Teoria dos Números (1.1 da ementa)

Prof. Rafael Alves Bonfim de Queiroz
rafael.queiroz@ufop.edu.br

- 1.1) Ordem e desigualdades, valor absoluto, indução matemática.

Order

- Observe that we define order in Z in terms of the positive integers N.
- All the usual properties of this order relation are a consequence of the following two properties of N:
  - P1 If a and b belong to N, then $a + b$ and ab belong to N.
  - P2 For any integer a, either $a \in N$, a $= 0$, or $-a \in N$.
- The following notation is also used:
  - $a > b$ means $b < a$: a is greater than b.
  - $a \leq b$ means $a < b$ or $a = b$: a is less than or equal to b.
  - $a \geq b$ means $b \leq a$: a is greater than or equal to b.

Inequalities

- The relations $<$, $>$, $\leq$ and $\geq$ are called inequalities in order to distinguish them from the relation $=$ of equality.
- Representation of the integers as points on a straight line, called the number line R
- We note that $a < b$ if and only if a lies to the left of b on the number line R . For example, $2 < 5$; $-6 < -3$; $4 \leq 4$; $5 > -8$; $6 \geq 0$; $-7 \leq 0$
- We also note that a is positive iff $a > 0$, and a is negative iff $a < 0$. (Recall "iff" means "if and only if")

Inequalities

- Proposition: The relation $\leq$ in Z has the following properties:
  - (i) $a \leq a$, for any integer a.
  - (ii) If $a \leq b$ and $b \leq a$, then $a = b$.
  - (iii) If $a \leq b$ and $b \leq c$, then $a \leq c$.
- Proposition (Law of Trichotomy): For any integers a and b, exactly one of the following holds: $a < b$, $a = b$, or $a > b$
- Proposition: Suppose $a \leq b$, and let c be any integer. Then:
  - (i) $a + c \leq b + c$.
  - (ii) $ac \leq bc$ when $c > 0$; but $ac \leq bc$ when $c < 0$.

Absolute Value

- The absolute value of an integer a. written $|a|$, is formally defined by if $a \geq 0$, $|a| = a$; if $a < 0$, $|-a| = a$
- Accordingly, $|a| > 0$ except when $a = 0$.
- Geometrically speaking, $|a|$ may be viewed as the distance between the points a and 0 on the number line R.
- Also, $|a - b| = |b - a|$ may be viewed as the distance between the points a and b. For example: (a) $|-3| = 3; |7| = 7; |-13| = 13$; (b) $|2 - 7| = |-5| = 5; |7 - 2| = |5| = 5$
- Some properties of the absolute value function follow.
- Proposition: Let a and b be any integers. Then:
  - (i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$
  - (ii) $-|a| \leq a \leq |a|$
  - (iii) $|ab| = |a||b|$
  - (iv) $|a \pm b| \leq |a| + |b|$
  - (v) $||a| - |b|| \leq |a \pm b|$

Mathematical Induction

- The principle of mathematical induction stated below essentially asserts that the positive integers N begin with the number 1 and the rest are obtained by successively adding 1.
- That is, we begin with 1, then $2 = 1 + 1$, then $3 = 2 + 1$, then $4 = 3 + 1$, and so on.
- The principle makes precise the vague phrase "and so on."

- **Princípio da Indução Matemática**: Seja S um conjunto de inteiros positivos com as duas propriedades a seguir:
  - (i) 1 pertence a S.
  - (ii) Se k pertence a S, então $k+1$ pertence a S.

  Então S é o conjunto de todos os inteiros positivos.
- **Princípio de Indução Matemática**: Seja P uma proposição definida sobre os inteiros $n \geq 1$ tal que:
  - (i) $P(1)$ é verdadeiro.
  - (ii) $P(k+1)$ é verdadeiro sempre que $P(k)$ for verdadeiro. Então P é verdadeiro para todo inteiro $n \geq 1$.

Example 1

- Let P be the proposition that the sum of the first n odd numbers is n^2 ; that is: $P(n) : 1 + 3 + 5 + \ + (2n - 1) = n^2$
- The *nth* odd number is $2n - 1$ and the next odd number is $2n + 1$.
- Clearly, $P(n)$ is true for $n = 1$; that is: $P(1) : 1 = 1^2$
- Suppose $P(k)$ is true. (This is called the inductive hypothesis.) Adding $2k + 1$ to both sides of $P(k)$ we obtain $1 + 3 + 5 + \ + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (2k + 1)^2$ which is $P(k + 1)$
- We have shown that P (k + 1) is true whenever P(k) is true. By the principle of mathematical induction, P is true for all positive integers n.

Example 2

- The symbol n! (read: n factorial) is defined as the product of the first n positive integers; that is: $1! = 1$, $2! = 2 \cdot 1 = 2$, $3! = 3 \cdot 2 \cdot 1 = 6$, and so on.
- This may be formally defined as follows:
  $1! = 1$ and $(n + 1)! = (n + 1)(n!)$, for $n > 1$
- Observe that if S is the set of positive integers for which ! is defined, then S satisfies the two properties of mathematical induction.
- Hence the above definition defines ! for every positive integer.
- There is another form of the principle of mathematical induction which is sometimes more convenient to use. Namely:
- Theorem (Induction: Second Form): Let P be a proposition defined on the integers $n \geq 1$ such that:
  - (i) $P(1)$ is true.
  - (ii) $P(k)$ is true whenever $P(j)$ is true for all $1 \leq j < k$.
  - Then P is true for every integer $n \geq 1$.

Well-Ordering Principle

- A property of the positive integers which is equivalent to the principle of induction, although apparently very dissimilar, is the well-ordering principle
- Teorema [**Princípio da Boa Ordem**]: Seja S um conjunto não vazio de inteiros positivos. Então S contém um mínimo elemento; isto é, S contém um elemento a tal que $a \leq s$ para cada s em S

Well-Ordering Principle

- Generally speaking, an ordered set S is said to be well-ordered if every subset of S contains a first element. Thus Teorema [**Princípio da Boa Ordem**]: states that N is well ordered.
- A set S of integers is said to be bounded from below if every element of S is greater than some integer m (which may be negative). (The number m is called a lower bound of S.)
- A simple corollary of the above theorem follows:
- Corollary 11.7: Let S be a nonempty set of integers which is bounded from below. Then S contains a least element.