

MATH 110AH - FALL 2021

Pablo S. Ocal

based on "Lectures on Abstract Algebra"

by Richard S. Elman.

Section 2: Well-ordering and induction.

The well-ordering principle: Let $\emptyset \neq S \subseteq \mathbb{Z}^+$. Then S contains a least element: there exists $a \in S$ such that $a \leq x$ for all $x \in S$.

Proposition: Let $\emptyset \neq T \subseteq \mathbb{Z}$. Suppose that there is an $N \in \mathbb{Z}$ such

that $N \leq x$ for all $x \in T$ (i.e. T is bounded from below). Then

T contains a least element.

Similarly, if T is bounded from above, it contains a largest element.

Proposition: There is no integer N satisfying $0 < N < 1$.

Proof: Let $S = \{n \in \mathbb{Z} \mid 0 < n < 1\}$. If $\emptyset \neq S$ then there exists a least

element $N \in S$. Now $0 < N < 1$ implies $0 < N^2 < N < 1$ and

since $N \in \mathbb{Z}$ then $N^2 \in \mathbb{Z}$, so $N^2 \in S$ contradicting minimality. \square .

Proposition: Let $S \subseteq \mathbb{Z}^+$ and $1 \in S$. Suppose that if $n \in S$, then

$n+1 \in S$. Then $S = \mathbb{Z}^+$.

Proof: Let $T = \{n \in \mathbb{Z}^+ \mid n \notin S\}$. If $T = \emptyset$ then $S = \mathbb{Z}^+$. If

$T \neq \emptyset$ then there exists a least positive element $n \in T$. Then

$n \notin S$ and $n-1 \notin T$. Since $1 \notin T$ then $n > 1$ and $n-1 \in \mathbb{Z}^+$.

Then $n-1 \in S$, but by hypothesis $n \in S$, contradiction.

□.

Theorem: (Induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be a true or false

statement. Suppose we know that $P(1)$ is true, and that if $P(u)$ is

true then $P(u+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Theorem: (Induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be a true or false

statement. Suppose that if $P(m)$ is true for all $m \leq n$ positive

integers, then $P(n)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proposition: The product of any $n \geq 1$ consecutive positive integers is

divisible by $n!$, i.e. for all $m, n \in \mathbb{Z}^+$ we have: $\frac{m \cdot (m+1) \cdots (m+n-1)}{n \cdot (n-1) \cdots 2 \cdot 1} \in \mathbb{Z}^+$

Corollary: For every $n \in \mathbb{Z}^+$, there exist n consecutive composite positive

integers.

Corollary: Let $p > 1$ be a prime. Then p divides $\binom{p}{n}$ for all $1 \leq n \leq p-1$.

Section 3: The greatest integer function.

Another way of showing that the binomial coefficients are integers.

Definition: The greatest integer function: $[] : \mathbb{R} \longrightarrow \mathbb{Z}$

gives $[x]$ the greatest integer $[x] \leq x$ for $x \in \mathbb{R}$.

Proposition: For $x \in \mathbb{R}$ and $m, n \in \mathbb{Z}^+$, the following hold:

$$1) [x] \leq x < [x] + 1.$$

$$2) [x+m] = [x] + m.$$

$$3) \left[\frac{x}{m} \right] = \left[\frac{[x]}{m} \right].$$

$$4) [x] + [y] \leq [x+y] \leq [x] + [y] + 1.$$

5) $\left[\frac{n}{m} \right]$ is the number of integers among $1, \dots, n$ that are divisible by m .

Proof: (1), (2), (3), (4) are straightforward.

5) Let $m, 2m, \dots, jm$ all the positive integers below n and divisible

by m . Now $jm \leq n < (j+1)m$ so $j \leq \frac{n}{m} < j+1$ so $\left[\frac{n}{m} \right] = j$. \square .

Theorem: Let $n \in \mathbb{Z}^+$ and $p > 1$ a prime. Suppose that $p^e \mid n!$ but

$$e+1, 1 - \sum_{k=1}^{\infty} \lceil \frac{n}{p^k} \rceil$$

$$p \nmid u! \text{. Then: } e = \sum_{i=1}^r [p_i].$$

Corollary: Suppose that $a_1, \dots, a_r \in \mathbb{Z}^+$ with $a_1 + \dots + a_r = u$. Then

the multinomial coefficient $\frac{u!}{a_1! \cdots a_r!} \in \mathbb{Z}^+$.

Section 4: Division and the greatest common divisor.

Proposition: Let $r, u, m \in \mathbb{Z}$, the following hold:

1) If $r|m$ and $r|u$ then $r|au+bu$ for all $a, b \in \mathbb{Z}$.

2) If $r|u$ then $r|un$.

3) If $r|u$ and $u \neq 0$ then $|u| \geq |r| \geq r$.

4) If $m|u$ and $u|m$ then $u = \pm m$.

5) If $mn=0$ then $m=0$ or $n=0$.

6) If $mr=ur$ then $m=n$ or $r=0$.

Theorem: (Division Algorithm) Let $u \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then there exist

unique $q, r \in \mathbb{Z}$ satisfying $u = qm+r$ and $0 \leq r < m$.

Proof: We need to show existence and uniqueness.

Uniqueness: Let (q, r) and (q', r') satisfy the conclusion.

We have $qm+r=u=q'm+r'$ and $0 \leq r < m$, $0 \leq r' < m$.

