MATH 135

ALGEBRA

PROFESSOR J.P. PRETTI • FALL 2014 • UNIVERSITY OF WATERLOO

Last Revision: December 2, 2014

Table of Contents

Future Modifications

1 Introduction to Proofs

1.1 Proofs

Definition 1.1 (proof)**.** A **proof** is a convincing argument leaving no doubt that a sentence is true.

Definition 1.2 (statement)**.** A **statement** is a sentence that is either true or false. It must have a truth value and cannot be both true and false. Compound statements can be formed using logical connectives.

Definition 1.3. A **proposition** is a true statement, proved with a valid argument.

Definition 1.4. A **theorem** is a significant proposition

Definition 1.5. A **lemma** is a helper proposition used in the proof of a theorem.

Definition 1.6. A **corollary** is a proposition that follows almost immediately from a theorem.

Definition 1.7. An **axiom** is a statement that is assumed to be true, no proof is needed.

Definition 1.8 (open sentence)**.** An **open sentence** is a sentence with variables, and its truth value can be either true or false.Its truth value is meaningless until its variables are replaced with specific numbers.

Example 1.1. $z^2 = 49$ is an open sentence. There is no way to determine whether the statement is true or false without determining a value for z.

Note. Never assume first statement is true. If you do, $1 = 2$ can prove $2 = 3$.

Example 1.2. Another bad proof. Let $a, b \in \mathbb{Z}$ and prove

$$(a - b) = (b - a)$$

Proof.

$$(a-b)^2 = (b-a)^2$$
$$(a-b)^2 = [-(a-b)]^2$$
$$(a-b)^2 = (-1)^2(a-b)^2$$
$$(a-b)^2 = (a-b)^2$$

□

Definition 1.9. A **compound statement** is a statement composed of several individual **component statements**. AND , OR and NOT $(\wedge \vee \neg)$ are three important logical operators (connectors) used to form compound statements.

Definition 1.10. A **truth table** for a logical operator defines the truth value of a compound statement using this operator.

A	B	$A \implies B$	$(\neg A) \vee B$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Definition 1.11. Two compound statements are **logically equivalent** if they have the same truth values for all possible states of their component statement. Equivalence is shown as $S_1 \equiv S_2$.

Definition 1.12. De Morgan's Laws (DML) state that for any two statements A and B

$$\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$$

$$\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$$

1.2 Implication

Definition 1.13. An **implication** is a statement of the form 'If H then C' where H and C are statements. A direct proof of an implication is assuming H is true and showing C must also be true. To use it, show H is true and conclude immediately that C is true.
Written in the form $H \implies C$.

Example 1.3. Prove the implication: If $x \in \mathbb{R}$, then $x^2 + 5x + 7 \geq 0$

Proof.

$$x^2 + 5x + 7 - \frac{25}{4} + \frac{25}{4}$$

$$x^2 + 5x + 7 - \frac{25}{4}$$

$$(x + \frac{5}{2})^2 + \frac{3}{4}$$

Since $(x + \frac{5}{2})^2 \geq 0$, adding $\frac{3}{4}$ to it will result in an answer greater than 0. □

Example 1.4. Prove the statement: If m is an even integer, then $7m^2 + 4$ is an even integer.

Proof. Suppose $m \in \mathbb{Z}$ is even, then m^2 is even. Also, $7m^2$ is even. Finally, $7m^2 + 4$ is even as required. □

1.3 Divisibility

Definition 1.14. An integer m divides an integer n if there exists an integer k so that $n = km$. $3 \mid 6$ while $3 \nmid 7$.

Example 1.5. If n is an integer and $14|n$, then $7 \mid n$

Proof. Suppose n is an integer and $14 \mid n$

$$14 \mid n \implies n = 14k, k \in \mathbb{Z}$$

$$n = 7(2k)$$

$$k \in \mathbb{Z} \implies 2k \in \mathbb{Z}$$

$$\therefore 7 \mid n$$

□

Theorem 1.1 (TD)**. Transitivity of Divisibility** states if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. $b = ax$ and $c = by$, then $a(xy) = c$. Since $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ then $xy \in \mathbb{Z}$. Therefore $a \mid c$. □

Theorem 1.2 (BBD)**. Bounds by Divisibility** states that if $a, b \in \mathbb{Z}$, if $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.

Theorem 1.3 (DIC)**. Divisibility of Integer Combinations** states if a, b and c are integers where $a \mid b$, and $a \mid c$, and x and y are any integers, then $a \mid (bx + cy)$.

Example 1.6. If $m \in \mathbb{Z}$ and $14 \mid m$ then $7 \mid 135m + 693$

Proof. Assume $(m \in \mathbb{Z}) \wedge (14 \mid m)$. Since $14 \mid m$ then $7 \mid m$. Also $7 \mid 693$ because $693 = 99(7)$. Therefore, using DIC, $7 \mid (135m + 1(693))$ □

1.4 Converse and Contrapositive

Definition 1.15. The **contrapositive** of the implication $H \implies C$ is $\neg C \implies \neg H$ The statement is flipped and reversed. A very powerful tool for proving implications where direct proof is too convoluted. The truth table for a contrapositive and the original statement is the same.

Example 1.7. Prove that $7 \nmid n \implies 14 \nmid n$

Proof. Use the contrapositive: $14 \mid n \implies 7 \mid n$. This was already proved. □

Definition 1.16. The **converse** of the implication $H \implies C$ is $C \implies H$. The statement is reversed. The converse may not be logically equivalent to the original statement.

Theorem 1.4. Furthermore, an implication is logically equivalent to other statements.

$$\neg(A \implies B) \equiv (A \wedge (\neg B))$$

$$(A \implies B) \equiv ((\neg A) \wedge B)$$

Example 1.8. $P(n)$: If n is an integer and $4n^3 - 2n - 1$ is odd then n is odd.

Note. To prove $P(n)$ is false, simply prove $\neg P(n)$

Proof. Only one example needs to be false for the entire statement to be false. Try $n = 2$, then $4(2)^3 - 2(2) - 1 = 27$. $P(2)$ is false, therefore $P(n)$ is false. □

1.5 If and Only If

Definition 1.17. The definition of A **if and only if** B is $(A \iff B) \equiv (A \implies B) \wedge (B \implies A)$.

Example 1.9. Consider the following $x^2 - x > 0 \iff x \in [0, 1]$

Proof.
($\Longrightarrow$) Assume $x^2 - x > 0$ then $x(x-1) > 0$

$$(x > 0 \wedge x > 1) \vee (x < 0 \wedge x < 1)$$
$$(x > 1) \vee (x < 0)$$

($\Longleftarrow$) Assume:$(x > 1) \vee (x < 0)$

$$(x > 0 \wedge x > 1) \vee (x < 0 \wedge x < 1)$$
$$x(x-1) > 0$$
$$x^2 - x > 0$$

□

Note. The two parts of the proof may not always be the reverse of each other. When they are the reverse, we can write a shorter "Chain of iffs"

Proof. Let $x \in \mathbb{R}$. Then $x^2 - x > 0$

$$\begin{aligned} &\Longleftrightarrow\ x(x-1) > 0 \\ &\Longleftrightarrow\ (x > 0 \wedge x > 1) \vee (x < 0 \wedge x < 1) \\ &\Longleftrightarrow\ (x > 1) \vee (x < 0) \\ &\Longleftrightarrow\ x \in [0, 1] \end{aligned}$$

□

2 Sets and Quantifiers

2.1 Sets

Definition 2.1. A **set** is a collection of objects. The objects that make up a set are called elements or members. Elements can be anything: numbers, letters, functions, happy faces, or even other sets.

Note. In Mathematics, the set of natural numbers, $\mathbb{N}$ consists of only positive integers. In Computer Science, 0 is included in that set.

