MATH 135 - Algebra for Honours Math

Kevin Carruthers

Winter 2013

Implications

Definition: An impication is a statement S such that a hypothesis (or assumption) H ensures the validity of the conclusion C, and may either be true or false. An implication is only false if a hypothesis is true and the conclusion is false (ie a counter-example exists). In other words, for S: $P \implies Q$ (P implies Q), S is true unless P is true and Q is false.

Note that this can give confusing results such as

- If $1 = 2$, then $2 = 2$
- If $1 = 2$, then $2 = 3$

Because $1 = 2$ is a false hypothesis, both of these implications are true, regardless of the vailidty of their conclusion.

Direct Proof

For a direct proof, we start by assuming the hypothesis, and derive the conclusion.

1. Always assume the hypothesis is true.
2. Never assume the conclusion is true.
3. Starting from the hypothesis, think of what can be derived using definitions, theorems, and logical deductions.
4. Look toward the conclusion, think of what needs to be achieved to prove the conclusion.

Proposition: ***For $S_0 = A \implies B$, $S_1 = B \implies C$, and $S_2 = A \implies C$, prove S_2 given S_0 and S_1.***

Proof:
Assume A. Since both A and $A \implies B$ are true, B is true. Since B and $B \implies C$ are true, C is true. Thus $A \implies C$ is true. QED.

Proposition: ***Given S_0, S_1, and S_2, assume S_0 and S_2 are true. Must S_1 be true?***

Proof:
$B \implies C$ is false if and only if B is true and C is false. If C is false, we have A is false, so we have both $A \implies B$ and $A \implies C$ are true, but $B \implies C$ is false. Thus S_0 and S_2 do not imply S_1. QED.

Divisibility

Definition: An integer m divides an integer n if there exists an integer k such that $n = km$. This is denoted as $m \,|\, n$.

Proposition: ***Transitivity of Divisibility***
Let a, b, and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:
Since $a \,|\, b$, there exists an integer k such that $b = ka$.
Since $b \,|\, c$, there exists an integer j such that $c = jb$.
Then $c = jka$. Since $jkin\mathbb{Z}$, we have $a \,|\, c$. QED.

Sets

A set is a collection of objects. We use the notation $einS$ for element e in set S. Sets can not have duplicate elements and may be defined in any order. They may be described in **set builder notation** $S = \{x_0, x_1, ..., x_n\}$, $T = \{2k + 1 \mid kin\mathbb{R}\}$

If S and T are sets, the **cartesian product** of S and T is

$$S \times T = \{(a, b) \mid ainS, binT\}$$

The order of elements within each pair does matter.

For a finite set S, the **cordinality** of S is the number of elements in S, denoted $|S|$. Note that $|S \times T| = |S||T|$. The empty set is the only one with a cordinality of 0.

Operations

Note that we use $\wedge$, $\vee$, and $\neg$ to denote "and", "or", and "not".

1. Union: $S \cup T = \{x \mid xinS \vee xinT\}$
2. Intersection: $S \cap T = \{x \mid xinS \wedge xinT\}$
3. Complement: $S^c = \{x \mid x \notin S\}$. Note that $S^{c^c} = S$.
   - Complements are transitive, ie $(A \cap B)^c = A^c \cap B^c$.
4. Difference (relative complement of B in A): $S \setminus T = \{x \mid xinS \wedge x \notin T\}$. In other words, $S \setminus T = S \cap B^c$.

- Relative complements are inversely transitive, ie $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Subsets

Definition: S is a **subset** of T ($S \subseteq T$) if and only if for every $xin\mathbb{R}$, $xinS \implies xinT$. Note that $S \subseteq S$ and the zero set is a subset of every other set.

For a set S, the **power set** is the set of all possible subsets of S, denoted by $\mathcal{P}(S)$ or 2^S

Example: for $S = \{1, 2\}$, $\mathcal{P}(S) = \big\{\{\}, \{1\}, \{2\}, \{1, 2\}\big\}$ thus $\{2\}in\mathcal{P}(S)$ but $2 \notin \mathcal{P}(S)$ so $\big\{\{2\}\big\}\subseteq \mathcal{P}(S)$. $|\mathcal{P}(S)| = 4$, or $|\mathcal{P}(n)| = 2^{|n|}$

Equality

$A = B$ if and only if for every $xin\mathbb{R}$, $(xinA \iff xinB)$. From the definitions of a subset, we also have $A = B \iff A \subseteq B$ and $B \subseteq A$.

Proposition: $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$
Proof:
Let $xinS \cap (T \cup U)$.
So $xinS$ and $xinT \cup U$.
We have two cases:
If $xinT$, $xinS \cap T$.
If $xinU$, $xinS \cap U$.
Therefore, $xin(S \cap T) \cup (S \cap U)$. QED.

Quantifiers

The **universal quantifier** $\forall$ means "for all" and the **existential quantifier** $\exists$ means "there exists".

