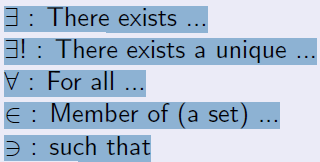
R: the set of all real numbers

Z: the set of all integers

Q: the set of all rational numbers



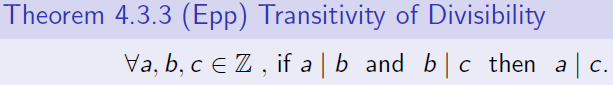


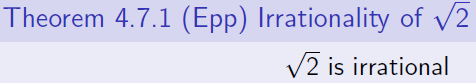
Theorem 4.3.1 (Epp)



That is, when dealing with positive integers, a divisor of a number cannot be larger than the number.

Note that the theorem is silent for the case b = 0, because 0 is not positive.





A **tautology** is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement**. A **contradiction** is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables.

(p -> q) : p is the hypothesis ( or antecedent) and q is the conclusion ( or consequent).

**Theorem 2.1.1 Logical Equivalences**

Given any statement variables *p, q*, and *r* , a tautology **t** and a contradiction **c**, the following logical equivalences

hold.

1. *Commutative laws: p* ∧ *q* ≡ *q* ∧*p p*∨ *q* ≡ *q* ∨ *p*

2. *Associative laws: (p* ∧ *q)* ∧ *r* ≡ *p* ∧ *(q* ∧ *r) (p* ∨ *q)* ∨ *r* ≡ *p* ∨ *(q* ∨ *r )*

3. *Distributive laws: p* ∧ *(q* ∨ *r )* ≡ *(p* ∧ *q)* ∨ *(p* ∧ *r ) p* ∨ *(q* ∧ *r )* ≡ *(p* ∨ *q)* ∧ *(p* ∨ *r )*

4. *Identity laws: p* ∧ **t** ≡*p p*∨ **c** ≡ *p*

5. *Negation laws: p* ∨ ∼*p* ≡ **t** *p* ∧ ∼*p* ≡ **c**

6. *Double negative law:* ∼*(*∼*p)* ≡ *p*

7. *Idempotent laws: p* ∧ *p* ≡*p p*∨ *p* ≡ *p*

8. *Universal bound laws: p* ∨ **t** ≡ **t** *p* ∧ **c** ≡ **c**

9. *De Morgan’s laws:* ∼*(p* ∧ *q)* ≡ ∼*p* ∨ ∼*q* ∼*(p* ∨ *q)* ≡ ∼*p* ∧ ∼*q*

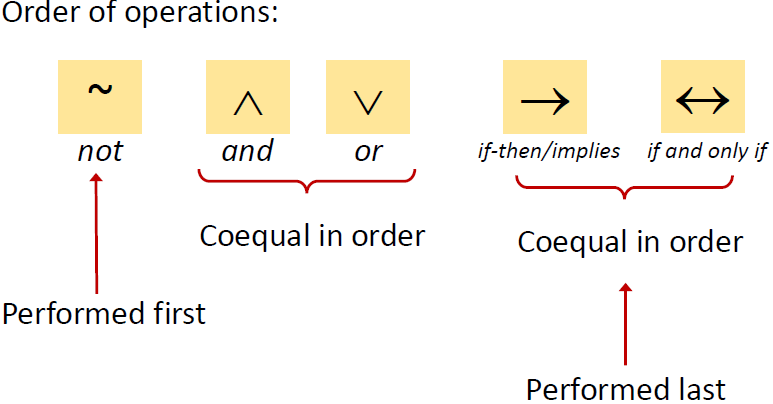
10. *Absorption laws: p* ∨ *(p* ∧ *q)* ≡*p p*∧ *(p* ∨ *q)* ≡ *p*

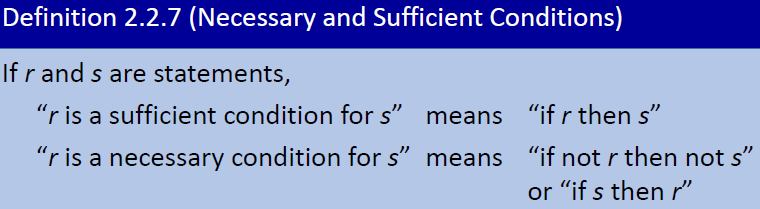
11. *Negations of* **t** *and* **c***:* ∼**t** ≡ **c** ∼**c** ≡ **t**

A conditional statement that is true by virtue of the fact that its hypothesis is false is often called **vacuously true or true by default.**

The converse of *p*->*q* is *q*->*p*. **===** The inverse of *p*->*q* is ~*p*->~*q*.