Definition 2.2. The set $\{\}$ contains no elements and is known as the **empty set**. We usually use $\emptyset$ as a symbol for the empty set. $\emptyset = \{\}$

Definition 2.3. The number of elements in a finite set is called the **cardinality** of the set. $|S|$ is used to denote a set's cardinality. The cardinality of the empty set is defined to be 0.

Definition 2.4. Whe working with very large sets, we refer to them as the **universe of discourse**. For example $x \in \mathbb{Z}$ means that the set of integers is the $\mathcal{U}$

Example 2.1. This is the **set-builder notation**.

$$S = \{x : P(x)\}$$

where $P(x)$ is a defining property of the elements x in S.

Example 2.2. Sometimes the universe of discourse is known, and a set can be written as

$$S = \{x \in \mathcal{U} : P(x)\}$$

A set of all even integers can be described as: $n \in \mathbb{Z} : 2 \mid n$.

Definition 2.5. The **union** of two sets S and T, written $S \cap T$ is a set that includes all items from either sets.

Definition 2.6. The **intersection** of two sets S and T, written $S \cup T$ is a set that includes only items that are present in both sets. $\{x : (x \in S) \wedge (x \in T)\}$

Definition 2.7. The **set-difference** of two sets S and T is the set of all elements in S that are not in T. Written as $S - T$ or $S \setminus T$.

Definition 2.8. The **complement** of a subset $S \subseteq \mathcal{U}$, written $\overline{S}$ consists of elements in $\mathcal{U}$ but not in S.

Definition 2.9. The **Cartesian product** of two sets S and T is the set

$$S \times T = \{(x, y) : x \in S, y \in T\}$$

Each element in S is paired up with each and every element in T.

$$|S \times T| = |S| \cdot |T|$$

Definition 2.10. S and T are said to be **disjoint sets** when $S \cap T = \emptyset$

Definition 2.11. A set S is called a **subset** of a set T, and is written $S \subseteq T$, when every element of S is also in T The subset of this set $\{a, b, c\}$ includes $\{a\}\{b\}\{c\}\{a, b\}\{b, c\}\{a, c\}\{a, b, c\}\{\}$

$$(S \subseteq T) = (x \in S \implies x \in T)$$

The empty set is a subset of any set $\emptyset \subseteq S$.

Definition 2.12. S is a **proper subset** and we write $S \subsetneq T$ when $S \subseteq T$ but $S \neq T$.

Definition 2.13. S is a **proper superset** and we write $S \supsetneq T$ when $S \supseteq T$ but $S \neq T$.

Method 2.1. To prove $S \subseteq T$, just prove $x \in S \implies x \in T$ through a direct proof.

To prove $S = T$, prove $x \in S \iff x \in T$

Example 2.3. Prove the following statement $S \neq T \iff S \cap T \neq S \cup T$

Proof. Use the contrapositive. Since it's an iff statement, hypothesis and conclusion don't necessary need to be switched because they are going to be proved both wasy. Prove $S = T \iff S \cap T = S \cup T$ Assume $S = T$, then $S \cap T = S \cup S = S = S \cup S = S \cup T$

Other direction must be proved as well. Assume $S \cap T = S \cup T$ Let $x \in S$. (Goal: $x \in T$).

$$\begin{aligned} &\implies (x \in S) \vee (x \in T) \\ &\implies x \in S \cup T \\ &\implies x \in S \cap T \\ &\implies (x \in S) \wedge (x \in T) \\ &\implies x \in T \end{aligned}$$

This proves $S \subseteq T$ To show $T \subseteq S$, a symmetrical argument can be used. □

2.2 Quantifiers

2.2.1 Universal Quantifier

Example 2.4. For every is shown by the symbol $\forall$ and **there exists** is shown by the symbol $\exists$.

Example 2.5. A statement with a quantifier can be written as

$$\forall x \in S, P(x)$$

Quantifier: $\forall$ Variable: x Domain: S Open sentence: $P(x)$

Example 2.6. Prove $\forall n \in \mathbb{N}, 2n^2 + 11n + 15$ is not prime.

Proof.

Let $m \in \mathbb{N}$. Then $2m^2 + 11m + 15 = (2m + 3)(m + 5)$
Since $m \geq 1$, then $2m + 5 \neq 1$ and $m + 3 \neq 1$
$\therefore 2m^2 + 11m + 15$ is composite (not prime).

□

Method 2.2. We just used the **select method**:
Prove $\forall x \in S, P(x)$ by picking a representative $s \in S$, and showing $P(s)$ is true.

Definition 2.14. When the domain is empty, the regardless of what the open sentence $P(x)$ is, the statement $\forall x \in \emptyset, P(x)$ is **vacuously true**. However $\exists x \in \emptyset, P(x)$ is always false.

Method 2.3. The **substitution method** substitutes an appropriate value of x from S and shows that $P(x)$ must be true to arrive at the desired conclusion.

Example 2.7. Let $a, b, c \in \mathbb{Z}$ Prove that if $\forall x \in \mathbb{Z}, a \mid (bxc)$, then $a \mid (b + c)$

Proof. Assume $\forall x \in \mathbb{Z}, a \mid (bx + c)$. Substitute $x = 1$ to get $a \mid (b + c)$ □

2.2.2 Existential Quantifier

Method 2.4. Construct Method begins with constructing an element s, showing $s \in S$ and then showing $P(s)$ is true.

Example 2.8. There exists an integer m such that $\frac{m-7}{2m+4} = 5$

$$\exists\, m \in \mathbb{Z}, \frac{m-7}{2m+4} = 5$$

Proof. Construct $m' = -3$. Clearly $-3 \in \mathbb{Z}$. Now substituting, we get $\frac{-3-7}{-6+4} = 5$ □

Method 2.5. The **object method** is where we name $s \in S$ such that $P(s)$ is true.

Example 2.9. $\forall n \in \mathbb{Z}$, if $14 \mid n$, then $7 \mid n$

Proof. Suppose $n \in \mathbb{Z}$ and $14 \mid n$. Then $n = 14k, k \in \mathbb{Z}$. $n = 7(2k)$. Since $k \in \mathbb{Z}$, $2k \in \mathbb{Z}$ so $7 \mid n$. □

Note. When introducing a new variable, define it and state the set that it comes from.

Definition 2.15. To negate a quantifier, change $\forall$ to $\exists$ and vice versa. Next, negate $P(x)$

$$\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$$

$$\neg(\exists x \in S, P(x)) \equiv \forall x \in S, \neg P(x)$$

Example 2.10. To negate a statement like this:

$$\neg(\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1)$$

$$\forall x \in \mathbb{R}, \neg(\forall y \in \mathbb{R}, x^3 - y^3 = 1)$$

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 \neq 1$$

2.3 Nesting Quantifiers

Example 2.11. Determine a truth value for each of the following statements

$$\forall x \in \mathbb{R}, \forall\, y \in \mathbb{R}, x^3 - y^3 = 1$$

$$\exists x \in \mathbb{R}, \exists\, y \in \mathbb{R}, x^3 - y^3 = 1$$

$$\forall x \in \mathbb{R}, \exists\, y \in \mathbb{R}, x^3 - y^3 = 1$$

$$\exists x \in \mathbb{R}, \forall\, y \in \mathbb{R}, x^3 - y^3 = 1$$

Ans: F T T F

Proof for 3. Let $x \in \mathbb{R}$. Construct $y = \sqrt[3]{x^3 - 1}$. Clearly $y \in \mathbb{R}$.
Now $x^3 - (\sqrt[3]{x^3 - 1})^3 = x^3 - x^3 + 1 = 1$ □

Disproof for 4. Negate the statement.