Examples:

$\forall x$, $x = 3$ is false if $xin\mathbb{Z}$ but true if $xin\{3\}$

$\exists y$, $y < 1$ is true if $yin\mathbb{Z}$ but not if $yin\mathbb{N}$

We can thus compare these qualifiers to logical statements. For example

$$\forall x, P(x) = P(x_0) \wedge P(x_1) \wedge P(x_2)...$$

and

$$\exists x, P(x) = P(x_0) \vee P(x_1) \vee P(x_2)...$$

Proving Statements Containing Quantifiers

Note that some quantifiers can be hidden in words. For example, the mathematical definition of divisibility is $a \,|\, c \implies \exists k in \mathbb{Z} \mid c = ka$

1. To prove that something exists, construct this thing.
2. To prove a universal property, select an arbitrary member of the universe and prove the property for this instance.

Nested Qualifiers

Proposition: $\forall x in \mathbb{R}, \exists y in \mathbb{R} \mid y < x$
Proof:
Let $x in \mathbb{R}$,
Then $y = x - 1$ satisfies $y in \mathbb{R}$ and $y < x$. QED.

but **Proposition:** $\exists y in \mathbb{R}, \forall x in \mathbb{R} \mid y < x$
Proof:
If such a y exists, then $x = y$ does not satisfy $y < x$.
This is a contradiction, thus the proposition is false. QED.

Proposition: $\forall x in \mathcal{P}(\mathbb{N}), x \notin \{\} \implies \exists y in x, \forall z in x \mid y < z$
Proof:
Can be accepted logically. QED.

Binary Relations

Let X be a set. A **binary relation** on X is a two-variable predicate $\mathcal{R}$ defined on X (ie for $\{(x, y) in X \text{ x } X\}, \mathcal{R}(x, y)$ may be either true or false). When $\mathcal{R}(x, y)$ holds, we say x *is* $\mathcal{R}$ *-related to* y and write $x\mathcal{R}y$.

Equality, ordering, and divisibility are all examples of relations. We also have

$$A \subseteq B \iff \forall x in S, (x in A \implies x in B)$$

and for any $A, B in \mathcal{P}(S)$ the disjointedness relation

$$A \perp B \iff A \cap B = \{\}$$

For a binary relation on set X, the relation is

- Reflexive if $\forall x in X, x\mathcal{R}x$
- Symmetric if $\forall x, y in X, x\mathcal{R}y \implies y\mathcal{R}x$
- Transitive if $\forall x, y, x in X, x\mathcal{R}y \wedge y\mathcal{R}z \implies x\mathcal{R}z$

Equivalence Relations

Let X be a non-empty set. An **equivalence relation** on X is a binary relation on X that is reflexive, symmetric, and transitive. The most common example of this is for $S = \{(x, y) in \mathbb{R}$ x $\mathbb{R} \mid x = y\}, x\mathcal{R}y$ is an equivalent relation.

Implication Modifiers

Converses

The **converse** of $A \implies B$ is $B \implies A$. Note that the converse does not necessarily have the same truth value as the original implication. If both statements are true, then the elements within them are equivalent.

Negations

Let A, B, and C be statements. Then

1. $\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$
2. $\neg(A \vee B) \iff (\neg A) \wedge (\neg b)$
3. $\neg(A \implies B) \iff A \wedge \neg B$
4. $\neg(\neg A)) \iff A$

Let S be a set, $P(x)$ is a statement dependant on $xinS$. Then

1. $\neg(\forall xinS, P(x)) \iff \exists xinS, \neg P(x))$
2. $\neg(\exists xinS, P(x)) \iff \forall xinS, \neg P(x))$

To find the negation of $P(x)$, we can do the following

$$\begin{aligned}
P(x) &= \exists yin\mathbb{R}, \forall xin\mathbb{R} \mid y < x \\
\neg P(x) &= \neg(\exists yin\mathbb{R}, \forall xin\mathbb{R} \mid y < x) \\
&= \forall yin\mathbb{R}, (\neg(\forall xin\mathbb{R} \mid y < x)) \\
&= \forall yin\mathbb{R}, \exists xin\mathbb{R} \mid y \geq x
\end{aligned}$$

Contrapositive

Definition: The contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$. A statement and its contrapositive are equivalent, and it can sometimes be easier to prove the contrapositive.

Proposition: ***For*** $ninZ$***, if*** n^2 ***is even then*** n ***is even***

Proof:
Suppose n is odd.
Then $n = 2k + 1$ for some $kin\mathbb{Z}$.
So $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$.
Then n^2 is odd. Thus we have n is odd $\implies$ n^2 is odd, so n^2 is even $\implies$ n is even.
QED.

Use a contrapositive when the hypothesis does not give much to work with or when the negation of the implication is nicer.

Contradiction

Assume the conclusion is false (or the contrapositive is false). If you derive something impossible, the assumption must be wrong.

Uniqueness

To prove the existence of x, suppose there are two of them x and y. Try to prove either it must be the case that $x = y$, or assume $x \neq y$ and reach a contradiction.

Deduction Overview

Methods of deduction:

- Direct: assume the hypothesis and find the conclusion.
- Example: especially with quantifiers, find an example which breaks the implication.
- Contrapositive: prove the contrapositive.
- Absurdity: Assume the implication (or contrapositive) is false, try to find something blatantly contradictory.

Induction

Induction is useful when proving general statements $\forall x$.

Principle of Mathematical Induction

Suppose $P(n)$ is a statement for $n \geq n_0$. If

1. $P(n_0)$ is true, and

2. $\forall k \geq n_0, P(k) \implies P(k+1)$.

Then, by induction, $P(n)$ is true $\forall n \geq n_0$.

