MATH 8: HANDOUT 21
NUMBER THEORY 3: PRIME FACTORIZATION

EUCLID'S ALGORITHM COROLLARIES

Theorem. *Let $d = \gcd(a, b)$. Then a number n can be written in the form*

$$n = xa + yb$$

for some $x, y \in \mathbb{Z}$ if and only if n is a multiple of $d = \gcd(a, b)$

Indeed, last time we proved (using Euclid's algorithm) that d can be written in this form. But then any multiple $n = kd$ can also be written in such a form: if $d = ax + by$, then $kd = a \cdot (kx) + b \cdot (ky)$.

Conversely, if $n = ax + by$, then since a, b are multiples of d, so is $ax + by$.

In particular, if $\gcd(a, b) = 1$, then one can write $1 = ax + by$.

As a corollary, we get the following result.

Theorem. *Let $a|bc$. If $\gcd(a, b) = 1$, then $a|c$.*

Proof. Since $\gcd(a, b) = 1$, we can write $ax + by = 1$. Multiplying by c, we get

$$c = acx + bcy$$

Since bc is divisible by a, we see that both summands are divisible by a. Thus, c is divisible by a. □

For example, if $11n$ is divisible by 6, then n must be divisible by 6, since 6 and 11 are relatively prime

PRIME FACTORIZATION

As a very special case of the result in the last section, we get the following.

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

Indeed, if m is not divisible by p, then $\gcd(m, p) = 1$, so we can use the theorem above to show that n is divisible by p.

(This statement may seem obvious. It is not: try arguing why it must be true without using Euclid's algorithm and you will see that your arguments will run in circles.)

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)**.** *Any integer $n > 1$ can be written in a unique way as the product of prime numbers: namely, there are some prime numbers p_1, p_2, ..., p_k (allowing repetition) such that $n = p_1 p_2 ... p_k$; moreover, if there are prime numbers q_1, q_2, ..., q_l such that $n = q_1 q_2 \ldots q_l$, then $k = l$ and 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. We had already proved before that any integer $n > 1$ can be written as product of primes.

To prove uniqueness of prime factorizations, suppose $n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l$. Then by the theorem above, one of q_i must be divisible by p_1. Since q_i are prime, it is only possible if $q_i = p_1$. Reordering the q's if necessary, we can make it so that $q_1 = p_1$, so $n = p_1 p_2 \ldots p_k = p_1 q_2 \ldots q_l$.

Dividing both sides by p_1, we get $p_2 \ldots p_k = q_2 \ldots q_l$. Same arguments as above tell us that $p_2 = q_j$ for some j. Repeating these arguments allows us to match each p_i with one of the factors q_j, i.e. that the p_1 through p_k and the q_1 through q_l are actually the same set of prime numbers. □

Grouping all copies of the same prime number p together, we can also write the prime factorization for a positive integer in the form

$$n = p_1^{a_1} \ldots p_k^{a_k}$$

where all p_i are *distinct* prime numbers.

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 22 and 16
  (b) Write $\gcd(22, 16)$ in the form $22k + 16l$
  (c) Are there any integer solutions to the equation $14k + 42l = 1$? How about $14k + 42l = 2$?
  (d) Determine the smallest number n such that $32k + 36l = n$ has integer solutions for k and l.

4. (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. [Hint: try a proof by contradiction.]

5. In how many zeros does the number 100! end?

6. Write all divisors of $2^2 3^4$

7. Find $\gcd(2^3 \cdot 3^4 \cdot 5, 2^2 \cdot 5^2 \cdot 7)$ using prime factorizations.

8. Let $m = p_1^{a_1} \ldots p_k^{a_k}$ be the prime factorization of m. Show that then all positive divisors of m are numbers of the form $d = p_1^{b_1} \ldots p_k^{b_k}$, for all possible choice of exponents b_i satisfying $0 \le b_i \le a_i$.
  How many divisors does m have? Express your answer in terms of a_i.

9. Let m, n be positive integers, and let
$$m = p_1^{a_1} \ldots p_k^{a_k}$$
$$n = p_1^{b_1} \ldots p_k^{b_k}$$
be their prime factorizations. Note that we have written them so that they use the same primes — we can always do that, if necessary making some exponents 0 (e.g. writing $2^3 \cdot 3^4 \cdot 5$ as $2^3 \cdot 3^4 \cdot 5 \cdot 7^0$).
  Prove that $\gcd(m, n) = p_1^{c_1} \ldots p_k^{c_k}$, where $c_i = \min(a_i, b_i)$

10. Assuming size/memory is not an issue, can you find a way to encode a sequence of positive integers $r_1, r_2, \ldots, r_k$ as a single integer n, such that it is possible to recover the numbers r_i in order from n? (The length of the sequence is not fixed: your algorithm should be able to encode sequences of any (finite) length.)