Discrete Mathematics with Applications

Dr Liew How Hui

May 2021

Outline

Logic for Equality

To make predicate logic useful, a generic relation equality (=) is needed. Given two expressions `a, b : A` we write `a = b : Prop` for the proposition that `a` and `b` are equal, that is they describe the same object.

How can we prove an equality? That is what is the introduction rule for equality? We can prove that every expression is `a : A` is equal to itself `a = a` using the tactic reflexivity. How can we use an assumption `H : a = b`? That is how can we eliminate equality? If we want to prove a goal `P` which contains the expression `a` we can use rewrite `H` to rewrite all those as into `b`s.

Logic for Equality (cont)

To demonstrate how to use these tactics we show that equality is an equivalence relation (see the Topic on Relations):

- reflexive: `forall a:A, a = a`
- symmetric: `forall a b:A, a=b -> b=a`
- transitive: `forall a b c:A, a=b -> b=c -> a=c.`

Logic for Equality (cont)

```
1  (* Equality *)
2  Variable A : Set.
3
4  Lemma eq_refl : forall a:A, a = a.
5  Proof.
6   intro a.
7   reflexivity.
8  Qed.
9
0  Lemma eq_sym : forall a b:A, a=b -> b=a.
1  Proof.
2   intros a b H.
3   rewrite H.
4   reflexivity.
5  Qed.
6
7  Lemma eq_trans : forall a b c:A, a=b -> b=c -> a=c.
8  Proof.
9   intros a b c ab bc.
0   rewrite ab.
1   exact bc.
2  Qed.
```

Outline

1. Logic for Equality
2. **Theory of Numbers**
   - Elementary Number Theory
   - Modular Arithmetic
   - Euclidean Algorithm
   - Linear Congruences
   - Chinese Remainder Theorem
   - Applications of Number Theory
3. Method of Proofs
   - Direct, Contrapositive, Contradiction
   - Two Classical Theorems
   - Mathematical Induction

Elementary Number Theory

Number theory is a branch of **pure mathematics** devoted primarily to the study of the **integers** and **integer-valued functions**.

Elementary number theory is a subbranch of number theory that studies integers without using "calculus".

Integers

$$\ldots, -2, -1, 0, 1, 2, \ldots$$

are the "generalisation" of natural numbers:

$$0, 1, 2, \ldots$$

How do we describe them using **predicate logic**?

Elementary Number Theory (cont)

- Modern algebra approach: $(\mathbb{Z}, +, \times)$ is an **integral domain** (a **nonzero commutative ring** in which the product of any two nonzero elements is nonzero) containing a **Euclidean function**, i.e. a function f from $\mathbb{Z} \setminus \{0\}$ to the non-negative integers (called the **norm**) satisfying the following fundamental division-with-remainder property: If a and b are in $\mathbb{Z}$ and b is nonzero, then there exist q and r in $\mathbb{Z}$ such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$. Note that for $\mathbb{Z}$, $f(a) = |a|$.
- Peano Axiom + Equivalence Relation: The most popular approach.

Elementary Number Theory (cont)

Peano axioms define the arithmetical properties of natural numbers ($\{0, 1, 2, \dots\} =: \mathbb{N}$) using a constant symbol 0 and a function S: Let n, m be any natural number.

1. 0 is a natural number.
2. $S(n)$ is a natural number.
3. $m = n$ if and only if $S(m) = S(n)$.
4. $S(n) = 0$ is false. I.e. there is no number "before" 0.
5. If ϕ is a unary predicate such that:
   - $\phi(0)$ is true, and
   - for every natural number n, $\phi(n)$ being true implies that $\phi(S(n))$ is true,

   then $\phi(n)$ is true for every natural number n.