Weak Induction

Weak induction is a general technique based directly on the Principle of Mathematical Induction (henceforth refered to as POMI), and is suited to proving statements of the form "$\forall n \geq n_0, P(n)$". It consists of two steps:

1. the **base case** (prove $P(n_0)$), and
2. the **induction step** (chose an arbitrary $k \geq n_0$ for which we assume $P(k)$, then prove $P(k+1)$).

Then we simply invoke the POMI to conclude $\forall n, P(n)$.

Proposition: $\forall n \geq 2, (1+x)^n > 1 + nx$
Proof:
For $n = 2$ we have

$$\begin{aligned} P(2) &= (1+x)^2 \\ &= 1 + 2x + x^2 \\ &> 1 + 2x + 0 \\ &> 1 + 2x \end{aligned}$$

This proves $P(2)$
Assume that $(1+x)^k > 1 + kx$. Then

$$\begin{aligned} P(k+1) &= (1+x)^{k+1} \\ &= (1+x)^k(1+x) \\ &> (1+kx)(1+x) \\ &> 1 + kx + x + kx^2 \\ &> 1 + (k+1)x + 0 \\ &> 1 + (k+1)x \end{aligned}$$

So $\forall k \geq 2, P(k) \implies P(k+1)$. Thus, by POMI, $\forall n \geq 2, (1+x)^n > 1 + nx$. QED.

Strong Induction

Strong induction is an alternative to weak induction which may be used when $P(k+1)$ is dependant on either multiple past cases or a single past case $P(j)$ where the relative location of $j < k$ cannot be determined.

Principle of Strong Induction, v1

Definition: Let $P(n)$ be a property concerning integers $n \geq n_0$. Suppose that the following are true:

1. $P(n_0)$, and
2. $\forall k \geq n_0, \forall n_o \leq j \leq k, P(j) \implies P(k+1)$

Then $\forall n, P(n)$.

Proposition: ***Every natural number*** $n > 1$ ***can be expressed as a product of primes.***

Proof:
For any $n \geq 2$, if n is prime then n is the product of a single prime (itself). Thus n is prime $\implies P(n)$.
Assume n is composite. By definition $\exists m \mid 1 < m < n \wedge m \,|\, n$.
For $n = md, din\mathbb{N}$, we have $1 < d < n$.
By induction hypothesis, $P(m) \wedge P(d)$, which means we can express m and d as products of primes. The we can write

$$m = p_0 p_1 ... p_s$$

and

$$d = q_0 q_1 ... q_t$$

so

$$n = md = (p_0 p_1 ... p_s)(q_0 q_1 ... q_t)$$

is a product of primes. By POSI, $\forall n \geq 2, n$ is a product of primes. QED.

Principle of Strong Induction, v2

The first version of POSI can fail given certain low values of k (for certain $P(n)$ we may have $P(n) \iff n \geq b \wedge b \geq n_0$). We thus modify POSI to separately verify the multiple base cases of $P(j)$ for $n_o \leq j \leq b$.

Definition: Let $P(n)$ be a property concerning integers $n \geq n_0$. Suppose, for some integer $b \geq n_0$, the following are true:

1. $P(n_0), P(n_0+1), ..., P(b)$, and
2. $\forall k \geq b, \forall n_o \leq j \leq k, P(j)$

Proposition: $\forall n \geq 60, n = 7x + 11y; n, x, yin\mathbb{Z}, x, y \geq 0$***. Use the following equalities:***

$$1 = 7(-3) + 11(2) \tag{1}$$
$$1 = 7(8) + 11(-5) \tag{2}$$
$$60 = 7(7) + 11(1) \tag{3}$$

Proof:
Equation (3) clearly verifies $P(60)$.
Since we have x is multiplied by 7 and $7 < 11$, we take $P(j)$ with $60 \leq j \leq 66$ as the base cases, all of which can be verified with a list of equations (omitted).
Assume that $k \geq 67$ is such that $P(j)$ holds for all $60 \leq j < k$.
Since $k \geq 67, k - 7 \geq 60$ and so $P(k - 7)$ is true, thus

$$k - 7 = 7x + 11y$$

for some x and y. We can manipulate this equation to have

$$k = 7(x + 1) + 11y$$

and since $x + 1 in \mathbb{Z} \wedge x + 1 \geq 0, P(k)$.
Thus we have shown that whenever $k \geq 67, P(60), ...P(k - 1)$ all true imply $P(k)$. By POSI, this proposition is true. QED.

Properites of Various Things

Divisibility

Proposition: *Divisibility of Integer Combinations*
Let $a, b, c in \mathbb{Z}$***.*** $a \mid b \wedge a \mid c \implies a \mid bx + cy, \forall x, y in \mathbb{Z}$
Proof:
Since $a \,|\, b \wedge a \,|\, c$, there exists $k, l in \mathbb{Z}$ such that $b = ka$ and $c = la$
Then $bx + cy = kax + lay = a(kx + ly)$. Since $kx + ly in \mathbb{Z}, a \,|\, bx + cy$. QED.

Proposition: *Bounds by Divisibility*
Let $a, b in \mathbb{Z}. a \mid b \wedge b \neq 0 \implies |a| \leq |b|$
Proof:
Since $a \,|\, b$, there exist $k in \mathbb{Z}$ such that $b = ka$.
Then $|b| = |ka| = |k||a| \geq |a|$. QED.