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 \neq 1$$

Let $x \in \mathbb{R}$, construct $y = x$, clearly $y \in \mathbb{R}$. Moreover, $x^3 - x^3 = 0 \neq 1$
The negation was proved to be true so the statement is false. □

Method 2.6. Proof by contradiction starts by assuming the statement is false, and prove that the assumption is false, therefore the statement is true. Two classics are proving $\sqrt{2}$ is irrational and proving that there is an infinite amount of prime numbers.

Example 2.12. Prove that there is no largest integer.

Proof. Assume there is a largest integer, n. Consider $n+1$. It is clearly an integer and $n+1 > n$. This is impossible by definition of n. This means that the original assumption is false and therefore there is no largest integer. □

Exercise 2.1. Prove $\sqrt{3}$ is irrational.

Definition 2.16. To distribute the universal quantifier,

$$[\forall x \in S, (P(x) \wedge Q(x)] \equiv [(\forall x \in S, P(x)) \wedge (\forall x \in S, Q(x))]$$

Definition 2.17. To distribute the existential quantifier,

$$[\exists x \in S, (P(x) \wedge Q(x)] \equiv [(\exists x \in S, P(x)) \vee (\exists x \in S, Q(x))]$$

2.4 Uniqueness

To prove uniqueness, either assume there are two objects X and Y that such that $P(X)$ and $P(Y)$. Show that $X = Y$, or assume X and Y are distinct, and derive a contradiction.

Theorem 2.1. If a and b are integers, and $b > 0$, then there exists unique integers q and r such that $a = qb + r$ where $0 \leq r \leq b$.

Proof. Suppose that $a = q_1 b + r_1$ with $0 \leq r_1 \leq b$. Also suppose $a = q_2 b + r_2$ with $0 \leq r_2 \leq b$. Without loss of generality, assume $r_1 < r_2$. Then $0 \leq r_2 - r_1 < b$ and $(q_1 - q_2)b = r_2 - r_1$. Hence $b \mid (r_2 - r_1$. By BBD, $b \leq r_2 - r_1$, which contradicts $r_2 - r_1 < b$. Therefore the assumption that $r_1 \neq r_2$ is false and $r_1 = r_2$. But then $(q_1 - q_2)b = r_2 - r_1$ implies $q_1 = q_2$. □

3 Induction

Example 3.1.

$$\text{Prove } P(n): \sum_{i=1}^{n} j(j+1) = \frac{1}{3}n(n+1)(n+2) \text{ for all } n \in \mathbb{N}$$

Proof. Consider $P(1)$, substitute and $P(1)$ is true, LHS = RHS.
Inductive Hypothesis:
Assume P(k) is true:

$$P(k): \sum_{j=1}^{k} j(j+1) = \frac{1}{3}k(k+1)(k+2)$$

Inductive conclusion:
Prove $P(k+1)$ is also true.

$$\text{LHS: } \sum_{j=1}^{k+1} j(j+1) = [\sum_{j=1}^{k+1} j(j+1)] + (k+1)(k+2) \text{ by IH}$$

$$= (k+1)(k+2) + (\frac{1}{3}k+1)$$

$$= \frac{1}{3}(k+1)(k+2)(k+3)$$

$$\text{RHS: } = \frac{1}{3}(k+1)(k+2)(k+3)$$

LHS = RHS. Therefore by the principle of mathematical induction (POMI), $P(n)$ is true for all natural numbers n. □

Method 3.1. Principle of mathematical induction (POMI) :
Suppose $P(n)$ is a statement on n. If $P(1)$ is true, and $\forall k \in \mathbb{N}, P(k) \implies P(k+1)$. Then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 3.2.

$$P(n): n! > 2^n \text{ for all } n \in \mathbb{N}, n \geq 4$$

Proof. Base case (BC): Consider $P(4)$, LHS: $4! = 24$ and RHS: $2^4 = 16$.
Since LHS $>$ RHS, $P(4)$ is true.
IH: Assume P(k) is true for some $k \in \mathbb{N}$ with $k \geq 4$.
IC: Consider $P(k+1)$, LHS$= (k+1)! = k!(k+1)$.
$> (4+1)2^k$ by IH.
$> (5)2^k$ since $k \geq 4$
RHS: 2^{k+1}.

$$5 \times 2^k > 2 \times 2^k$$

By POMI, $P(n)$ is true for all $n \in \mathbb{N}, n \geq 4$ □

Exercise 3.1.

$$P(n) : 6 \mid (2n^3 + 3n^2 + n)$$

Prove $P(n)$ is true by induction.

Proof. BC: $P(1)$. Since $6 \mid 6$, $P(1)$ is true.
IH: Assume $P(k)$ is true for some $k \in N$, with $k \geq 1$.
IC: Consider $P(k+1)$. $6 \mid (2(n+1)^3 + 3(n+1)^2 + (n+1)$.

$$6 \mid (2n^3 + 9n^2 + 13n + 6)$$

$$6 \mid (2n^3 + 3n^2 + n + 6(n^2 + 2n + 1))$$

Since $6 \mid 6$, by DIC, $6 \mid (2n^3 + 3n^2 + n + 6(n^2 + 2n + 1))$.
By POMI, $P(n)$ is true for all $n \in \mathbb{N}$ □

Example 3.3. POMI does not work with this example. POSI must be used.
Define a sequence $\{x_m\}$ by $x_1 = 4, x_2 = 68$ and $x_m = 2x_{m-1} + 15x_{m-2}$ for all $m \geq 3$

$$P(n) : 2(-3)^n + 10(5)^{n-1}$$

Proof. Consider when $n = 1$. LHS: $x_1 = 4$. RHS: $2(-3)^1 + (10)(5^0) = 4$. $P(1)$ is true. $P(2)$ is also true after repeating the previous step.
IH: Assume $P(1), P(2), \ldots, P(k-1), P(k)$.
IC: $2(-3)^{n+1} + 10(5)^n$

$$\begin{aligned} x_{k+1} &= 2x_k + 15x_{k-1} \qquad \text{With just POMI, cannot continue further} \\ &= 2[2(-3)^n + 10(5)^{n-1}] + 15[2(-3)^{n-1} + 10(5)^{n-2}] \\ &= (-3)^{n-1}(2 \times 2 \times -3 + 2 \times 15) + 5^{n-2}(2 \times 10 \times 5 + 15 \times 10) \\ &= 18(-3)^{n-1} + 250(5)^{n-2} \\ &= 2(-3)^{n+1} + 10(5)^n \end{aligned}$$

The result is true for $n = k + 1$, and so holds for all $n \in \mathbb{N}$ by POSI. □

Method 3.2. Principle of Strong Induction (POSI) :
Let (n) be a statement that depends on $n \in \mathbb{N}$. If

1. $P(1), P(2), \ldots, P(b)$ are true for some positive integer b, and
2. $P(1), P(2), \ldots, P(k)$ are all true implies $P(k+1)$ is true for all $k \in \mathbb{N}$

then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 3.4. $P(n) : n$ has a prime factor. Prove that $P(n)$ is true for all $n \in \mathbb{N}, n \geq 2$.

Proof. BC: $P(2)$ is true because $2 \mid 2$ and 2 is prime.
IH: Assume r has a prime factor for all r with $2 \leq r \leq k$ and some $k > 2$.
IC: Consider $n = k + 1$.
Case 1: n is prime, then n is a prime factor of itself.
Case 2: n is composite, then $n = st$ for some $s, t \in \mathbb{N}$ with $1 \leq s, t \leq n$
Since $2 \leq s \leq k$, by IH, some prime divides s. $s \mid n$ by definition of divisibility, thus the prime factor also divides n by TD.
In either case, n has a prime factor, therefore by POSI, $P(n)$ is true for all $n \geq 2$ □

Example 3.5. The Fibonacci sequence is defined as following:

$$f_1 = 1, f_2 = 1 \qquad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 3$$

Prove $f_k < (\frac{7}{4})^k$.

