MATH 215: LECTURE 4- MORE ON NUMBER THEORY

TOM BENHAMOU
UNIVERSITY OF ILLINOIS AT CHICAGO

The purpose of this lecture is to provide more advanced and complex proofs which appears in number theory.

1. Basic theorems in Number theorey

1.1. The division theorem.

One of the most basic theorems in Number theory is the division theorem. It is an example of an existence and uniqueness theorem.

Remark 1.1. Uniqueness of a property means that there are no two distinct object with that property. So in order to prove uniqueness, we usually take two objects with the property and prove that they are not distinct i.e. they are equal.

Theorem 1.2. *For any integers n, m, such that $m > 0$ there exist unique integers r, q such that:*

$$n = q \cdot m + r, \quad 0 \leq r < m$$

q is called the *quotient* and r is called the *remainder*.

Proof. Let n, m be integers and suppose that $m > 0$. Proving existence and uniqueness are two different tasks, hence we split the proof into two parts:

(1) Existance: We want to prove that there exist natural numbers k, r such that $n = km + r$ and $0 \leq r < m$. For this, consider the set $S = \{n - am \mid a \in \mathbb{Z}, \text{ and } n - am \geq 0\}$. Clearly $S \subseteq \mathbb{N}$, and we claim that $S \neq \emptyset$.
   (a) If $n \geq 0$, then for $a = 0$ we hanve that $n = n - am \in S$, hence $S \neq \emptyset$.
   (b) If $n < 0$, we let $a = n$. Since $m \geq 1$, we conclude that $1 - m \leq 0$ and:
   $$n - am = n - nm = n(1 - m) \geq 0$$
   So $n - am \in S$ and $S \neq \emptyset$.

   Now we need to use the feature of the natural numbers we discussed in the previous chapter, that every non-empty set of natural numbers has a minimal element. Denote by $r = \min(S)$. In particular $r \in S$ so there is q such that $n - qm = r$ and $n = qm + r$. We still need to prove that $0 \leq r < m$. Since $r \in S \subseteq \mathbb{N}$, we have that $r \geq 0$.

Date: October 21, 2022.

To see that $r < m$, suppose toward a contradiction that $r \geq m$ and denote by $r' = r - m$. Then $r > r' \geq 0$, since $r \geq m \geq 0$. Also $r' = r - m = n - qm - m = n - (q+1)m$, hence $r' \in S$. This is a contradiction to the minimality of r.

(2) Uniqueness: To prove uniqueness we assume that r_0, q_0 and r_1, q_1 both satisfy the property of the theorem, namely

$$n = q_0 m + r_0,\ n = q_1 m + r_1,\ 0 \leq r_0, r_1 < m$$

and we need to prove that $q_0 = q_1$, $r_0 = r_1$. we conclude that $q_0 m + r_0 = q_1 m + r_1$ Let us split into cases:

(a) If $r_0 \leq r_1$, then $(q_0 - q_1)m = r_1 - r_0 \geq 0$. Now $0 \leq r_1 - r_0 < m$ and therefore $q_0 - q_1$ must be a natural number. Assume toward a contradiction the $q_0 - q_1 \geq 1$, then $m > r_1 - r_0 = (q_0 - q_1)m \geq m$, contradiction. Hence $q_0 - q_1 = 0$ and $q_0 = q_1$. Also we conclude that $r_1 - r_0 = 0$ and therefore $r_1 = r_0$.

(b) The case $r_1 \leq r_0$ is symmetric.[1]

□

Definition 1.3. Let n be any integer and $m > 0$. We denote by $n \mod m$ the remainder $0 \leq r < m$ of the division of n by m.

Definition 1.4. We say that n_1 and n_2 are *congruent modulo m* if

$$n_1 \mod m = n_2 \mod m,$$

and we denote this by $n_1 \equiv n_2 \mod m$.

Exercise. *Prove the following statements:*

(1) For any integers n_1, n_2 and $m > 0$ $n_1 \equiv n_2 \mod m$ if and only if $n_1 - n_2$ is divisible by m.

(2) For every integers n and $m > 0$, $n \equiv (n \mod m) \mod m$

1.1.1. *Greatest common divisor.* Among the most useful definitions in number theory is the definition of the greatest common divisor of two integers:

Definition 1.5. Let $n_1, n_2 \in \mathbb{Z}$ be any non zero integers. The *greatest common divisor* of n_1, n_2, denoted by $gcd(n_1, n_2)$ is the largest (positive) number d such that d divides both n_1 and n_2.

