# discrete math

Bechir Brahem

## 1 Points About Logic

### 1.1 Proposition

**Definition.** A proposition is a statement (communication) that is either true or false.

### 1.2 Predicate

**Definition.** A predicate can be understood as a proposition whose truth depends on the value of one or more variables.

# 2 Induction,WOP and Invariants

## 2.1 Well Ordering Principle

**Theorem.** Every nonempty set of nonnegative integers has a smallest element.

**scheme of the proof.** Principle, you can take the following steps:
More generally, to prove that "P(n) is true $\forall n \in \mathbb{N}$ ." using the Well Ordering

- Define the set, C , of counterexamples to P being true. Namely, define

$$C ::= \{n \in \mathbb{N} | P(n) is false\}$$

- Use a proof by contradiction and assume that C is nonempty.
- By the Well Ordering Principle, there will be a smallest element, n, in C .
- Reach a contradiction (somehow)—often by showing how to use n to find another member of C that is smaller than n. (This is the open-ended part of the proof task.)
- Conclude that C must be empty, that is, no counterexamples exist. QED■

**examples.** it can be used to prove the sum of integers is:$\sum_0^n k = \frac{n(n+1)}{2}$ or to show that every integer is a product of primes.(*Fundamental theorem of arithmetic without uniqueness*)

**proof.** let the predicate P(n):=" $\forall n \in \mathbb{N} | n = p_1 p_2 ... p_k$ " let S=n — P(n) is false n is a positive integer, we assume that S$\neq \emptyset$ by the WOP S has a smallest element $n_0$. if $n_0$ was a prime it would be in S so $n_0$ is not a prime $\Rightarrow$ $n_0$=ab $\Rightarrow$ $0 < a, b < n_0$ so a=$p_1 p_2 ... p_k$ and b= $q_1 q_2 ... q_k$ where $p_i$ and $q_i$ are primes $\Rightarrow$ ab$\in S \Rightarrow n_0 \in S$ absurd. hence we have P(n)

## 2.2 Induction

**scheme of the proof.** let P(n) be the predicate we want to provein S.
If:

$$\begin{cases} P(n_0) \ is \ true \\ P(n) \Rightarrow \ P(n+1) \end{cases}$$

Then:
P(m) is true $\forall m \in S$

## 2.3 Strong Induction

**scheme of the proof.** let P(n) be the predicate we want to prove in S.
If:

$$\begin{cases} P(n_0) \ is \ true \\ \forall n \in S, \ we \ have \ P(0), P(1)...P(n) \Rightarrow P(n+1) \end{cases}$$

Then:
P(m) is true $\forall m \in$ S

**examples.** P(n)::=”*Every integer greater than 1 is a product of primes.*”
2 is a prime so we have P(2).
assuming we have P(0)...P(n),
if n+1 is a prime then P(n+1)
if n+1 is composite then n+1=ab such that $1 < a, b < n$. so we have P(a) and P(b) and so n+1 is a prime. $\Rightarrow P(n+1)$
so $\forall m \in S, P(m)$

## 2.4 Invariants

The idea of the proof by invariant is that for some process there is a proprety X that remains constant for every state.

**example.** say that a robot on a grid can only move diagonally.from the initial position (0,0) the robot can go to (1,1),(-1,1),(1,-1),(-1,-1)
*claim. a robot can never reach (1,0) if (0,0) is its initial position.*
**proof.** the invariant:*if (0,0) is the initial state then whatever position the robot gets into (x,y) x+y is even.*
base case: 0+0 is even.
induction:if the robot is in position (x,y) we assume that x+y is even then the next position (a,b) will be:(x+1,y+1) or (x-1,y-1) or (x-1,y+1) or (x+1,y-1). and so in every case a+b is even.
for any position (x,y) to be reachable x+y must be even.
and so (1,0) is not reachable from (0,0)

**scheme of the proof** In summary, if you would like to prove that some property X holds for every step of a process, then it is often helpful to use the following method:

- Define P(t) to be the predicate that X holds immediately after step t .
- Show that P(0) is true, namely that X holds for the start state.
- show that:

$$\forall t \in \mathbb{N}, P(t) \Rightarrow P(t+1)$$

# 3 Number Theory

## 3.1 Math theory

### 3.1.1 Basics

**Definition.** a divides b (notation a — b) iff there is an integer k such that

$$\text{ak} = \text{b}$$

**Theorem.** Let n and d be integers such that d $\neq$ 0. Then there exists a unique pair of integers q and r, such that:

$$\text{n=dq+r} \text{ , } 0 \leq r \leq |d|$$

**Euclid Algorithm.** for b$\neq$0

$$\text{gcd(a,b)=gcd(b,rem(a,b))}$$

**Bezout Theorem.** The greatest common divisor of a and b is a linear combination of a and b. That is:

$$\text{gcd(a,b)=sa + tb}$$

for some t,s

### 3.1.2 Prime Numbers.

- **Twin Prime Conjecture** There are infinitely many primes p such that p + 2 is also a prime
- **Conjectured Inefficiency of Factoring** Given the product of two large primes n=pq, there is no efficient procedure to recover the primes p and q. That is,no polynomial time procedure. Best solution so far

$$e^{1.9(ln\ \ n)^{\frac{1}{3}}(ln\ \ ln\ \ n)^{\frac{2}{3}}}$$

- **Goldbach's Conjecture** every even integer greater than two is equal to the sum of two primes.

**Prime Distribution.**

$$\pi\text{(n)::=card(\{p, p is prime and 2}\leq\text{p}\leq\text{n \})}$$

**Prime Number Theorem.**

$$\lim_{x\to\infty} \frac{\pi(n)}{n/ln(n)} = 1$$

**Fundamental Theorem of Arithmetic.** Every positive integer is a product of a unique weakly decreasing sequence of primes.

### 3.1.3 Modular Arithmetic

On the first page of his masterpiece on number theory, Disquisitiones Arithmeticae, Gauss introduced the notion of "congruence." Now, Gauss is another guy who managed to cough up a half-decent idea every now and then, so let's take a look at this one. Gauss said that a is congruent to b modulo n iff n — (a-b). This is written

$$a \equiv b(mod\ n)$$

$$a \equiv b(mod\ n) \quad \Leftrightarrow \quad rem(a, n) = rem(b, n) \tag{1}$$

We have $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then:

$$a + c \equiv b + d(mod\ n)$$

$$ab \equiv cd(mod\ n)$$

### 3.1.4 The Ring $\mathbb{Z}_n$

$\mathbb{Z}_n$={r | for a$\in \mathbb{Z}, a \equiv r(mod\ n)$} for example $\mathbb{Z}_n$={0,1,2...n},
we define $r = a \boldsymbol{+_n} b$ :$(a, b) \in \mathbb{Z}_n \rightarrow r \in \mathbb{Z}_n$ such that a+b≡ r (mod n)
for example $5 +_7 4 = 2$
we define $r = a \boldsymbol{\cdot_n} b$ :$(a, b) \in \mathbb{Z}_n \rightarrow r \in \mathbb{Z}_n$ such that a·b≡ r (mod n)
for example $5 \cdot_7 4 = 6$