Proof. BC: $f_1 = f_2 = 1 < (\frac{7}{4})^1 < (\frac{7}{4})^2$ so $P(1)$ and $P(2)$ are true.
IH: Assume $P(r)$ is true for all r where $1 \leq r \leq k$ and some $k \in \mathbb{N}, k \geq 2$
IC:

$$f_{k+1} < (\frac{7}{4})^{k-1}(\frac{11}{4}) \qquad \text{by IH}$$
$$f_{k+1} < (\frac{7}{4})^{k}(\frac{44}{16})$$
$$f_{k+1} < (\frac{7}{4})^{k}(\frac{49}{16}) \qquad \text{changed } 44 \text{ to } 49. \text{ Statement still true.}$$
$$f_{k+1} < (\frac{7}{4})^{k}(\frac{7}{4})^2$$
$$f_{k+1} < (\frac{7}{4})^{k+2}$$

The result is true for $n = k + 1$, and so holds for all $n \in \mathbb{N}$ by POSI. □

Example 3.6. $P(n)$: In every group of n people, all the people have the same birthday.

Wrong Proof: BC: $n = 1$. True.
IH: Assume $P(1), P(2), \ldots, P(k)$ are true for $k \in \mathbb{N}$
Consider $n = k + 1$.
Kick somebody out of the group. Everybody left has the same birthday by IH. Let the person back in but kick somebody else out. Use the IH again, on the new subgroup, and everyone has the same birthday still.

Flaw: Falls apart for $k + 1 = 2$. □

——————————-Midterm stops here ——————————————

4 Greatest Common Divisor

4.1 Introduction to GCD

Definition 4.1. Let $a, b \in \mathbb{Z}$ where $a \neq 0 \vee a - b \neq 0$. The **greatest common divisor** of a and b, written $\gcd(a, b)$, is a positive integer d, such that $d \mid a$ and $d \mid b$. If $c \mid a$ and $c \mid 0$, then $c = d$.

Example 4.1.

$$\gcd(50, 30) = 10 \qquad \gcd(-36, 44) = 4 \qquad \gcd(-12, -18) = 6 \qquad \gcd(0, 100) = 100$$

We define $\gcd(0, 0)$ to be 0.

Theorem 4.1 (GCD WR)**. GCD With Remainders** states: if a and b are integers not both zero, and q and r are integers such that $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d = \gcd(a, b)$. Since $d = \gcd(a, b)$, $d \mid b$. Observe that $r = a - qb$. Since $d \mid a$ and $d \mid b$, d $\mid (a(1) + b(-q))$ by DIC, so $d \mid r$.

Let $c \mid b$ and $c \mid r$. Then $c \mid (b(q) + r(1))$ by DIC. Since $a = qb + r$, $c \mid a$. Then since $d = \gcd(a, b)$ and $c \mid a$ and $c \mid b$, then $c \leq d$. Hence $d = \gcd(b, r)$. □

Example 4.2. Prove that the GCD exists.

Proof. True by definition for $\gcd(0, 0)$. Otherwise, when $a \neq 0$ or $b \neq 0$, then if $a \mid b$, $a \leq |b|$ by BBD. $1 \mid a$ and $1 \mid b$. □

Example 4.3. Prove that there is only one gcd.

Proof. Suppose $s = \gcd(a, b)$ and $t = \gcd(a, b)$.Since $s = \gcd(a, b)$, $s \mid a$ and $s \mid b$. Therefore since $t = \gcd(a, b)$, $s \leq t$ Similarly, $t \leq s$. $\therefore t = s$. □

Theorem 4.2 (GCD CT)**. GCD Characterization Theorem** states if d is a positive common divisor of $a, b \in \mathbb{Z}$, and there exists integers x and y so that $ax + by = d$ then $d = \gcd(a, b)$

4.2 Primes

Definition 4.2. An integer $p > 1$ is a **prime** if its only divisors are 1 and p, and **composite** otherwise.

Theorem 4.3 (PAD)**. Primes and Divisibility** states: if p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Assume p is prime and $p \mid ab$. Consider two cases

1. If $p \mid a$, there is nothing to show.
2. Assume $p \nmid a$. The only divisors of p are 1 and p. Therefore $\gcd(a, p) = 1$. By CAD, $p \mid b$.

$$P \implies (Q \vee R) \equiv ((P \wedge \neg Q) \implies R)$$

□

Theorem 4.4 (UFT)**.** The **Fundamental Theorem of Arithmetic** or **Unique Factorization Theorem** states that if $n \in N$, then n can be written as a product of prime factors, and the factorization is unique.

Theorem 4.5 (DFPF)**. Divisors From Prime Factorization:** If $a \in N$ and $a = p_1^{\alpha 1} p_2^{\alpha 2} \cdots p_k^{\alpha k}$ is the PF into distinct powers of primes, then the divisors of a are

$$d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \text{ where } 0 \leq d_i \leq \alpha_i \text{ for } i = 1, 2, \ldots, k$$

Theorem 4.6 (GCD PF)**. GCD from Prime Factorization** shows that if the prime factorization of two numbers are given, their GCD is the product of the primes to the lower exponent between the two numbers.

Example 4.4. Find the GCD of $24750 = 2^1 3^2 5^3 11^1$ and $434511 = 3^3 7^1 11^2 19^1$

Solution.

$$\gcd(24750, 434511) = 3^3 7^1 11^2 = 7623$$

4.3 Extended Euclidean Algorithm

Definition 4.3. The **floor** of a number x, written $\lfloor x \rfloor$ is the largest integer less than or equal to x.

Example 4.5. Compute $\gcd(1386, 322)$.

Solution. Begin with a table:

x	y	r	q
1	0	a	0
0	1	b	0

After the first two rows are generated, use the formula

$$q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$$

In this case

$$q_3 = \left\lfloor \frac{1386}{322} \right\rfloor = 4$$

Next, $\text{Row}_i = \text{Row}_{i-2} - q_i \times \text{Row}_{i-1}$. In the example we get $x = 1, y = -4, r = 98$.

After completing the table we get

x	y	r	q
1	0	a	0
0	1	b	0
1	-4	98	4
-3	13	28	3
10	-43	14	3
-23	99	0	2

Definition 4.4 (EEA)**.** The **Extended Euclidean Algorithm** is used to not only compute $\gcd a, b)$, but also the data x and y for the certificate (check). $a, b \in \mathbb{N} \implies d = gcd(a, b)$ can be computed and $\exists x, y \in \mathbb{Z}, ax + by = d$. It requires $a > b$, if $a < b$, simply swap the numbers.

4.4 Properties of GCDs

Definition 4.5. Two integers are **coprime** if their gcd is 1.

Theorem 4.7 (CAD)**. Coprimeness and Divisibility** states that if $a, b, c \in \mathbb{Z}$ and $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

Proof. Assume $c \mid ab$ and $\gcd(a, c) = 1$. By EEA, $ax + cy = 1$ for some $x, y \in \mathbb{Z}$. Multiply to get $abx + bcy = b$. Since $c \mid ab$, $ab = ck$ for some integers k. Substitute and factor the equation $c(kx + by) = b$. Since $kx + by$ is an integer, $c \mid b$. □

Theorem 4.8 (DB GCD)**. Division by the GCD**: Let a and b be integers. If $\gcd(a, b) = d \neq 0$ then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Exercise 4.1. Prove if $\gcd(a, b) = 1$, then for any $c \in \mathbb{N}$, $\gcd(a, bc) = \gcd(a, c)$.