Exercise. *(1) $gcd(n_1, n_2) \leq n_1, n_2$.*

(2) $gcd(n_1, n_2) = n_1$ if and only if n_1 divides n_2.

Proposition 1.6. *Suppose that $n_1, n_2 \neq 0$ are any integers, and $r = n_1 \mod n_2$. Then $gcd(n_1, n_2) = gcd(r, n_2)$*

For example, to compute $gcd(90, 12)$ we can calculate $90 = 7 \cdot 12 + 6$ thus $6 = 90 \mod 12$ and by the proposition $gcd(90, 12) = gcd(6, 12) = 6$.

[1] This symmetry occurs when the assumptions on r_0, r_1 are identical and therefore we can simply repeat the proof switching between r_0, r_1.

Proof. Let q be such that $n_1 = qn_2 + r$. Denote $d_1 = gcd(n_1, n_2)$ and $d_2 = gcd(r, n_2)$ and we want to prove that $d_1 = d_2$. On one hand, d_2 divides r and n_2 and therefore it divides $qn_2 + r = n_1$. Since $d_1 = gcd(n_1, n_2)$ is the maximal number dividing both n_1 and n_2 we get that

$$(I) \;\; d_2 \leq d_1$$

On the other hand, d_1 divides both n_1 and n_2 and therefor it divides $n_1 - qn_2 = r$. Again by maximality of $d_2 = gcd(r, n_2)$ we have that

$$(II) \;\; d_1 \leq d_2$$

From $(I) + (II)$ we see that $d_1 = d_2$. □

Euclidean algorithm: The previous proposition suggests an algorithm to compute the greatest common divisor of two numbers $n_1 \geq n_2 \neq 0$:

(1) If n_2 divides n_1, $gcd(n_1, n_2) = n_2$.
(2) Otherwise, compute $r = n_1 \mod n_2$ and repeat steps $(1) + (2)$ with $n_2 \geq r$.

For example, let us compute $gcd(378, 132)$:

- $378 = 2 \cdot 132 + 114$ (hence $378 \mod 132 = 114$).
- $132 = 114 + 18$.
- $114 = 6 \cdot 18 + 6$.
- 6 divides 18 hence $gcd(378, 132) = 6$.

Definition 1.7. Two integers $n_1, n_2 \neq 0$ are called *coprime* is $gcd(n_1, n_2) = 1$.

Example 1.8. $gcd(10, 21) = 1$ hence $10, 21$ are coprime. Since 3 divides both $15, 18$, $gcd(15, 18) > 1$ (an actually equals 3) we conclude that $15, 18$ are not coprime.

Proposition 1.9. *Let $n, m \neq 0$ be any integers, and $d = gcd(n, m)$. Then $\frac{n}{d}, \frac{m}{d}$ are coprime.*

Proof. Suppose not, then $gcd(\frac{n}{d}, \frac{m}{d}) = 1$ and there is $k > 1$ dividing both $\frac{n}{d}, \frac{m}{d}$. Then there are m_1, m_2 such that $km_1 = \frac{n}{d}$, $km_2 = \frac{m}{d}$. It follows that $dkm_1 = n$ and $dkm_2 = m$, hence $d < dk$ divides both n, m which contradicts the maximality of $d = gcd(n, m)$. □

Theorem 1.10 (Beźout Identity). *For any integers $n_1, n_2 \neq 0$, n_1, n_2 are coprime, if and only if there are integers s, t such that $sn_1 + tn_2 = 1$*

Proof. Let n_1, n_2 be non zero integers and denote by $d = gcd(n_1, n_2)$. We need to prove an "if and only if" statement and we prove it by a double implication.

(1) $\underline{\Longleftarrow}$: Suppose that there are integers s, t such that $sn_1 + tn_2 = 1$. We want to prove that n_1, n_2 are coprime, namely that $d = 1$. Indeed, since d divides both n_1, n_2 it divides $sn_1 + tn_2$ and thus d divided 1. Since d is a positive, we conclude that $d = 1$.

