact that greatest common divisors are factors of both numbers. In the case where $\gcd(p, a) = 1$, using Euclid's Algorithm we can write $1 = xp + ya$ for some integers x, y , and thus $b = (xp + ya)b = xpb + yab$. Then, by the definition of divisibility, (ab is divisible by p) $\implies (ab = kp)$ for some integer k , thus $xpb + yab = xpb + ykp = pxb + pky = p(xb + ky)$, therefore $b = p(xb + ky)$ and hence b is divisible by p , again by the definition of divisibility. \square

To continue on our journey through numbers, we explore the following idea: every number has a unique representation in terms of prime numbers - in a sense, one can understand the nature of a number by knowing which primes comprise it. This concept solidifies the relationship between primes and divisibility, via the following theorem:

Theorem (Fundamental Theorem of Arithmetic). *For any integer n such that $n > 1$, n can be written in a unique way as the product of prime numbers: namely, there are some prime numbers p_1, p_2, \dots, p_k (allowing repetition) such that $n = p_1 p_2 \dots p_k$; moreover, if there are prime numbers q_1, q_2, \dots, q_k such that $n = q_1 q_2 \dots q_k$, then the q_i can be rearranged so as to coincide exactly with the p_i (i.e., they are the same set of prime numbers).*

Proof. First we must prove that all numbers have a prime factorization (at least one). We can do this by contradiction: assume that there are numbers that do not have a prime factorization. Then there is a smallest one; call it n . Because n does not have a prime factorization, it cannot itself be prime, therefore $n = ab$ for positive integers $a < n, b < n$. Use the fact that $a < n$ to deduce that a does have a prime factorization - and similarly for b - then we can write n as the product of the prime factorizations of a and b , which is a contradiction.

To prove uniqueness of prime factorizations, suppose $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_k$. We will assume first that there are no common factors, i.e. $p_i \neq q_j$ for all i, j . Then $p_1 p_2 \dots p_k = q_1 q_2 \dots q_k \implies (q_1 q_2 \dots q_k$ is divisible by p_1).

Using our first theorem, we can deduce from this that one of the integers from q_1 through q_k is divisible by p_1 (the details are left as an exercise). Let q_i be divisible by p_1 ; then q_i is prime, so its only factors are 1 and q_i , but p_1 can equal neither 1 nor q_i because p_1 is a prime number (hence greater than 1) that is distinct from all the q_1 through q_k . This is a contradiction, therefore there must be some common factors in the equality $p_1 p_2 \dots p_k = q_1 q_2 \dots q_k$.

We can then cancel out the common factors, repeat the preceding argument, and eventually deduce that $1 = 1$, i.e. that the p_1 through p_k and the q_1 through q_k are actually the same set of prime numbers. \square

2. HOMEWORK

1. Determine the prime factorization of:
 - (a) 10
 - (b) 20
 - (c) 35
 - (d) 60
 - (e) $64 \cdot 81$
 - (f) 10^k for $k \in \mathbb{Z}$
2. Determine how many factors each of the following numbers have:
 - (a) 10
 - (b) 60
 - (c) 97
 - (d) 99
 - (e) 10^5
 - (f) $34 \cdot 35$
3. Use Euclid's Algorithm to solve the following:
 - (a) Determine the gcd of 10 and 101
 - (b) Determine the gcd of 99 and 1001
 - (c) Determine the gcd of 22 and 16
 - (d) Write $\gcd(22, 16)$ in the form $22k + 16l$
 - (e) Are there any integer solutions to the equation $14k + 42l = 1$? How about $14k + 42l = 2$?
 - (f) Determine the smallest number n such that $32k + 36l = n$ has integer solutions for k and l .
4. Prove that if a_1, a_2, \dots, a_k are integers such that the product $a_1 a_2 \dots a_k$ is divisible by a prime number p , then one of the numbers a_1 through a_k is divisible by p .
5.
 - (a) Prove that, given any nonzero integer a , every prime number that appears in the prime factorization of a^2 must appear an even number of times.
 - (b) Deduce that there are no nonzero integers a, b such that $a^2 = 2b^2$. [Hint: how many times does 2 appear in the prime factorization of $2b^2$?]
 - (c) We say a number x is *rational* if it can be written as a fraction of integers, i.e. $x = \frac{a}{b}$ for some integers a, b (where b is nonzero). Prove that $\sqrt{2}$ is irrational (not rational). [Hint: try a proof by contradiction.]
6. Prove that there are no integer solutions to the pair of equations $a + b = 7$, $a^2 + b^2 = 19$. [Hint: try squaring one of the equations.]
7. Suppose the sum of a rectangle's area and perimeter is 139. Can such a rectangle have integer side lengths?
8. Assuming size/memory is not an issue, can you find a way to encode a sequence of positive integers r_1, r_2, \dots, r_k as a single integer n , such that it is possible to recover the numbers r_i in order from n ?