Division Algorithm

Proposition: ***Let*** $a in \mathbb{Z} \wedge b in \mathbb{N}$***. Then there exist unique integers*** q, r ***such that*** $a = qb + r$ ***where*** $0 \leq r < b$

Greatest Common Divisors

Definition: For any $a, b in \mathbb{Z}$ not both 0, the greatest common divisor of a and b, denoted $\gcd(a, b)$, is the integer d such that $d \,|\, a \wedge d \,|\, b$ and $c \,|\, a \wedge c \,|\, b \implies c \leq d$.

Proposition: ***GCD with Remainders***
If $a, b, q, rin\mathbb{Z}$ ***such that*** $a = qb + r$***, then*** $\gcd(a, b) = \gcd(b, r)$

Proof:

Let $d = \gcd(a, b)$.
Since d is a common divisor of $a, b, d \mid b$.
We see that $r = a - qb$. Since $a - qb$ is an integer combination of a and b, $d \mid a - qb$, so $d \mid r$.
Let c be a common divisor of b and r. So $c \mid b \wedge c \mid r$.
Since $qb + r$ is an integer combination of b and r, $c \mid qb + r$. So $c \mid a$. Therefore, c is a common divisor of a, b. Since $d = \gcd(a, b), c \leq d$.
Thus $d = \gcd(b, r)$ so $\gcd(a, b) = \gcd(b, r)$. QED.

Proposition: ***GCD Characterization***
For $a, bin\mathbb{Z}$***, if*** $d \mid a, d \mid b, d \geq 0$***, and*** $\exists x, yin\mathbb{Z}$ ***such that*** $ax + by = d$***, then*** $d = \gcd(a, b)$***.***

Proof:

If $a = b$ then $\gcd(a, b) = 1$ so then $x = 1, y = 0$ is an integer solution to $ax + by = a$.
Without loss of generality, assume $a > b$. Define function $E(a, b)$ to be the number of steps required when feeding (a, b) into the Euclidean algorithm. We will prove by induction on $E(a, b)$.
$E(a, b) = 1$ so $b \mid a$. Then $\gcd(a, b) = b$.
Assume for some $k \geq 1$ the result holds when $E(a, b) = k$.
Suppose $E(a, b) = k + 1$. In the first step of the alogirthm, we calculate $a = qb + r$ and $\gcd(a, b) = \gcd(b, r)$.
Let $d = \gcd(a, b)$. Then $E(b, r) = k$, so there exists $x_0, y_0 in\mathbb{Z}$ such that $bx_0 + ry_0 = \gcd(b, r) = d$.
Substitute $r = a - qb$ to get $d = bx_0 + (a - qb)y_0 = ay_0 + b(x_0 - qy_0)$.
Then $x = y_0, y = x_0 - qy_0$ is an integer soution to $ax + by = d$. QED.

Coprimes

Definition: For $a, bin\mathbb{Z}$, a and b are coprime if $\gcd(a, b) = 1$.

Proposition: ***Coprimesness and Divisibility***
If $a, b, cin\mathbb{Z}$ ***where*** $c \mid ab$ ***and*** a ***and*** c ***are coprime, then*** $c \mid b$***.***

Proof:

Since $\gcd(a, c) = 1$, there exist x, y such that $ax + cy = 1$. Then $bax + bcy = b$.
Since $c \mid ab \wedge c \mid c$, $c \mid bax + bcy$ (by integer combination) so $c \mid b$. QED.

Proposition: ***Primes and Divisibility***
If $a, bin\mathbb{Z}$***,*** p ***is prime and*** $p \mid ab$***, then*** $p \mid a$ ***or*** $p \mid b$***.***

Proof:

Assume $p \nmid a$. Since the only positive factors of p are 1 and p and $p \nmid a$, $\gcd(p, a) = 1$.
Given Coprimeness and Divisibility, $p \mid b$. So $p \mid a \vee p \mid b$. QED.

Proposition: ***Division by GCD***
If $a, bin\mathbb{Z}$ ***where*** $d = \gcd(a, b > 0$ ***then*** $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$

Linear Diophantine Equations

Definition: An LDE has the form $a_0x_0 + a_1x_1 + ... + a_nx_n = c$ where $a_0, ...a_n, cin\mathbb{Z}$ and $x_0, ...x_n$ are integer variables.

Given the one variable case $ax = c$, there exists a solution if and only if $a \mid c$. If there is a solution, that solution is unique. For the two variable case $ax+by = c$ the set of all solutions is $\{(x_0, y_0)in\mathbb{Z}$ x $\mathbb{Z} \mid ax_0 + by_0 = c\}$.

Generally, $ax + by = c$ has an integer solution whenever $\gcd(a, b) \mid c$.

Proposition: ***LDE 1***
Let $a, b, cin\mathbb{Z}, d = \gcd(a, b)$***. Then*** $ax + by = c$ ***has an integer solution if and only if*** $d \mid c$***.***

Proposition: ***LDE 2***
Let $a, b, cin\mathbb{Z}, d = \gcd(a, b) > 0$***. If*** (x_0, y_0) ***is an integer solution to*** $ax + by = c$***, the complete set of integers is*** $\left\{\left(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n\right) \mid nin\mathbb{Z}\right\}$***.***

Primes

Euclid's Theorem hols that there are infintiely many primes. Note that every integer greater than two is a product of primes.