(2) $\Longrightarrow$: Suppose that n_1, n_2 are coprime i.e. $d = 1$. We want to prove that there are integers s, t such that $sn_1 + tn_2 = 1$ Let $A = \{an_1 + bn_2 \mid a, b \in \mathbb{Z} \text{ and } an_1 + bn_2 > 0\}$. Clearly, $A \subseteq \mathbb{N}$. Also, note that $A \neq \emptyset$ since for example[2] $|n_1| = n_1 \cdot sign(n_1) + n_2 \cdot 0 \in A$. Therefore, there is a minimal number in the set A, denote $x = \min(A) > 0$. By the definition of A, there are $s, t \in \mathbb{Z}$ such that $x = sn_1 + tn_2$. we will prove that $x = 1$ and thus proving the implication. By the division theorem, find q, r such that

$$n_1 = qx + r \quad 0 \leq r < x$$

Now

$$r = n_1 - qx = n_1 - q(sn_1 + tn_2) = (1 - qs)n_1 + (-t)n_2$$

and since $1 - qs, -t$ are integers we conclude that either $r \in A$ in case $r > 0$ or $r = 0$. It is impossible that $r > 0$ since this would means that $r \in A$ is smaller than x which is the **minimal** member of A. Hence $r = 0$ and thus x divides n_1. Similarly, we prove that x divides n_2. Thus by the definition of gcd, $0 < x \leq d = 1$. we conclude that $x = 1$.

□

Corollary 1.11. *Suppose that a divides $b \cdot c$ and $gcd(a, b) = 1$. Then a divides c.*

Proof. Suppose that a divides bc and that $gcd(a, b) = 1$. We want to prove that a divides c. By the Beźout identity, there are s, t such that $1 = sa + tb$. Multiply the equation by c, to obtain $c = sac + tbc$. Clearly a divides sac. By the assumption of the corollary, a divides bc and also tbc. It follows that a divides $sac + tbc = c$. □

2. Prime numbers

Definition 2.1. A natural number $p > 1$ is called a *prime number* if the only natural numbers which divides p are $1, p$.

Example 2.2. 2,3,5,7,11,13 are prime numbers, which 4,6,8,9,10,12 are not. Clearly, every even number beside 2 is not a prime.

Exercise. *Suppose that p is a prime number and n is any integer. Then either p divides n, or p, n are coprime.*

In what comes next, we will need another variation on induction called *strong* or *complete* induction.

[2] $|n_1|$ denoted the absolute value of n_1 and $sign(n_1) = 1$ in case $n_1 > 0$ and $sign(n_1) = -1$ if $n_1 < 0$

2.1. **Complete induction.** Similar to regular induction, strong induction has three step: the induction base, the induction hypothesis, and the induction step. The only difference is with the induction hypothesis, in regular induction we assume for a general n that $q(n)$ holds and in the induction step we derive $q(n+1)$. In strong induction we assume that more, that for every $k \leq n$ $q(k)$ holds and derive $q(n+1)$ from all the previous cases. Practically, the structure of a prove by *complete induction/strong induction* is the following:

(1) The induction base: Prove $q(0)$ (or any other base).
(2) Induction hypothesis: Assume that for a general n, for every $k \leq n$, $q(k)$ holds.
(3) Induction step: Prove $q(n+1)$ from the induction hypothesis.

As an example we shall prove the following easy claim:

Proposition 2.3. *For any natural number $n > 1$, there is a prime number p such that p divides n.*

Proof. **The induction base**: For $n = 2$, we have that 2 is a prime and 2 divides 2.

Induction hypothesis: Suppose that for every $1 < k \leq n$, there is a prime p such that p divides k.

The induction step: Let us prove that there is a prime p dividing $n+1$. Let us split into cases:

(1) If $n+1$ is prime, define $p = n+1$, then p is a prime dividing $n+1$.
(2) If $n+1$ is not a prime, then there is $1 < m < n+1$ such that m divides $n+1$. It follows that $m \leq n$ and by the strong induction hypothesis there is a prime p such that p divides m. Since p divides m and m divides $n+1$ it follows that p divides $n+1$.

□

Theorem 2.4. *There are infinitely many primes.*

Proof. Suppose toward a contradiction that there are only finitely many primes $p_1, ..., p_n$. Consider the number $m = p_1 \cdot p_2 .... \cdot p_n + 1$. By the previous proposition there is a prime p such that p divides m. Since $p_1, .., p_n$ list all the primes, there is $1 \leq i \leq n$ such that $p = p_i$. Since p_i divides m and also p_i divides $p_1 ... p_n$, we have that p_i divides $m - p_1 ... p_n = 1$ hence p_i divides 1, so $p_i = 1$, contradicting the fact that p_i is prime. □