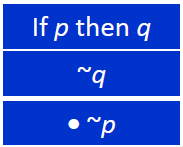






*r* is a necessary and sufficient condition for *s* means “*r*, if and only if, *s*”.

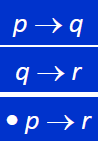
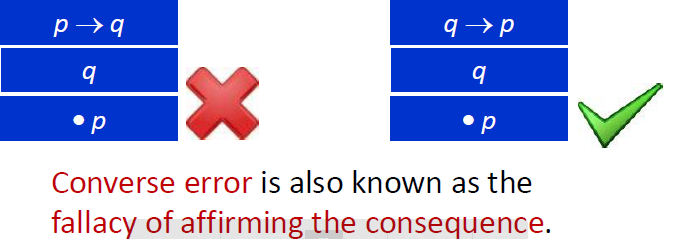
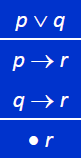
**Modus Tollen’s** **Generalisation**



**Specialisation**  **Elimination**



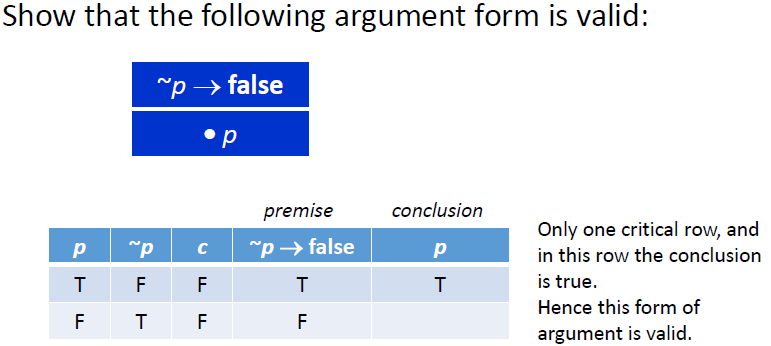
**Transitivity Proof by Division into Cases**

**Inverse Error:**



An argument is called **sound** if, and only if, it is valid and all its premises are true. An argument that is not sound is called **unsound**.



*Q*(*n*) be “*n* is a factor of 8”, *R*(*n*) be “*n* is a factor of 4”, *S*(*n*) be “*n*< 5 and *n*3”, then their truth sets are

{1,2,4,8}, {1,2,4}, and {1,2,4} respectively.

***R*(*n*) => *Q*(*n*)**

**R(n) <=> S(n)**

primes *p*, *p* is odd: ⱻ a prime *p* such that *p* is not odd.

ⱻ a triangle *T* such that the sum of the angles of *T* equals 200: triangles *T*, the sum of the angles of *T* does not equal 200.

**Informal Negation:**

If a computer program has more than 100,000 lines, then it contains a bug:

There is at least one computer program that has more than 100,000 lines and does not contain a bug.

**In general, a statement of the form *x* in *D*, if *P*(*x*) then *Q*(*x*) is called vacuously true or true by default if, and only if, *P*(*x*) is false for every *x* in *D*.**

**Ambiguous Language**

You are visiting a computer microchips factory. The factory guide tells you:

There is a person supervising every detail of the production process.

“there is” –existential quantifier; “every” –universal quantifier.

Which of the following best describes its meaning?

There is one single person who supervises all the details of the production process.

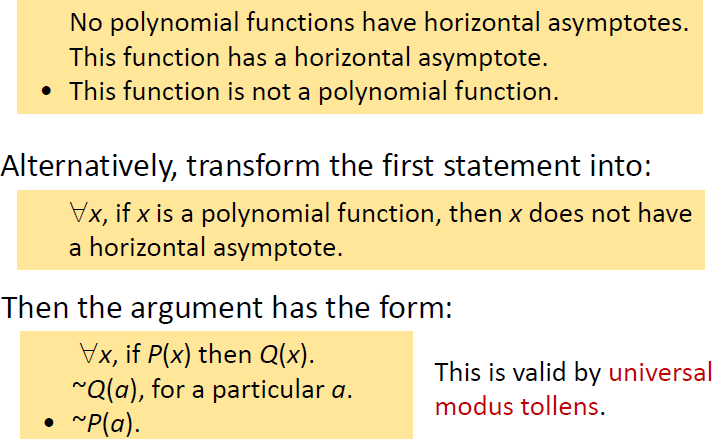
For any particular production detail, there is a person who supervises the detail, but there might be different supervisors for different details.