Proposition: ***Each composite integer*** n ***has a prime divisor of at most*** $\sqrt{m}$

Fundamental Theorem of Arithmetic

Proposition: ***Every integer greater than one can be expressed uniquely as a product of primes (up to the order of the factors).***

Prime Factorization

Each positive integer can be writen as $n = p_0^{n_0}p_1^{n_1}...p_k^{n_k}$ where each p is a distinct prime and each n is a non-negative integer.

Proposition: ***If*** $a = p_0^{n_0}p_1^{n_1}...p_k^{n_k}$ ***is a prime factorization of*** a***, then*** d ***is a positive divisor of*** a ***if and only if*** $d = p_0^{d_0}p_1^{d_1}...p_k^{d_k}$ ***where*** $d_i \leq a_i$ ***for each*** i***.***

Proposition: ***If*** $a = p_0^{a_0}p_1^{a_1}...p_k^{a_k}$ ***and*** $b = p_0^{b_0}p_1^{b_1}...p_k^{b_k}$ ***are prime factorizations of*** a ***and*** b***, then*** $\gcd(a, b) = p_0^{d_0}p_1^{d_1}...p_k^{d_k}$ ***where*** $d_i = \min(a_i, b_1)$ ***for all*** i***.***

Congruences

Definition: Let m be a fixed positive integer and $a, bin\mathbb{Z}$. Then a is congruent to b module m if $m \mid a - b$. We write $a \equiv b \pmod{m}$. Equivelently, $a \equiv b \pmod{m}$ if $a = b + km$ for some $kin\mathbb{Z}$.

Note that congruences are reflexive, symmetric, and transitive.

Arithmetic of Cogruences

Proposition: ***Let*** $a, b, a', b'in\mathbb{Z}, min\mathbb{N}$***. If*** $a \equiv a' \pmod{m}$ ***and*** $b \equiv b \pmod{m}$ ***then***

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

Modular Arithmetic

Definition: Let $min\mathbb{N}$. For any $ain\mathbb{Z}$, we define $[a] = \{kin\mathbb{Z} \mid a \equiv k \pmod{m}\}$. In turn, this allows us to define $\mathbb{Z}_m = \{[0], [1], ...[m-1]\}$.

Within $\mathbb{Z}_5$ we have $[3] + [4] = [7] = [2]$ and $[1] - [3] = [1] + [2] = [3]$.

The main point of this: $a \equiv b \pmod{m} \iff [a] = [b]$ in $\mathbb{Z}_m$.

This also gives us two representations of **Fermat's Little Theorem**:

- If p is prime and $p \nmid a$ where $ain\mathbb{Z}$, then $a^{p-1} \equiv 1 \pmod{p}$
- In $\mathbb{Z}_p$, if $[a] \neq [0]$ then $[a^{p-1}] = 1$

Linear Congruences

$ax \equiv b \pmod{m} \iff [a][m] = [b]$ in $\mathbb{Z}_m$.

Proposition: $ax \equiv b \pmod{m}$ ***has an integer solution if and only if*** $\gcd(a, m) \mid b$***.***

Chinese Remainder Theorem

The CRT deals with simultaneous congruences. Example $n \equiv a_1 \pmod{m}_1$ and $n \equiv a_2 \pmod{m}_2$.

Proposition: ***If*** m_1 ***and*** m_2 ***are coprime, then there exists a solution to this set of congruences. If*** n_0 ***is one such solution, the entire set of solutions can be given by*** $n \equiv n_0 \pmod{m_1 m_2}$***.***

Generalized form: if $m_0, m_1, ...m_k in \mathbb{N}$ where all are coprime, then for any $a_0, a_1, ...a_k in \mathbb{Z}$, the set of congruences has a solution. If n_0 is a solution, then the complete solution set is $n \equiv n_0 \pmod{m_0 m_1 ... m_k}$.

System of Linear Congruences

For the system of linear congruences $2x + 4y \equiv 5 \pmod{13}$ and $2x + 5y \equiv 7 \pmod{13}$, we often write this as $\begin{bmatrix} 3 & 4 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 7 \end{bmatrix} \pmod{13}$. We can then use vector algebra to solve this. We solve for $A^{-1} = \det(A)^{-1} \begin{bmatrix} b & -b \\ -c & a \end{bmatrix}$, and use $\begin{bmatrix} x \\ y \end{bmatrix} = A^{-1} \begin{bmatrix} 5 \\ 7 \end{bmatrix} \pmod{13}$.

Square and Multiply

Example problem: Find the remainder of $\frac{a^n}{m}$ when n is large.

Example: find the remainder of $9^1 9$ divides by 100.
$9^1 \equiv 9 \pmod{100}$
$9^2 \equiv 81 \pmod{100}$
$9^4 \equiv 81^2 \equiv 61 \pmod{100}$
$9^8 \equiv 61^2 \equiv 21 \pmod{100}$
$9^{16} \equiv 21^2 \equiv 41 \pmod{100}$
$9^{19} \equiv 41(81)9 \equiv 89 \pmod{100}$.

While technically valid, this method takes $2\log_2(n)$ steps. One possible optimization is to use FLT as a shortcut.