2.2. **Fundamental theorem of arithmetic.** The most important feature of primes is that every natural number can be decomposed into prime. This fact will be proven later on in this sub section. Let us start with a very useful lemma, called *Euclid's lemma*:

Lemma 2.5 (Euclid's lemma)**.** *Let p be a prime number which divides ab. Then either p divides a or p divides b.*

Corollary 2.6. *If p is a prime dividing $a_1....a_n$ and for every $i \neq j$ a_i, a_j are coprime, then there exists i such that p divides a_i*

Proof. Exercise. Hint: use Euclid lemma and (regular) induction on n, □

Proof. Suppose that p id a prime that divides ab. We wnt to prove that (p divides a) $\vee$ (p divides b). Let us split into cases:

(1) If p divides a, we are done.
(2) If p does not divide a, then p and a are coprime and by the Beźout identity there are integers s, t such that $1 = sa + tp$. Multiply by b the equation, then $b = sab + tp$. Since p divides both sab and tp, it also divides b, as wanted.

□

Theorem 2.7 (The fundamental theorem of arithmetics)**.** *Every natural number $x > 1$ can be decomposed uniquely to a product of prime numbers. Formally, there exists $p_1, .., p_n$ distinct primes and powers $k_1, ..., k_n$ such that $x = p_1^{k_1}...p_n^{k_n}$, moreover, if x admits another decomposition $x = q_1^{r_1}...q_m^{r_m}$ then $\{p_1, ..., p_n\} = \{q_1, ..., q_k\}$ and if $p_i = q_j$ then $k_i = r_j$.*

Proof. Let $x > 1$ be a natural number. This is an existence and uniqueness proof.

(1) Existence: Exercise. Hint: Use strong induction.
(2) Uniqueness: We will prove inductively on x, that x admits a unique prime decomposition.

The induction base: For $x = 2$, since 2 is the minimal prime, there cannot be a factorization of 2 into primes beside $2 = 2$

The induction hypothesis: suppose that for every $k \leq x - 1$, there is a unique factorization into primes.

The induction step: Let us prove that x has a unique factorization into primes. Indeed, suppose that

$$q_1^{r_1}...q_m^{r_m} = x = p_1^{k_1}...p_n^{k_n}$$

are two factorizations of x. Clearly p_1 divides the righthand side. Hence it divides $q_1^{r_1}...q_m^{r_m}$. Since for $i \neq j$, $q_i^{r_i}$ and $q_j^{r_j}$ are coprime, by Euclid's lemma we conclude that there is i such that p_1 divides $q_i^{r_i}$. It follows that there is m such that $p_1 m = q_i^{r_i}$

□

3. The existence of irrational numbers

Claim 3.0.1. *Every rational number $q = \frac{m}{n} \neq 0$ can be represented as $q = \frac{m'}{n'}$, where n', m' are coprime*[3].

[3] the fraction $\frac{m'}{n'}$ is called a *reduced fraction*.

Proof. Let $n, m \neq 0$ be any integers and let $d = gcd(n, m)$. By Proposition 1.9, $\frac{n}{d}, \frac{m}{d}$ are coprime. Moreover,

$$\frac{m}{n} = \frac{\frac{m}{d}}{\frac{n}{d}}$$

so we can let $m' = \frac{m}{d}$ and $n' = \frac{n}{d}$ to witness the theorem. □

Theorem 3.1. *$\sqrt{2}$ is irrational.*

Proof. Suppose toward a contradiction that $\sqrt{2}$ is rational. Then there are coprime integers n, m such that $\sqrt{2} = \frac{m}{n}$. It follows that $2 = \frac{m^2}{n^2}$ and $n^2 2 = m^2$, hence m^2 is even. It follows that m is even (why? prove it!) so there is k such that $m = 2k$ and $n^2 2 = (2k)^2 = 4k^2$. dividing the equation by 2 we have that $n^2 = 2k^2$, and by the same reasoning n should also be even. However, this is a contradiction to the choice of n, m being coprime on one hand and both even on the other hand. □

Exercise. *Prove that $\sqrt{18}$ is irrational.*

Proof. Suppose otherwise that $\sqrt{18}$ is rational, then

$$\sqrt{18} = \sqrt{9 \cdot 2} = \sqrt{9}\sqrt{2} = 3\sqrt{2}$$

It follows that $\sqrt{2} = \frac{\sqrt{18}}{3}$. Since fraction of rational numbers is rational we conclude that $\sqrt{2}$ is rational, contradiction. □