Proof. By EEA, $ax + by = 1$ and $ax' + cy' = d$ for some $x, y, x', y' \in \mathbb{Z}$ where $d = \gcd(a, c)$. Multiply the equations to get $(ax + by)(ax' + cy') = d$.

$$a(xx' + cxy' + byx') + bc(yy') = d$$

The new LHS is an integer linear combination of a and bc. By definition, $d \in \mathbb{Z}, d > 0, d \mid a$. We also known $d \mid c$ and clearly $c \mid bc$ so by TD, $d \mid bc$. Hence by GCD CT, $d = \gcd(a, bc)$ □

5 Modular Arithmetic

5.1 Linear Diophantic Equation

Theorem 5.1 (LDET 1)**. Linear Diophantine Equation Theorem, Part 1** states the linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ where $d = \gcd(a, b)$.

Proof. $\Rightarrow$: Suppose $ax_0 + by_0 = c$ has an integer solution, and $d = \gcd(a, b)$.
By definition $d \mid a$ and $d \mid b$ so by DIC, $d \mid ax + by$, and $d \mid c$.

$\Leftarrow$: Assume $c = dk$ where $k \in \mathbb{Z}$. By EEA, $ax_0 + by_0 = d$ where $x, y \in \mathbb{Z}$. Therefore $c = (ax_0 + by_0)k = ax_0k + by_0k$. Since x_0k and y_0k are integers, then there exists an integer solution to $ax + by = c$. □

Theorem 5.2 (LDET 2)**.** Let $\gcd(a, b) = d$ where $a, b \neq 0$. If $x = x_0$ and $y = y_0$ is a particular integer solution to $ax + by = c$, then the complete integer solution is

$$x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n, \forall n \in \mathbb{Z}$$

Example 5.1. $20x + 35y = 5$. If one solution is $(x, y) = (2, -1)$ then the complete solution is

$$(x, y) = (2 + 7n, -1 - 9n), \forall n \in \mathbb{Z}$$

Note. Another solution is $(-5, 3)$ and $(x, y) = (-5 + 7n, 3 - 4n), \forall n \in \mathbb{Z}$ represents the same set.

Example 5.2. Find all solutions to $15x - 24y = 9$ where $0 \leq x, y \leq 20$.

Solution. Equation can be divided by 3. $5x - 8y = 3$ One particular solution is $(x, y) = (-1, -1)$ The complete solution is

$$(x, y) = (-1 - 8n, -1 - 5n)$$

Now we must add in the domain restrictions.

$-1 - 8n \geq 0$	$-1 - 5n \geq 0$	$-1 - 8n \leq 20$	$-1 - 5n \leq 20$
$8n \leq -1$	$5n \leq -1$	$8n \geq -21$	$5n \geq -21$
$n \leq -\frac{1}{8}$	$n \leq -\frac{1}{8}$	$n \geq -\frac{21}{8}$	$n \geq -\frac{21}{8}$
$n \leq -1$	$n \leq -1$	$n \geq 2$	$n \geq -4$

Therefore the only solutions are $n = -1$ and $n = -2$. Plug them into the complete solution to get $(7, 4)$ and $(15, 9)$

5.2 Congruence

Definition 5.1. Let m be a fixed positive integer. Let $a, b \in \mathbb{Z}$, if $m \mid (a - b)$, then

$$a \equiv b \pmod{m}$$

Otherwise, we write $a \not\equiv b \pmod{m}$

Theorem 5.3 (CER)**. Congruence Equivalent Relation:** Let $m \in \mathbb{N}$. Let $a, b, c \in \mathbb{Z}$. Then

- **Reflexivity:** $a \equiv a \pmod{m}$
- **Symmetry:** $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
- **Transitivity:** $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

Theorem 5.4 (PC)**. Properties of Congruence:** Let $a, a', b, b' \in \mathbb{Z}$ If $a \equiv a' \pmod{m}$ and $b \equiv b \pmod{m}$, then

- $a \pm b \equiv a' \pm b' \pmod{m}$
- $ab \equiv a'b' \pmod{m}$

Example 5.3. Is $5^9 + 62^{2000} - 14$ divisible by 7?

Solution.

$$\begin{aligned}
5^9 + 62^{2000} - 14 &\equiv 5^9 + 62^{2000} && \pmod 7 \\
&\equiv 5^9 + (-1)^{2000} && \pmod 7 \\
&\equiv 5^9 + 1 && \pmod 7 \\
&\equiv (5^2)^4 5 + 1 && \pmod 7 \\
&\equiv 4^4(-2) + 1 && \pmod 7 \\
&\equiv (4^2)^2(-2) + 1 && \pmod 7 \\
&\equiv 2^2(-2) + 1 && \pmod 7 \\
&\equiv -7 && \pmod 7 \\
&\equiv 0 && \pmod 7
\end{aligned}$$

Example 5.4. A positive integer is divisible by 9 iff the sum of its digits is divisible by 9.

Proof. Let $n \in \mathbb{N}$. Write $n = a_r \times 10^r a_{r-1} \times 10^{r-1} \dots a_1 \times 10 + a_0$ Mod everything by 9

$$\equiv a_r + a_{r-1} + \cdots + a_1 + a_0$$

$\therefore$ If the sum of an integer's digits is divisible by 9, the integer is divisible by 9. □

Definition 5.2 (CD)**. Congruences and Division** states if $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod m$.

Proof. Assume $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$. Then $m \mid (ac - bc)$. Therefore $m \mid c(a - b)$. Additionally, by CAD, $m \mid a - b$. Therefore $a \equiv b \pmod m$ □

Definition 5.3 (CISR)**. Congruent Iff Same Remainder** states

$$a \equiv b \pmod m \iff a \text{ and } b \text{ have the same remainder when divided by } m$$

For example $24 \equiv 17 \pmod 7$. Then $24 \equiv 3 \pmod 7$ and $17 \equiv 3 \pmod 7$.

Example 5.5. What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?

Solution. Reduce the modulo 4 using PC.

$$\begin{aligned}
77^{100}(999) - 6^{83} &\equiv 1^{100}(-1) - 6^{83} \pmod 4 \\
&\equiv -1 + 2^2 \times 2^{81} \pmod 4 \\
&\equiv -1 + 0 \times 2^{81} \pmod 4 \\
&\equiv 3 \pmod 4
\end{aligned}$$

Note. Only write $\pmod n$ if there is a congruent sign, don't write it if there is an equal sign.

Example 5.6. What is the last digit of

$$5^{32}3^{10} + 9^{22}$$

Solution. Use PC and reduce modulo 10. Note that

$$5^2 \equiv 5 \pmod{10}, 5^4 \equiv 5^2 \equiv 5 \pmod{10} \dots 5^{32} \equiv 5 \pmod{10}$$
$$3^{10} \equiv (-1)^5 \equiv -1 \pmod{10}$$
$$9^{22} \equiv (-1)^{22} \equiv 1 \pmod{10}$$

$$\begin{aligned} 5^{32}3^{10} + 9^{22} &\equiv 5(-1) + 1 \pmod{10} \\ &\equiv -4 \pmod{10} \\ &\equiv 6 \pmod{10} \end{aligned}$$

Therefore the last digit is 6.

Linear Congruences

Example 5.7.

$$4x \equiv 5 \pmod{8}$$
$$4x - 5 = 8y'$$
$$4x + 8y = 5$$

$\gcd(4, 8) = 2$ and $2 \nmid 5$ so the equation does not have a solution.

Example 5.8.

$$5x = 3 \pmod{7}$$
$$5x + 7y = 3$$

A particular solution is $(x, y) = (2, -1)$. By LDET 2, the complete solution is

$$x = 2 + 7n \qquad \forall n \in \mathbb{Z}$$
$$x \equiv 2 \pmod{7}$$

The value of y doesn't matter, question only asks for x.

Alternatively, by CISR, every integer solution is congruent to exactly one of the elements $\{0, 1, 2, 3, 4, 5, 6\}$. By PC if $x_0 \in \mathbb{Z}$ is a solution, then all $x \equiv x_0 \pmod{7}$ work too.