Complex Numbers

The set of complex numbers is defined as $\mathbb{C} = \{a + bi \mid a, b in \mathbb{R}\}$. The standard form of one such number is $z = a + bi$, where a is the **real part** and bi is the **imaginary part**.

We also define the conjugate $\overline{a + bi} = a - bi$ and the modulus $|a + bi| = \sqrt{a^2 + b^2}$.

Complex numbers are commutative and distributive under addition and multiplication. The additive identity is 0 and the additive inverse of $a = bi$ is $-a - bi$. The multiplicative idnetity is 1 and the multiplicative inverse of $a + bi$ is $\frac{a-bi}{a^2+b^2}$.

Properties of Complex Numbers

1. $|z| = 0 \iff z = 0$
2. $z \cdot \overline{z} = |z|^2$
3. $|zw| = |z||w|$

4. $|z+w| \leq |z| + |w|$ *(this is the triangle inequality for complex numbers)*

Complex Angles

We write $\cos\theta + i\sin\theta$ as $e^{i\theta}$ and for $z = a + bi = r(\cos\theta + i\sin\theta) = re^{i\theta}$.

Thus we have

- $\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}$
- $\sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i}$
- $\cosh\theta(x) = \frac{e^{x}+e^{-x}}{2}$
- $\sinh\theta(x) = \frac{e^{x}-e^{-x}}{2}$

So we know $\cos(x) = \cosh(ix)$ and $\sin(x) = -i\sinh(ix)$.

Nth Roots

For $a, zin\mathbb{C}$, we want $z^n = a$. Suppose $a = re^{i\theta}$ and $z = se^{i\phi}$. Then $s = r^{\frac{1}{n}}$ and $\phi = \frac{\theta+2\pi k}{n}$

Polynomials

Definition: Let $\mathbb{F}$ be a field (informally, a number system closed under arithmetic operations, i.e. $\mathbb{R}$). A polynomial in x over $\mathbb{F}$ is anything of the form $\sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1}x_{n-1} + \ldots a_1 x + a_0$ where $n \geq 0$, $nin\mathbb{N}$, $a_n, a_{n-1}, \ldots a_1, a_0 in\mathbb{F}$. The set of all polynomials in x over $\mathbb{F}$ is denoted as $\mathbb{F}(x)$.

Polynomials such as x^2+1 can not be factored in $\mathbb{R}$, but it can be factored in $\mathbb{C}$ with $(x+i)(x-i)$. In $\mathbb{Z}_2$, we can factor it as $(x+1)^2$, but it is not factorizable in $\mathbb{Z}_n, n \neq 2$. Thus the same polynomial can act quite differently given varying $\mathbb{F}$.

For any two polynomials in $\mathbb{F}$, we define addition and subtraction in the obvious way (by coefficient terms) as $f(x) \pm g(x) = \sum_{i=0}^{n}(a_i \pm b_1)x^i$. Multiplication is defined as $f(x)g(x) = \sum_{i=0}^{n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)x^i$ (note that this equation also works for power series). This also gives us the power formula $f^k(x) = \sum_{i=0}^{n}\binom{k+i-1}{i-1}x^i$.

Though there is no formula for division, we do have the **division algorithm for polynomials**: if $f(x), g(x) in\mathbb{F}$ and $g(x)$ is not the zero poynomial, then there exist unique polynomials in $\mathbb{F}$ such that $f(x) = p(x)g(x) + r(x)$ and the degree of $r(x)$ is between zero and the degree of $g(x)$.

Cryptography

Private Key

The keys must be kept between two users. Anyone with the key can decode the ciphertext, but otherwise they can not. Key exchange needs to be done privately. $\binom{100}{2} = 4950$ keys are required.

Key management among a large group of people is a problem.

Public Key

The key for encryption is published, thus we need a system where knowing the encryption key does not help in decrypting a message.

RSA

Key Generation:

1. Pick two big prime numbers p, q.
2. Let $n = pq$.
3. Let $\phi(n) = (p-1)(q-1)$.
4. Pick e that is coprime with $\phi(n)$.
5. Find d such that $ed \equiv 1 \pmod{\phi(n)}$.

The receiver published the public encryption key e, n and keeps the private decryption key d, n to themselves.

Encryption and Decryption:

We only encrypt integer messages M where $0 \leq M < n$. For encryption, the cipher text C is one where $C \equiv m^e \pmod{n}$. The decrypted text D is one where $D \equiv C^d \pmod{n}$. This works when $M \equiv D \pmod{n}$ in all cases.

Example: Public key $(19, 4307)$, private key $(1099, 4307)$. We turn an English message into integers, so we have "PR" is $M = 1618$. $C \equiv 1618^{10} \equiv 2762 \pmod{4307}$. To decrypt C we have $D \equiv 2762^{1099} \equiv 1618 \pmod{4307}$.