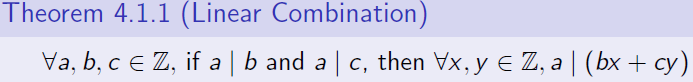
For all squares *x*, there is a circle *y* such that *x* and *y* have the same color:

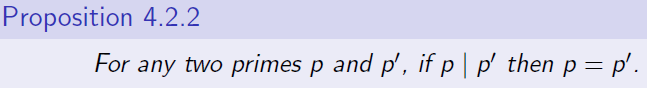
a square *x* such that circles *y*, *x* and *y* do not have the same color.

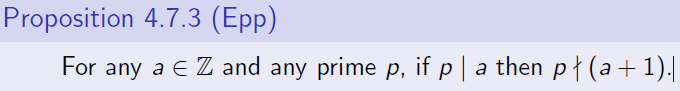
The rule of universal instantiation:

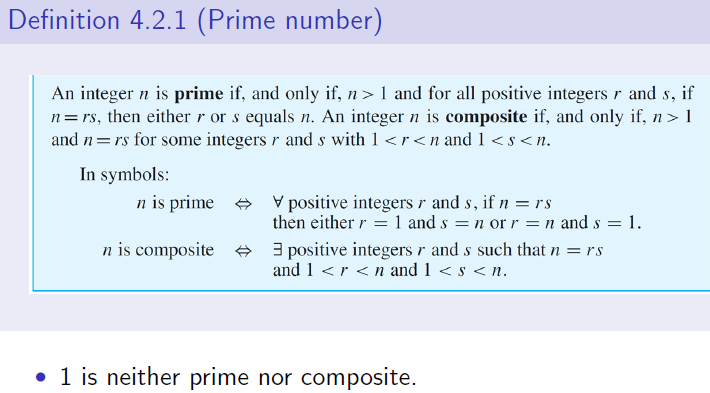
If some property is true of *everything* in the set, then it is true of *any particular* thing in the set.