Example 5.9.

$$2x \equiv 4 \pmod{6}$$
$$2(0) = 0 \not\equiv 4 \pmod{6}$$
$$2(1) = 2 \equiv 4 \pmod{6}$$
$$2(2) = 4 \not\equiv 4 \pmod{6}$$
$$2(3) = 6 \not\equiv 4 \pmod{6}$$
$$2(4) = 8 \not\equiv 4 \pmod{6}$$
$$2(5) = 10 \equiv 4 \pmod{6}$$

Therefore the solution is $x \equiv 2, 5 \pmod{6}$
Using LDE, $x \in \{2 + 3n : n \in \mathbb{Z}\}$ and the complete solution is $x \equiv 2 \pmod{3}$

Note. The two sets are actually equal.

Definition 5.4 (LCT 1)**. Linear Congruence Theorem** states the linear congruence $ax \equiv c \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid c$.

Definition 5.5 (LCT 2)**.** Let $\gcd(a, m) = d \neq 0$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Furthermore there exists d solutions $\mod m$, and if $x = x_0$ is a solution, the complete solution is

$$\left\{[x_0], \left[x_0 + \frac{m}{d}\right], \left[x_0 + 2\frac{m}{d}\right], \left[x_0 + (d-1)\frac{m}{d}\right]\right\}$$

Congruent Classes

Fix $m = 6$

$$\begin{aligned}[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod{6}\} \\ &= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = 6k\} \\ &= \{6k : k \in \mathbb{Z}\}\end{aligned}$$

Definition 5.6. Let $m \in \mathbb{N}, a \in \mathbb{Z}$. The **congruence class** of $a \pmod{m}$ is

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$$

Example 5.10. If $m = 6$, $[5] = [17]$ because $5 \pmod{6} \equiv 17 \pmod{6}$. There are exactly 6 congruent classes modulo 6.

$$\mathbb{Z}_6 = \Big\{[0], [1], [2], [3], [4], [5]\Big\}$$

Definition 5.7. Let $m \in \mathbb{N}$. The integers modulo m are

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

Definition 5.8. Fix $m \in \mathbb{N}$. Consider Z_m

$$[a] + [b] = [a + b]$$

$$[a] \times [b] = [a \times b]$$

Exercise 5.1. Consider $\mathbb{Z}_{21}$ Solve $[48][x] = [10]$

Solution.

$$[48][x] = [10] = [6][x] = [10]$$

$$[6x] = [10]$$

$$6x \equiv 10 \pmod{21}$$

$$3x = 5 \pmod{21}$$

Since $\gcd(3, 21) \nmid 5$, there is no solution.

Inverses

In $\mathbb{Z}_m, [a] + [-a] = [0] \, \forall a \in \mathbb{Z}$

Definition 5.9. Multiplicative Inverse: Let $m \in \mathbb{N}, a \in \mathbb{Z}$. The multiplicative inverse of $[a]$ is some $[b] \in \mathbb{Z}_m$ such that $[a][b] = [b][a] = [1]$. We write $[b] = [a]^{-1}$

Example 5.11. In $\mathbb{Z}_{18}$, $[5]^{-1} = [11]$ because multiplying the two gives $[1]$. The multiplicative inverse of $[9]$ does not exist.

5.3 Fermat's Little Theorem

Definition 5.10 (FIT)**.** Let p be prime and $a \in \mathbb{Z}$, If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Suppose p is prime and $p \nmid a$. Assume $ra \equiv sa \pmod{p}$ where $0 < r \geq s < p$. Then $p \mid a(r-s)$. By PAD, $p \mid r - s$. Therefore $r = s$. This tells us that $a, 2a, 3a, \ldots, (p-1)a$ are unique modulo p. Hence $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Since $\gcd(p, (p-1)!) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$ □

Corollary 5.1. Let p be prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$

Corollary 5.2. Let $[a]$ be a non-zero element of $\mathbb{Z}_p$, then $[a]^{-1}$ exists.

Example 5.12 (Polynomial Congruence)**.** Find all $x \in \mathbb{Z}$ such that $x^5 + x^3 + 2x^2 + 1$ is divisible by 5.

Solution. We solve $x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod{5}$. Brute force solution. First simplify using a corollary to FIT:

$$x^5 \equiv x \pmod{5}$$

x	0	1	2	3	4
$x^3 + 2x^2 + x + 1$	1	0	4	4	1

By PC, the full solution is $x \equiv 1 \pmod{5}$

Simultaneous Congruences

Solve

$$x \equiv 2 \pmod{13} \tag{1}$$

$$x \equiv 17 \pmod{29} \tag{2}$$

Write 1 as $x = 2 + 13s$ where $s \in \mathbb{Z}$. Substitute into 2.

$$2 + 13s = 17 \pmod{29}$$

$$13s \equiv 15 \pmod{29}$$

$$13sx - 29y = 15$$

x	y	r	m
1	0	29	0
0	1	13	0
1	-2	3	2
-4	9	1	4
$-$	$-$	0	0

By LDET 2 $29(-4) + 13(9) = 1$
$29(-60) + 13(135) = 15$
$s \equiv 135 \pmod{29} \equiv 19 \pmod{29}$. Write $s = 19 + 29t$ where $t \in \mathbb{Z}$.

$$x = 2 + 13(19 + 29t)$$

$$x = 249 + 377t$$

The solution is $x \equiv 249 \pmod{377}$.

Theorem 5.5 (CRT)**. Chinese Remainder Theorem**: If $\gcd(m_1, m_2) = 1$ then for all $a_1, a_2 \in \mathbb{Z}$ there exists a solution to

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

Moreover, if $x = x_0$ is a solution, then the completely solution is $x \equiv x_0 \pmod{m_1 m_2}$.

Example 5.13. Solve

$$x \equiv 5 \pmod{6} \tag{3}$$
$$x \equiv 2 \pmod{7} \tag{4}$$
$$x \equiv 3 \pmod{11} \tag{5}$$

Inspecting and checking gives $x \equiv 23 \pmod{42}$ is the solution to 3 and 4 by CRT.

$$x \equiv 23 \pmod{42} \tag{6}$$
$$x \equiv 3 \pmod{11} \tag{7}$$

By rearranging and using EEA, solution is

$$x = 443 \pmod{462}$$

Example 5.14.

$$3x \equiv 2 \pmod{5} \tag{8}$$
$$2x \equiv 6 \pmod{7} \tag{9}$$

The solution to 8 is $x \equiv 4 \pmod{5}$ and to 9 is $x \equiv 3 \pmod{7}$. Solve these two linear congruences to get $x = 24 \pmod{35}$

Example 5.15.

$$x \equiv 4 \pmod 6 \tag{10}$$
$$x \equiv 2 \pmod 8 \tag{11}$$

Rewrite 10 as $x = 4 + 6s$ where $s \in \mathbb{Z}$ Sub into 11,

$$4 + 6s \equiv 2 \pmod 8$$
$$6s \equiv 6 \pmod 8$$

Using LCT 1 or 2, there is a unique solution mod 4.

$$s \equiv 1 \pmod 4$$
$$s = 1 + 4t$$
$$x = 4 + 6(1 + 4t)$$
$$x = 10 + 24t$$
$$x \equiv 10 \pmod{24}$$

Example 5.16.

$$x^2 \equiv 34 \pmod{99}$$

Use CRT to consider

$$x^2 \equiv 34 \pmod 9$$
$$x^2 \equiv 34 \pmod{11}$$

Rewrite as

$$x^2 \equiv 7 \pmod 9$$
$$x^2 \equiv 1 \pmod{11}$$

There are two solutions to each equation, so by multiplying each pair, there are four solutions.

$$x \equiv 23, 32, 67, 76 \pmod{99}$$

Example 5.17. Solve $x^3 - 29x^2 + 35x + 38 = 0 \pmod{195}$

Solution.

$$195 = 15 \times 13$$
$$x^3 + x^2 + 5x + 8 \equiv 0 \pmod{15}$$
$$x^3 + 10x^2 + 9x + 12 \equiv 0 \pmod{13}$$

Use a table to find all solutions. Every combination of a solution to the first equation to a solution to the second equation is a simultaneous linear congruence.