WLOG suppose $r \leq r'$, then $0 \leq r' - r = (q - q')m$. If $q = q'$

then $r' - r = 0$ and we are done. If $q \neq q'$ then $r' - r > 0$

and $m \mid r' - r$. Thus $m \leq r' - r < r' < m$, a contradiction.

Existence: If $n > 0$, let $S = \{s \in \mathbb{Z}^+ \mid sn > n\} \subseteq \mathbb{Z}^+$. Since

$n > 0$ we have $m \geq 1$ so $(n+1)m = mn + m \geq n + m > n$ so

$n+1 \in S \neq \emptyset$. There exists a least integer $q+1 \in S$, so $qn \leq n$.

Now $qn \leq n < (q+1)n$, choose $r = n - qn \geq 0$, we then have:

$$0 \leq r = n - qn < (q+1)n - qn = m.$$

If $n < 0$, there exist $q', r' \in \mathbb{Z}$ with $|n| = q'm + r'$ and

$0 \leq r' < m$. If $r' = 0$ then $q = -q'$ and $r = 0$ work. If $r' \neq 0$

then $q = -q'-1$ and $r = m - r'$ work. \square .

Definition: Let $n, m \in \mathbb{Z}$ at least one non-zero. A $d \in \mathbb{Z}$ is called

a greatest common divisor if it satisfies the following:

i) $d > 0$,

ii) $d|m$ and $d|n$,

iii) If $e \in \mathbb{Z}$ satisfies $e|m$ and $e|n$, then $e|d$.

If $\gcd(u, v) = 1$ we say that they are relatively prime.

Theorem: Let $m, n \in \mathbb{Z}$ with $n \neq 0$. Then $\gcd(m, n)$ exists and is unique.

Theorem: (Euclidean Algorithm) Let $a, b \in \mathbb{Z}^+$ with $b \neq a$. Then

there exists $k \in \mathbb{Z}^+$ and equations:

$$a = bq_1 + r_1, \quad b = r_1 q_2 + r_2, \quad \dots, \quad r_{k-2} = r_{k-1} q_k + r_k, \quad r_{k-1} = r_k q_{k+1}$$

with: $0 < r_1 < b, \quad 0 < r_2 < r_1, \quad \dots, \quad 0 < r_k < r_{k-1}$

for $q_1, \dots, q_{k+1}, r_1, \dots, r_k \in \mathbb{Z}$.

Theorem: (General Euclid's Lemma) Let $a, b \in \mathbb{Z}$ relatively prime, $a \neq 0$.

If $a \mid bc$ for some $c \in \mathbb{Z}$, then $a \mid c$.

Corollary: If $p > 1$ prime satisfies $p \mid a_1 \dots a_r$ with $a_1, \dots, a_r \in \mathbb{Z}$, then

$p \mid a_i$ for some $1 \leq i \leq r$.

Corollary: Let $p > 1$ be a prime. Then p divides $\binom{p}{n}$ for all $1 \leq n \leq p-1$.

Proof: We know that $n! \mid p(p-1)\dots(p-n+1)$ since these are n

consecutive positive integers. If $1 < s < p$, then $\gcd(s, p) = 1$, so

$\gcd(n!, p) = 1$ so by Euclid's lemma $n! \mid (p-1)\dots(p-n+1)$.

Hence $p \cdot n! \mid p(p-1) \cdots (p-n+1)$, so $p \mid \frac{p(p-1) \cdots (p-n+1)}{n!}$. \square .

Proposition: Let $p \in \mathbb{Z}$, $|p| > 1$. Then p is prime if and only if whenever

$p \mid ab$ with $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Theorem: (Fundamental Theorem of Arithmetic) Let $n \in \mathbb{Z}$, $n > 1$.

Then there exist unique primes $1 < p_1 < \cdots < p_r$ and $e_1, \dots, e_r \in \mathbb{Z}$ such

that $n = p_1^{e_1} \cdots p_r^{e_r}$.

Proof: We need to show existence and uniqueness.

Existence: Let $S = \{n \in \mathbb{Z}^+ \mid n > 1 \text{ and it is not a product of primes}\}$.

If $S = \emptyset$, we are done. Suppose $S \neq \emptyset$, then there exists a minimal

$n \in S$. Since S does not contain any primes, n is not a prime.

Hence there exist $u_1, u_2 \in \mathbb{Z}^+$ such that $n = u_1 \cdot u_2$, $1 < u_1$, and

$1 < u_2$. By minimality of n we have $u_1, u_2 \notin S$, so u_1 and u_2 are

product of primes, so $n = u_1 \cdot u_2$ is a product of primes, contradiction.

Uniqueness: Suppose $p_1^{e_1} \cdots p_r^{e_r} = n = q_1^{f_1} \cdots q_s^{f_s}$ with $1 < p_1 < \cdots < p_r$ and

$1 < q_1 < \cdots < q_s$ primes and $e_1, \dots, e_r, f_1, \dots, f_s \in \mathbb{Z}^+$. WLOG $p_1 \leq q_1$,

since $p_1 \mid n$ by Euclid's Lemma $p_1 \mid q_i$, but $p_1 \leq q_i$ and both are prime so $i=1$ and $p_1 = q_1$. Dividing by $p_1 = q_1$, we obtain

$p_1^{e_1-1} \cdots p_r^{e_r} = n = q_1^{\delta_1-1} \cdots q_s^{\delta_s}$. Using induction, we are done. \square .