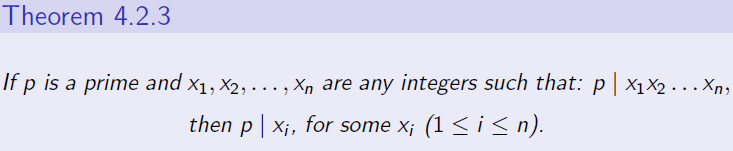


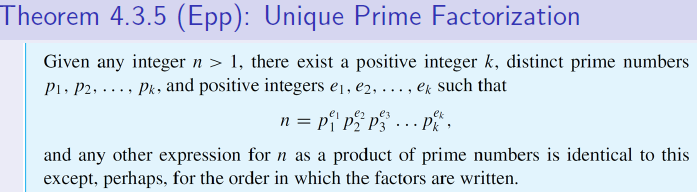


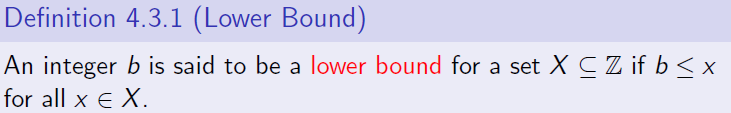








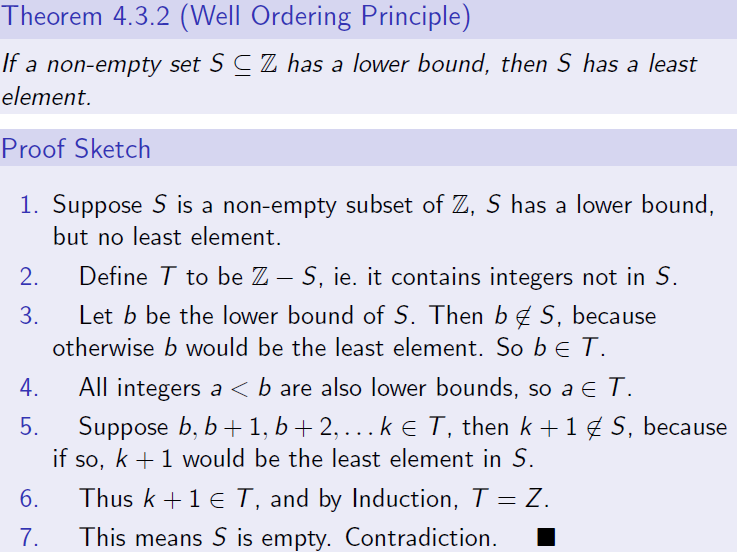


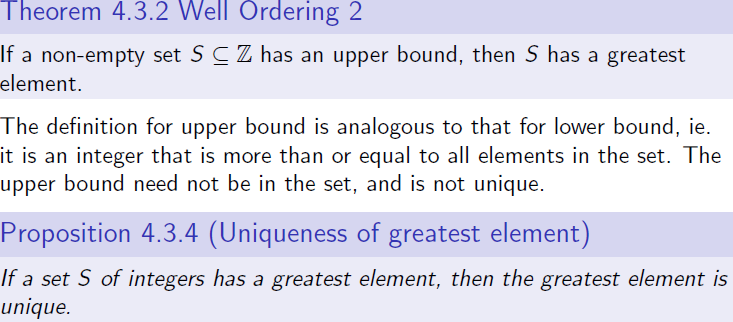


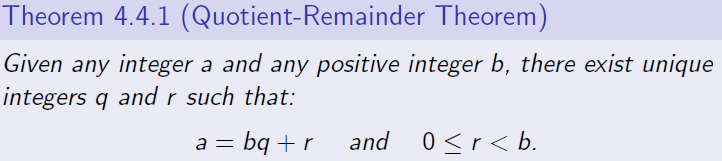
**Note that this definition does not require b to be a member of X. Moreover, there may be more than one lower bound (i.e. the lower bound is not unique).**

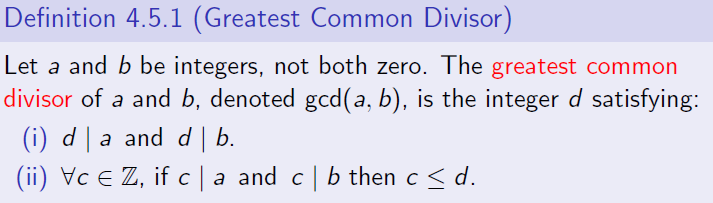
Proposition 4.3.3 (Uniqueness of least element)

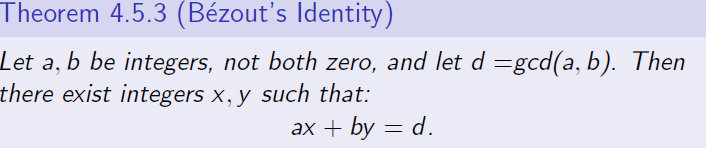
If a set S of integers has a least element, then the least element is unique.