Finish, should have 12 different solutions

5.4 Cryptography

- Choose primes p and q and $p \neq q$. Set $n = pq$ and let $\phi(n) = (p-1)(q-1)$
- Choose ϵ where $1 < \epsilon \leq \phi(n)$ and $\gcd(\epsilon, \phi(n)) = 1$
- Solve $\epsilon d = 1 \pmod{\phi(n)}$ where $0 < d \leq \phi(n)$
- Publish public key (e, n)
- Secure private key (d, n)

Example 5.18. Set $p = 2, q = 11, n = 22$

$$\phi(n) = 10$$

Let $e = 3$

$$3d = 1 \pmod{10}$$
$$d = 7$$

Public key: $(3, 22)$. Private key: $(7, 22)$.

Encryption

1. Generate message M where $0 \leq M < n$
2. Compute C where $0 \leq C < n$ and $M^\epsilon \equiv C \pmod{n}$
3. Send ciphertext C

1. Compute R where $0 \leq R < n$ and $C^d \equiv R \pmod{n}$

Example 5.19. Encryption:

$$\begin{aligned} M &= 8 \\ 8^3 &\equiv C \pmod{22} \\ 8 \times 8^2 &\equiv 8 \times 22 \pmod{22} \\ 8 \times 8^2 &\equiv 50 \pmod{22} \\ 8 \times 8^2 &\equiv 6 \pmod{22} \end{aligned}$$

Decryption:

$$\begin{aligned} 6^7 &\equiv r \pmod{22} \\ &\equiv 6^4 \times 6^2 \times 6 \pmod{22} \\ &\equiv 14^2 \times 14 \times 6 \pmod{22} \\ &\equiv 14^2 \times 84 \pmod{22} \\ &\equiv 196 \times 18 \pmod{22} \\ &\equiv 20 \times 18 \pmod{22} \\ &\equiv 8 \pmod{22} \end{aligned}$$

Theorem 5.6 (RSA)**.** In RSA $R = M$

Proof.

$$R \equiv C^d \pmod{n}$$
$$\equiv (M^e)^d \pmod{n}$$
$$(M^e d) \pmod{n}$$
$$M^{1+k(p-1)(q-1)} \pmod{n} \qquad \exists k \in \mathbb{Z}$$
$$M \times M^{k(p-1)(q-1)} \pmod{n}$$

Since $p \mid n$ then

$$M \times M^{k(p-1)(q-1)} \pmod{p}$$

There are two cases:

1. $p \nmid M$

$$R \equiv M \times (M^{p-1})^{k(q-1)} \pmod{p}$$
$$R \equiv M \pmod{p} \text{ by FLT}$$

2. $p \mid M$

$$R \equiv 0 \pmod{p}$$
$$R \equiv M \pmod{p}$$

Similarly, show

$$R \equiv M \pmod{q}$$

Then R and M are both solutions to $x \equiv M \pmod{p}$ and $x \equiv P \pmod{q}$.
Since $p \neq q$, $\gcd(p, q) = 1$ so by CRT, $R \equiv M \pmod{pq}$, then $R \equiv M \pmod{n}$
Since $0 \leq M < n$ then $P = M$.

□

6 Complex Numbers

Definition 6.1. A **complex number** in standard form is an expression of the form $x+yi$ where $x, y \in \mathbb{R}$. The complex numbers, written $\mathbb{C}$ is the set $\{x + yi : x, y \in \mathbb{R}\}$

Example 6.1. For $x + yi \in \mathbb{C}$, x is the real part and y is the imaginary part. We write $\mathrm{Re}(x + yi) = x$ and $\mathrm{Im}(x + yi) = yi$

Definition 6.2. With $x + yi$, if $y = 0$, the number is purely real. If $x, y \neq 0$ then $x + yi$ is purely imaginary.

$$\mathbb{R} \subsetneq \mathbb{C}$$

Arithmetic

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$
$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

Example 6.2. Solve $x^2+2x+3=0$

$$x=\frac{-2\pm\sqrt{4-4(1)(3)}}{2}$$
$$x=-1\pm\sqrt{-2}$$
$$x=-1+\sqrt{2}i,-1-\sqrt{2}i$$

Example 6.3. Express $\frac{1+2i}{3-4i}$ in standard form.

Solution. Multiply by conjugate

$$\left(\frac{1+2i}{3-4i}\right)\left(\frac{3+4i}{3+4i}\right)=\frac{-5+10i}{25+0i}$$
$$=-\frac{1}{5}+\frac{2}{5}i$$

Theorem 6.1.

$$i^{0 \pmod 4}=i$$
$$i^{1 \pmod 4}=-1$$
$$i^{2 \pmod 4}=-i$$
$$i^{3 \pmod 4}=1$$

Definition 6.3. The **complex conjugate** of $z=x+yi$ is $\overline{z}=x-yi$.

If z and w are complex numbers,

$$\overline{z+w}=\overline{z}+\overline{w}$$
$$\overline{zw}=\overline{z}\,\overline{w}$$
$$z+\overline{z}=2\Re(z)$$
$$z-\overline{z}=2\Im(z)$$

Definition 6.4. The **modulus** of the complex number $z=x+yi$ is

$$|z|=|x+yi|=\sqrt{x^2+y^2}$$

This is also the distance between the number and the origin on the complex plane.

$$\overline{z}z=|z|^2$$
$$|zw|=|z||w|$$
$$|z+w|\le|z|+|w|$$

6.1 Graphical Representation

Definition 6.5. The **complex plane** or **Argand plane** is similar to the Cartesian plane with the x axis being labelled as the real axis, and y as imaginary axis.

- Conjugate $\implies$ reflection over real axis.
- Modulus $\implies$ distance from origin.
- Addition $\implies$ vector addition.

Definition 6.6. Given the polar coordinates (r, θ), the corresponding Cartesian cordinates (x, y) are

$$x = r\cos\theta$$

$$y = r\sin\theta$$

Given the Cartesian coordinates (x, y), the corresponding polar coordinates are determined by

$$r = \sqrt{x^2 + y^2}$$

$$\cos\theta = \frac{x}{r}$$

$$\sin\theta = \frac{y}{r}$$

Definition 6.7. The **polar form** if a complex number z is

$$z = r(\cos\theta + i\sin\theta)$$

where r is the modulus of z and the angle θ is called an argument of z.

Theorem 6.2. If

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_2)$$

$$z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$$

Then $z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$

Theorem 6.3 (DMT)**. De Moivre's Theorem** states:
Let $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$. Then $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$

Corollary 6.1. If $z = r(\cos\theta + i\sin\theta)$ then

$$z^n = r^n\cos(n\theta) + i\sin(n\theta)$$

Definition 6.8. The **complex exponential function** is

$$e^{i\theta} = \cos\theta + i\sin\theta$$

Properties include:

$$e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$

$$(e^{i\theta})^n = e^{in\theta}$$

Definition 6.9. If a s a complex number, then the complex numbers that solve $z^n = a$ are called the **complex n-th roots**. De Moivre's theorem is used to solve these.

