21-127 Final Theorems & Definitions

Christian Broms

Wednesday 9^{th} May, 2018

1 Theorems

Theorem 1. WEAK INDUCTION PRINCIPLE. Let $p(n)$ be a satement about natural numbers, and let $b \in \mathbb{N}$. If

1. $p(b)$ is true; and

2. For all $n \geq b$, if $p(n)$ is true, then $p(n+1)$ is true;

then $p(n)$ is true for all $n \geq b$.

Theorem 2. STRONG INDUCTION PRINCIPLE. Let $p(x)$ be a satement about natural numbers, and let $b \in \mathbb{N}$. If

1. $p(b)$ is true; and

2. For all $n \geq \mathbb{N}$, if $p(k)$ is true for all $b \leq k \leq n$, then $p(n+1)$ is true;

then $p(n)$ is true for all $n \geq b$.

Theorem 3. BINOMIAL THEOREM. Let $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Theorem 4. WELL ORDERING PRINCIPLE. Let X be a set of natural numbers. If X is inhabited, the X has a least element.

Theorem 5. DEMORGAN'S LAWS FOR LOGICAL OPERATORS. Let p and q be propositions. Then

1. $\neg(p \vee q) \sim (\neg p) \wedge (\neg q)$

2. $\neg(p \wedge q) \sim (\neg p) \vee (\neg q)$

Theorem 6. DEMORGAN'S LAWS FOR QUANTIFIERS. Let $p(x)$ be a logical formula. Then

1. $\neg(\exists x, p(x)) \sim \forall x, (\neg p(x))$

2. $\neg(\forall x, p(x)) \sim \exists x, (\neg p(x))$

Theorem 7. DEMORGAN'S LAWS FOR SETS. Let X, Y, Z be sets. Then

1. $Z \backslash (X \cup Y) = (Z \backslash X) \cap (Z \backslash Y)$

2. $Z \backslash (X \cap Y) = (Z \backslash X) \cup (Z \backslash Y)$

Theorem 8. PASCAL'S IDENTITY. $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k+1}$

Theorem 9. DIVISION THEOREM. Let $a, b \in \mathbb{Z}$, with $b \neq 0$. There exist uniqe $q, r \in \mathbb{Z}$ such that

$$a = qb + r \text{ and } 0 \leq r < |b|$$

Theorem 10. BEZOUT'S LEMMA. Let $a, b, c \in \mathbb{Z}$ and let $d = \gcd(a, b)$. The equation

$$ax + by = c$$

has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ if and only if $d|c$.

Theorem 11. FUNDAMENTAL THEOREM OF ARITHMETIC. Let $a \in \mathbb{Z}$ be a non-zero non-unit. There exist primes $p_1, \ldots, p_k \in \mathbb{Z}$ such that

$$a = p_1 \times \cdots \times p_k$$

Moreover, this expression is essentially unique: if $a = q_1 \times \cdots \times q_\ell$ is another expression of a as a product of primes, then $k = \ell$ and, re-ordering the q_i if neccessary, for each i there is a unit u_i such that $q_i = u_i p_i$

Theorem 12. [MODULAR PROPERTIES]. Let $a, b, c \in \mathbb{Z}$ and let n be a modulus. Then

1. $a \equiv a \mod n$;

2. If $a \equiv b \mod n$, then $b \equiv a \mod n$;

3. If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

Theorem 13. [MODULAR ARITHMATIC]. Fix a modulus n and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that

$$a_1 \equiv b_1 \mod n \text{ and } a_2 \equiv b_2 \mod n$$

The following congruences hold

1. $a_1 + a_2 \equiv b_1 + b_2 \mod n$;

2. $a_1 a_2 \equiv b_1 b_2 \mod n$;

3. $a_1 - a_2 \equiv b_1 - b_2 \mod n$;

Theorem 14. TOTIENT THEOREM. Let $a \in \mathbb{Z}$. The order of a is the least $k \geq 0$ such that $a^k \equiv 1 \mod n$.

Theorem 15. FRESHMAN EXPONENTIATION RULE. Let $a, b \in \mathbb{Z}$ and p a positive prime. Then, $(a+b)^p \equiv a^p + b^p \mod p$.

Theorem 16. FERMAT'S LITTLE THEOREM. Let $a, p \in \mathbb{Z}$ with p a positive prime. Then $a^p \equiv a \mod p$.