Proposition: $D \equiv M \pmod{n}$

Proof:
We have $D \equiv M^{ed} \pmod{n}$.
We then split n into p and q.
We first claim that $M^{ed} \equiv M \pmod{p}$.
Suppose $p \nmid M$. By FLT, $M^{p-1} \equiv 1 \pmod{p}$.
Since $eD \equiv 1 \pmod{\phi(n)}, \exists k in \mathbb{Z}$ such that $ed = 1 + k(p-1)(q-1)$.
Then $M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv MM^{k(p-1)(q-1)} \pmod{p}$.
Since $M^{p-1} \equiv 1 \pmod{p}$, this is equivalent to $M1^{k(q-1)}$, so $M^{ed} \equiv M \pmod{p}$.
Now suppose $p \mid M$. Then $M \equiv 0 \pmod{p}$ and $M^{ed} \equiv 0 \pmod{p}$.
So $M^{ed} \equiv M \pmod{p}$.
By switching the roles of p and q, we get that $M^{ed} \equiv M \pmod{q}$.
This implies simultaneous congruence, and by CRT we have $M^{ed} \equiv M \pmod{pq}$. QED.

Propositions

This section is a summary of all "important" propositons covered in this course. For an exhaustive list, see the next pages.

Proposition (Transitivity of Divisibility (TD)). *For $a, bin\mathbb{Z}$, $a \mid b \wedge b \mid c \implies a \mid c$*

Proposition (Divisibility of Integer Combinations (DIC)). *For $a, b, c, x, yin\mathbb{Z}$, $a \mid b \wedge a \mid c \implies a \mid bx + cy$.*

Proposition (Bounds by Divisibility (BBD)). *For $a, bin\mathbb{Z}$, $a \mid b \wedge b \neq 0 \implies |a| \leq |b|$.*

Proposition (Division Algorithm (DA)). *For $a, bin\mathbb{Z}$ and $b > 0$, $\exists q, r \mid a = qb + r \wedge 0 \leq r < b$.*

Proposition (GCD with Remainders (GCD WR)). *For $a, bin\mathbb{Z}$ not both zero, if we have integers q, r such that $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.*

Proposition (GCD Characterization Theorem (GCD CT)). *If d is a positive common divisor of a and b, and there exists integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.*

Proposition (Extended Euclidean Algorithm (EEA)). *For $a, bin\mathbb{Z}$ both positive, then $d = \gcd(a, b)$ can be computed and there exist integers x and y such that $ax + by = d$.*

Proposition (Congruences and Division (CD)). *$ac \equiv bc \pmod{m} \wedge \gcd(c, m) = 1 \implies a \equiv b \pmod{m}$.*

Proposition (Fermat's Little Theorem (FLT)). *If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proposition (Fermat's Little Theorem Corollary (F$\mathbb{L}$T)). *For any integer a and prime p, $a^p \equiv a \pmod{p}$.*

Proposition (Existence of Inverses is $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)). *If p is prime and $[a]$ is a non-zero element within $\mathbb{Z}_p$, then $\exists [b] in\mathbb{Z}_p \mid [a] \cdot [b] = 1$*

Proposition (Chinese Remainder Theorem (CRT)). *For any set of linear congruences, if $\gcd(m_0, ...m_k) = 1$, then the solution can be given by $n = n_0 \pmod{m_0...m_k}$.*

Proposition (RSA). *If p and q are distinct primes, $n = pq$, e and d are positive integers such that $ed \equiv 1 \pmod{(p-1)(q-1)}$, $0 \leq M < n$, $M^e \equiv C \pmod{n}$, and $C^d \equiv R \pmod{n}$ where $0 \leq R < n$, then $R = M$.*

Proposition (Cardinality of Disjoint Sets (CDS)). *If S and T are disjoint finite sets, then $|S \cup T| = |S| + |T|$*

Proposition (Cardinality of Intersecting Sets (CIS)). *If S and T are any finite sets, then $|S \cup T| = |S| + |T| - |S \cap T|$*

Proposition (Cardinality of Subsets of Finite Sets (CSFS)). *If S and T are finite sets and $S \subset T$, then $|S| < |T|$*

Propositions (Full List)

Proposition (Transitivity of Divisibility (TD)). *For $a, binℤ$, $a \mid b \wedge b \mid c \implies a \mid c$*

Proposition (Divisibility of Integer Combinations (DIC)). *For $a, b, c, x, yinℤ$, $a \mid b \wedge a \mid c \implies a \mid bx + cy$.*

Proposition (Bounds by Divisibility (BBD)). *For $a, binℤ$, $a \mid b \wedge b \neq 0 \implies |a| \leq |b|$.*

Proposition (Division Algorithm (DA)). *For $a, binℤ$ and $b > 0$, $\exists q, r \mid a = qb + r \wedge 0 \leq r < b$.*

Proposition (GCD with Remainders (GCD WR)). *For $a, binℤ$ not both zero, if we have integers q, r such that $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.*

Proposition (GCD Characterization Theorem (GCD CT)). *If d is a positive common divisor of a and b, and there exists integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.*

Proposition (Extended Euclidean Algorithm (EEA)). *For $a, binℤ$ both positive, then $d = \gcd(a, b)$ can be computed and there exist integers x and y such that $ax + by = d$.*

Proposition (Coprimeness and Divisibility (CAD)). *Let $a, b, cinℤ$. If a and c are coprime, $c \mid ab \implies c \mid b$*

Proposition (Division by GCD (DB GCD)). *For $a, binℤ$, not both zero, $d = \gcd(a, b) \implies 1 = \gcd(\frac{a}{d}, \frac{b}{d})$*

Proposition (Linear Diophantine Equation Theorem 1 (LDET1)). *Let $a, b, cinℤ$ and $d = \gcd(a, b)$. $ax + by = c$ has an integer solution if and only if $d \mid c$*

