

Problem Set VII

NUMBER THEORY AND ARITHMETIC

Due Mar. 18th

Think about all the problems and try to come up with ideas to solve them and write those.

Note: This time you only need to do only one of the problems but if you haven't done enough for the last week's problems, go back and do one or two problems there.

Let's first recall a couple of things we discussed in class:

- **Fundamental Theorem of Arithmetic.** Every integer $n \geq 2$ is either a prime or else can be written as a product of (not necessarily distinct) primes. Modulo the order in which the primes appear, there is exactly one way to decompose an integer into primes.

For example, $24 = 2 \times 2 \times 2 \times 3$, $3381 = 3 \times 7 \times 7 \times 23$.

In a fancier language, the theorem says: Every integer $n \geq 2$ can be written as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where $p_1 < p_2 < \cdots < p_k$ are primes, each power a_j is at least 1, and $k \geq 1$. This decomposition is unique in the sense that if we have another decomposition

$$n = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

into primes $q_1 < q_2 < \cdots < q_l$ and b_j at least one, then $k = l$, $p_j = q_j$ and $a_j = b_j$ for all $j = 1, 2, \dots, k$.

- If a_1, a_2, \dots, a_n are integers then we denote the greatest common divisor of those by $\gcd(a_1, a_2, \dots, a_n)$.
1. (a) If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of $n \geq 2$ as in above, find a formula for the number of divisors of n . (*Hint:* First try it for simpler cases when $n = p^a$ has only one prime divisor or $n = p^a q^b$ has two prime divisors and then generalize that.)
(b) An even number is divisible by 5 and has 35 divisors. What it can be?
 2. (a) Let n be an integer which is not divisible by any integer $2 \leq k \leq \sqrt{n}$. Prove that n is prime.
(b) If p is a prime prove that $p \mid \binom{p}{k}$, whenever $0 < k < p$.
(c) Prove that $p \mid n^p - n$, for any $n \in \mathbb{N}$.

3. For integers a and b show the following:

(a) $\gcd(a, b) = \gcd(a, a - b)$,

(b) if $0 \leq r < b$ is the remainder of a when divided by b prove that $\gcd(a, b) = \gcd(b, r)$,

(c) prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for any $n \in \mathbb{N}$.

4. If $\gcd(a, b) = 1$, prove that

(a) $\gcd(a - b, a + b) \leq 2$,

(b) $\gcd(a - b, a + b, ab) = 1$,

(c) $\gcd(a^2 - ab + b^2, a + b) \leq 3$.