Example 6.4. Solve $z^6 = -64$. (Find all sixth roots of -64)

Solution. Let $z = r(\cos\theta + i\sin\theta)$. By DMT,

$$z^6 = r^6(\cos 6\theta + i\sin 6\theta)$$

In addition,

$$-64 = 64(\cos\pi + i\sin\pi)$$

$z^6 = -64$ so $r^6 = 64$. Thus $r = 2$ since $r \geq 0$.

$$-64 = 64(\cos 6\theta + i\sin 6\theta)$$

$$6\theta = \pi$$
$$\theta = \frac{\pi + 2\pi k}{6}, \forall k \in \mathbb{Z}$$

There are 6 unique values for θ, hence 6 solutions.

$$\theta = \frac{\pi}{6}, \frac{3\pi}{6}, \frac{5\pi}{6}, \frac{7\pi}{6}, \frac{9\pi}{6}, \frac{11\pi}{6}$$

The solutions are

$$2(\cos\theta + i\sin\theta)$$

substituted with all possible values of θ.

Theorem 6.4 (CNRT)**. Complex n-th Roots Theorem** states that if $r(\cos\theta + i\sin\theta)$ is the polar form of a complex number a, then then solutions to $z^n = a$ are

$$\sqrt[n]{r}(\cos(\frac{\theta + 2k\pi}{n}) + i\sin(\frac{\theta + 2k\pi}{n})) \qquad \text{for } k = 0, 1, 2, \ldots, n-1$$

Note. There are n solutions all equally spaced on a circle of radius $\sqrt[n]{r}$ centered at the radius.

Definition 6.10. An **n-th root of unity** is a complex number that solves $z^n = 1$.

7 Polynomials

Definition 7.1. A **field** is a set of numbers that allows addition, subtraction, multiplication and division. It includes the rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$ and the integers modulo a prime p, $\mathbb{Z}_p$.

Definition 7.2. A **polynomial in x over the field $\mathbb{F}$** is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where all of the a_i belong to $\mathbb{F}$. The a_i are called **coefficients**.

Example 7.1. $\mathbb{F}[x]$ denotes the set of polynomials in x with coefficients from $\mathbb{F}$.

Example 7.2. Examples of polynomials over a field:

- $[2]x^3 + [1]x + [4] \in \mathbb{Z}_5[x]$.
- $x^3 + 7ix + (5 - 2i) \in \mathbb{C}[x]$

Method 7.1. The product of polynomials $f(x)$ and $g(x)$ is

$$f(x) \cdot g(x) = \sum_{i=0}^{m+n} c_i x^i$$

$$c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 = \sum_{j=0}^{i} a_j b_{i-j}$$

This is just the long division formula.

Theorem 7.1. Division Algorithm: If $f(x)$ and $g(x)$ are polynomials in $\mathbb{F}[x]$ then there exists a unique polynomial $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

To find the quotient and remainder polynomials, use long divison.

Theorem 7.2 (FTA)**.** The **Fundamental Theorem of Algebra** states that for all complex polynomials $f(z)$ with $\deg(f(z)) \geq 1$, there exists a $z_0 \in C$ so that $f(z_0) = 0$
Unfortunately that's all that can be determined. There is no strict formula for determining the value of the root.

Theorem 7.3. Remainder Theorem states that the remainder when the polynomial $f(x)$ is divided by $(x - c)$ is $f(c)$.

Theorem 7.4 (FT)**. Factor Theorem** states that the linear polynomial $(x - c)$ is a factor of the polynomial $f(x)$ if and only if c is a root of the polynomial $f(x)$.

Theorem 7.5 (RRT)**. Rational Roots Theorem:** If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients and $\frac{p}{q}$ is a rational root of $f(x)$ where $\gcd(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.

Proof. Assume the hypothesis is true. Substitute to get

$$a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \cdots + a_1(\frac{p}{q}) + a_0 = 0$$

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

Then

$$p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 p q^{n-1}) = -a_0 q^n$$

Since every variable is an integer $p \mid a_0 q^n$. Since $\gcd(p, q) = 1$, by CAD, $p \mid a_0$. A similar approach may be used for q. □

Example 7.3. Solve $2x^3 + x^2 - 6x - 3 = 0 \in \mathbb{C}$
If $\frac{p}{q}$ is a rational root in lowest terms, the $p \mid (-3)$ and $q \mid 2$ by RRT.

$$\frac{p}{q} \in \left\{\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}\right\}$$

Note.

$$f\left(-\frac{1}{2}\right) = -\frac{1}{4} + \frac{1}{4} + 3 - 3 = 0$$

$x + \frac{1}{2}$ is a factor of $f(x)$. Use long division to get $f(x) = (2x+1)(x^2-3)$.

$$\therefore x = -\frac{1}{2}, \sqrt{3}, -\sqrt{3}$$

Example 7.4. Fully factor $x^3 - \frac{32}{15} + \frac{1}{5}x + \frac{2}{5} = \mathbb{Q}[x]$

Solution. We will find the roots of

$$15x^3 - 32x^2 + 3x + 2$$

By RRT, $x = 2, -\frac{1}{5}, \frac{1}{3}$

$$(x-2)(x+\frac{1}{5})(x-\frac{1}{3})$$

Exercise 7.1. Prove $\sqrt{2}$ is irrational.

Solution. Let $x = \sqrt{2}$, and note that x is a root of $x^2 - 2$. By RRT, the rational roots of $x^2 = 2$ are $\{\pm 1, \pm 2\}$. Trying all possibilities, none of these are roots , therefore all the roots are irrational, and $\sqrt{2}$ must be irrational.

Exercise 7.2. Prove that $\sqrt{5} + \sqrt{3}$ is irrational.

Solution. Let $x = \sqrt{5} + \sqrt{3}$.

$$\begin{aligned} x^2 &= 5 + 2\sqrt{15} + 3 \\ x^2 &= 8 + 2\sqrt{15} \\ x^2 - 8 &= 2\sqrt{15} \qquad \text{square both sides} \\ x^4 - 16x^2 + 64 &= 60 \\ x^4 - 16x^2 + 4 &= 0 \end{aligned}$$

By RRT, the only possible roots are $\{\pm 1, \pm 2, \pm 4\}$ and none of them are roots. $\sqrt{5} + \sqrt{3}$ is a root to the polynomial, and therefore $\sqrt{5} + \sqrt{3}$ is irrational.

Theorem 7.6 (CJRT)**. Conjugate Roots Theorem:** Suppose $c \in \mathbb{C}$ is a root of a real polynomial. Then $\bar{c}$ is alos a root of the polynomial.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$.
Assume $f(x) = 0$ for some $c \in C$.

$$f(c) = 0$$
$$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0 = 0$$
$$\overline{a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0} = \overline{0}$$
$$\overline{a_n c^n} + \overline{a_{n-1}c^{n-1}} + \cdots + \overline{a_1 c} + \overline{a_0} = 0 \qquad \text{by PCJ}$$
$$\overline{a_n}\,\overline{c}^n + \overline{a_{n-1}}\,\overline{c}^{n-1} + \cdots + \overline{a_1}\,\overline{c} + \overline{a_0} = 0 \qquad \text{by PCJ}$$
$$a_n \overline{c}^n + a_{n-1}\overline{c}^{n-1} + \cdots + a_1 \overline{c} + a_0 = 0$$
$$f(\overline{c}) = 0$$

Note. This requires $f(x) \in \mathbb{R}[x]$. For example $(x+i)^2 = x^2 + 2ix - 1$. $-i$ is a root but $\overline{-i}$ is not a root.

□

Exercise 7.3. Fully factor $x^4 - 5x^3 + 16x^2 - 9x - 13$ given that $2 - 3i$ is a root.

Theorem 7.7 (RQF)**. Real Quadratic Factors:** Let $f(x)$ be a polynomial with real coefficients. If $c \in \mathbb{C}$, and c is a root of f, where $\Im(c) \neq 0$, then there exists a real quadratic factor of $f(x)$ with c as a root.

Theorem 7.8 (RFRP)**. Real Factors of Real Polynomials:** Let $f(x)$ be a polynomial with real coefficients. Then $f(x)$ can be written as a product of real linear and real quadratic factors.

Example 7.5.

$$x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$$