Theorem 17. EULER'S THEOREM. Let n be a modulus and let $a \in \mathbb{Z}$ with $a \perp n$. Then

$$a^{\varphi(n)} \equiv 1 \mod n$$

Theorem 18. WILSON'S THEOREM. Let $n > 1$ be a modulus. Then n is prime if and only if $(n-1)! \equiv -1 \mod n$.

Theorem 19. CHINESE REMAINDER THEOREM. Let m, n be moduli and let $a, b \in \mathbb{Z}$. If m and n are coprime, then ther exists an integer solution x to the simulaneous congruences

$$x \equiv a \mod n \text{ and } x \equiv b \mod n$$

Moreover, if $x, y \in \mathbb{Z}$ are two such solutions, then $x \equiv y \mod mn$.

Theorem 20. [FUNCTION GENERALIZATIONS]. Let $m, n \in \mathbb{N}$.

1. If there exists an injection $f : [m] \to [n]$, then $m \leq n$.

2. If there exists a surjection $g : [m] \to [n]$, then $m \geq n$.

3. If there exists a bijection $h : [m] \to [n]$, then $m = n$.

Theorem 21. DEMORGAN'S LAWS FOR FINITE SETS. Let $n \in \mathbb{N}$. For each $i \in [n]$ let X_i be a set, and let Z be a set. Then

1. $Z \backslash (\bigcup_{i=1}^{n} X_i) = \bigcap_{i=1}^{n} (Z \backslash X_i)$

2. $Z \backslash (\bigcap_{i=1}^{n} X_i) = \bigcup_{i=1}^{n} (Z \backslash X_i)$

Theorem 22. MULTIPLICATION PRINCIPLE. Let $\{X_1, \ldots, X_n\}$ be a family of finite sets, with $n \geq 1$. Then $\Pi_{i=1}^{n}$ is finite and

$$|\Pi_{i=1}^{n} X_i| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|$$

Theorem 23. INCLUSION-EXCLUSION PRINCIPLE. Let $n \geq 2$ and let $X_1, X_2, \ldots, X_n$ be sets. Then

$$|\bigcup_{i=1}^{n} X_i| = \sum_{j \subseteq [n]} (-1)^{|J|+1} |\bigcap_{j \in J} X_j|$$

where for the purposes of the formula we take $\bigcap_{j \in \emptyset} X_j = \emptyset$

Theorem 24. DEMORGAN'S LAWS FOR SETS. Let Z be a set and let $\{X_i | i \in I\}$ be an indexed family of sets. Then

1. $Z \backslash \bigcup_{i \in I} X_i = \bigcap_{i \in I} (Z \backslash X_i)$

2. $Z \backslash \bigcap_{i \in I} X_i = \bigcup_{i \in I} (Z \backslash X_i)$

Theorem 25. TRIANGLE INEQUALITY. Let $x, y \in \mathbb{R}$. Then $|x + y| \leq |x| + |y|$. Moreover, $|x + y| = |x| + |y|$ if and only if x and y have the same sign.

Theorem 26. TRIANGLE INEQUALITY (VECTORS). Let $\vec{x}, \vec{y} \in \mathbb{R}^2$. Then

$$||\vec{x} + \vec{y}|| \leq ||\vec{x}|| + ||\vec{y}||$$

with equality if and only if $a\vec{x} = b\vec{y}$ for some real numbers $a, b \geq 0$.

Theorem 27. CAUCHY-SCHWARZ INEQUALITY. Let $n \in N$ and let $x_i, y_i \in \mathbb{R}$ for each $i \in [n]$. Then

$$|\vec{x} \cdot \vec{y}| \leq ||\vec{x}|| \cdot ||\vec{y}||$$

with equality if and only if $a\vec{x} = b\vec{y}$ for some $a, b \in \mathbb{R}$ which are not both zero.

Theorem 28. SQUEEZE THEOREM. Let $(x_n), (y_n)$ and (z_n) be sequence of real numbers such that

1. $(x_n) \to a$ and $(z_n) \to a$; and
2. $x_n \leq y_n \leq z_n$ for all $n \in \mathbb{N}$.

Then $(y_n) \to a$.

Theorem 29. MONOTONE CONVERGENCE THEOREM. Let (x_n) be a sequence of real numbers.

1. If (x_n) is increasing and has an upper bound, then it converges
2. If (x_n) is decreasing and has a lower bound, then it converges

Theorem 30. BAYES' THEOREM. Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events with positive probabilities. Then

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A|B)\mathbb{P}(B)}{\mathbb{P}(A)}$$