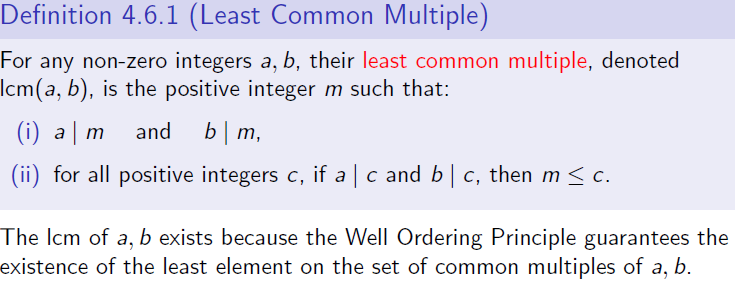


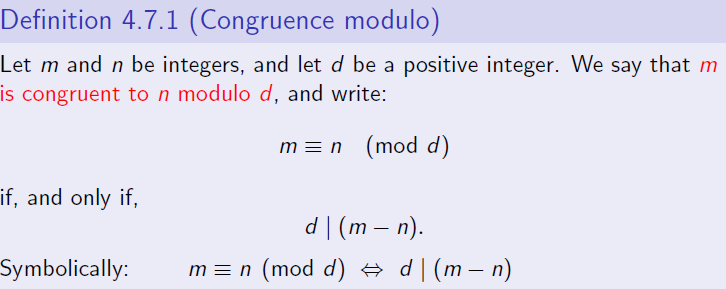


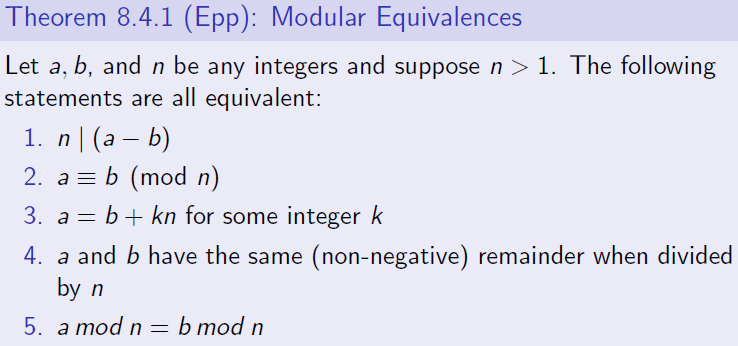


Once a solution pair (x; y) is found, additional pairs may be generated by (x + kb/d, y - ka/d), where k is any integer.

Integers a and b are relatively prime (or coprime) if gcd(a, b) = 1.







For any integers a; n with n > 1, if an integer s is such that as = 1 (mod n), then s is called the multiplicative inverse of a modulo n. The commutative law still applies in modulo arithmetic.

Theorem 4.7.3 (Existence of multiplicative inverse)

For any integer a, its multiplicative inverse modulo n (where n > 1), the inverse, exists if, and only if, a and n are coprime. Recall that two numbers are coprime, or relatively prime, i\_ their gcd is 1.

Corollary 4.7.4 (Special case: n is prime)

If n = p is a prime number, then all integers a in the range 0 < a < p have multiplicative inverses modulo p.

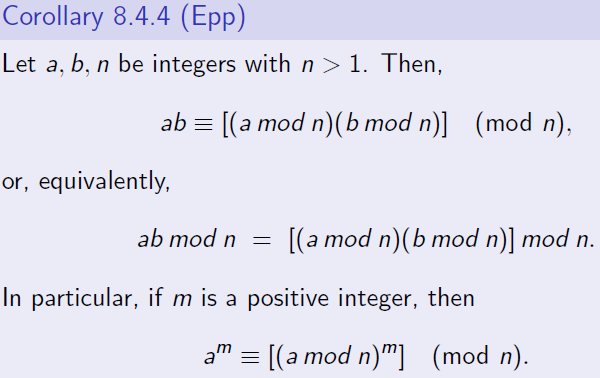
**Theorem 4.3.2 Divisors of 1**

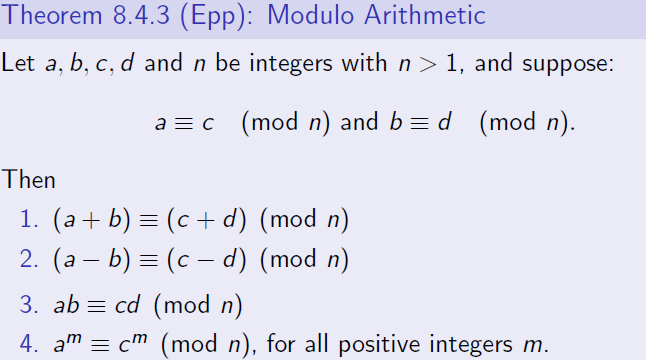
The only divisors of 1 are 1 and −1.

Theorem 8.4.9 (Epp)

For all integers a; b; c; n, with n > 1 and a and n are coprime,

if ab \_ ac (mod n), then b \_ c (mod n).





**Theorem 4.2.1**

Every integer is a rational number.

Theorem 4.2.2

The sum of any two rational numbers is rational.

Theorem 4.3.4 Divisibility by a Prime

Any integer n > 1 is divisible by a prime number.

Theorem 4.4.2 The Parity Property

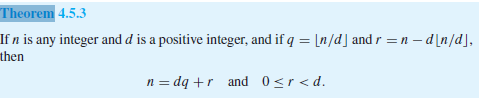
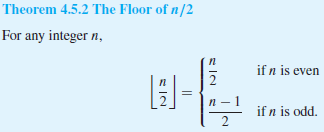
Any two consecutive integers have opposite parity.

Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, |x + y| ≤ |x| + |y|.

**Theorem 4.5.1**

For all real numbers *x* and all integers *m,* \_*x* + *m*\_ = \_*x*\_ + *m*.



**Theorem 4.6.3**

The sum of any rational number and any irrational number is irrational.

Proposition 4.6.4

For all integers n, if n2 is even then n is even.