Proposition (Linear Diophantine Equation Theorem 2 (LDET2)). *Let $a, b, cinℤ$ and $d = \gcd(a, b) \neq 0$. If (x_0, y_0) is one particular integer solution to $ax + by = c$, then the complete set of integer solutions is*

$$\left(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n\right) \mid ninℤ$$

Proposition (Euclid's Theorem (INF P)). *There are an infinite number of primes.*

Proposition (Fundamental Theorem of Arithmetic (UFT)). *Every integer greater than 1 can be uniquely expressed as a product of primes (apart from the order of the factors)*

Proposition (Primes and Divisibility (PAD)). *If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$*

Proposition (Divisors from Prime Factorization (DFPF)). *If $x = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$ is a prime power decomposition of x, then d is a positive integer of x if and only if $d = p_1^{d_1} p_2^{d_2} ... p_n^{d_n}$ where $d_i \leq a_i$ for each i.*

Proposition (GCD from Prime Factorization (GCD PF)). *If $a = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} ... p_k^{b_k}$, then $\gcd(a, b) = p_1^{d_1} p_2^{d_2} ... p_k^{d_k}$ where $d_i = \min(a_i, b_i)$ for each i.*

Proposition (Congruence is an Equivalence Relation (CER)). *Let $minℕ$ and $a, b, cinℤ$. Then $a \equiv a \pmod{m}$, $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$, and $a \equiv b \pmod{m} \wedge b \equiv c$*

$\pmod m \implies a \equiv c \pmod m$

Proposition (Properties of Congruence (PC)). *If* $a \equiv a' \pmod m \wedge b \equiv b' \pmod m$, *then* $a + b \equiv a' + b' \pmod m$, $a - b \equiv a' - b' \pmod m$, *and* $ab \equiv a'b' \pmod m$

Proposition (Congruences and Division (CD)). $ac \equiv bc \pmod m \wedge \gcd(c, m) = 1 \implies a \equiv b \pmod m$.

Proposition (Congruent iff Same Reminder (CISR)). *Let* $a, bin\mathbb{Z}, min\mathbb{N}$. *Then* $a \equiv b \pmod m \iff a\%m = b\%m$

Proposition (Fermat's Little Theorem (FLT)). *If* p *is prime and* $p \nmid a$, *then* $a^{p-1} \equiv 1 \pmod p$.

Proposition (Linear Congruence Theorem 1 (LCT 1)). *Let* $\gcd(a, m) = d \geq 1$. *The linear congruence* $ax \equiv c \pmod m$ *has a solution if and only if* $d|c$. *Moreover, if* x_0 *is one solution, then the complete solution is* $x \equiv x_0 \pmod{\frac{)}{m}d}$.

Proposition (Linear Congruence Theorem 2 (LCT 2)). *Let* $\gcd(a, m) = d \geq 1$. *The equation* $[a][x] = [c]$ *in* $\mathbb{Z}_m$ *has a solution if and only if* $d \mid c$. *Moreover, if* $[x_0]$ *is one solution, the complete solution would be* $x = [x_0], [x_0 + \frac{m}{d}], ...[x_0 + (d-1)\frac{m}{d}]$.

Proposition (Chinese Remainder Theorem (CRT)). *For any set of linear congruences, if* $\gcd(m_0, ...m_k) = 1$, *then the solution can be given by* $n = n_0 \pmod{m_0 ... m_k}$.

Proposition (Properties of Conjugates (PC)). *If* z *and* w *are complex numbers, then* $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{zw}$, $\overline{\overline{z}} = z$, $z + \overline{z} = 2Re(z)$, $z - \overline{z} = 2Im(z)$

Proposition (Properties of Modulus (PM)). *If* $z, win\mathbb{C}$, *then* $|z| = 0 \iff z = 0$, $|z| = |\overline{z}|$, $|z|^2 = z\overline{z}$, $|zw| = |z||w|$, $|z + w| \leq |z| + |w|$

Proposition (DeMoivre's Theorem (DMT)). *For any* $\theta in\mathbb{R}$ *and* $nin\mathbb{Z}$, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$

Proposition (Complex nth Roots Theorem (CNRT)). *If* $a = r(\cos\theta + i\sin\theta)$, *then the solutions to* $z^n = a$ *are* $r^{\frac{1}{n}}\left[\cos\frac{\theta+2k\pi}{n} + i\sin\frac{\theta+2k\pi}{n}\right]$ *for* $k = 0, 1, ...n - 1$.

Proposition (Fundamental Theorem of Algebra (FTA)). *For all complex polynomials,* $f(x)$ *with* $\deg(f(x)) \geq 1$, $\exists x_0 in\mathbb{C} \mid f(x_0) = 0$

Proposition (Remainder Theorem (RT)). *The remainder of* $f(x)$ *divided by* $x - c$ *is* $f(c)$

Proposition (Factor Theorem (FT)). *The linear polynomial* $x - c$ *is a factor of* $f(x)$ *if and only if* $f(c) = 0$

Proposition (Conjugate Roots Theorem (CRT)). *Let* $f(x)in\mathbb{R}[x]$, *if* $cin\mathbb{C}$ *is a root of* $f(x)$, *then so is* $\overline{c}$