Elementary Number Theory (cont)

The first two Peano axioms are used in Coq:

```
Inductive nat : Set :=
  | O : nat
  | S : nat -> nat.
```

According to `http://www.cs.nott.ac.uk/~psztxa/g52ifr/html/Arith.html`, axioms 3 to 5 can be "proved" in Coq.

```
Definition pred (n : nat) : nat :=
  match n with
  | 0 => 0
  | S n => n
  end.
```

Elementary Number Theory (cont)

```
Lemma peano3 : forall m n:nat, S m = S n -> m = n.
intros m n H.
fold (pred (S m)). (* In Goal, m = pred (S m) *)
rewrite H.         (* rewrite pred (S m) as pred (S n) *)
unfold pred.
reflexivity.
Qed.

Lemma peano4 : forall n:nat, S n <> 0.
intro n H.
discriminate H.
Qed.

Lemma peano9 : forall P : nat -> Prop,
 P 0 -> (forall m : nat, P m -> P (S m))
     -> forall n : nat, P n.
intros P H0 HS n.
induction n.
exact H0.
apply HS.
exact IHn.
Qed.
```

Elementary Number Theory (cont)

The arithmetic operations are defined as

```
Fixpoint add n m :=
  match n with
  | 0 => m
  | S p => S (p + m)
  end
where "n + m" := (add n m) : nat_scope.

Fixpoint mul n m :=
  match n with
  | 0 => 0
  | S p => m + p * m
  end
where "n * m" := (mul n m) : nat_scope.
```

Elementary Number Theory (cont)

Proving properties of addition and multiplication for natural numbers can be complex.
An example of proof for the associativity of addition is given below.

```
Lemma plus_assoc :
 forall l m n:nat, l + (m + n) = (l + m) + n.
Proof.
 intros l m n.
 induction l.
 simpl.
 reflexivity.
 simpl.
 rewrite IHl.
 reflexivity.
Qed.
```

Elementary Number Theory (cont)

Coq already defined natural numbers and integers, we can practise with Coq to feel how the theory of natural numbers is applied:

- Check S(S(S(0))).
- Check Nat.add 123 456.

Note that Nat.add 123 123456 won't work because 123456 'S' would cause Coq system to crash.

So mathematical definition above is good for mathematical proving but not computer calculation.

Outline

1. **Logic for Equality**
2. **Theory of Numbers**
   - Elementary Number Theory
   - Modular Arithmetic
   - Euclidean Algorithm
   - Linear Congruences
   - Chinese Remainder Theorem
   - Applications of Number Theory
3. **Method of Proofs**
   - Direct, Contrapositive, Contradiction
   - Two Classical Theorems
   - Mathematical Induction

Elementary Number Theory

After the definition of addition and multiplication in natural numbers, the next thing is to generalised them to integers. The mathematics is complicated, in software, it is possible to introduce $-n$ and define $-0 = 0$.

Divisibility is the "inverse" operation for integer "multiplication". The interesting results associated with divisibility is what made number theory attractive.

Elementary Number Theory

Definition 3.2.1

If n and $d \neq 0$ are integers, then n *is divisible by* d if there is an integer k such that $n = dk$. In this case, n is called the *multiple of* d. d is called the *factor* or *divisor* of n. We also say that d *divides* n and denote it by $d|n$. If d does not divide n, we denote it as $d \nmid n$.

Example: $n = 5$, $d = 3$, 5 is **not divisible** by 3 because there is **no integer** k such that $5 = 3k$.

Example: $n = 6$, $d = 3$, 6 is **divisible** by 3 because there is **an integer** $k = 2$ such that $6 = 3k$.

Elementary Number Theory (cont)

Based on our definition, *divisors are assumed to be nonzero*. If d is a divisor of n, then n is also divisible by $-d$ (indeed, $n = dk$ implies that $n = (-d)(-k)$), so that the divisors of an integer always occur in pairs. To find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers. For this reason, we shall usually limit ourselves to a consideration of positive divisors.

Elementary Number Theory (cont)

Example 3.2.3:

1. If a and b are integers, is $4a + 4b$ divisible by 2?
2. Does 4 divides 18?
3. Is 32 a multiple of -16?
4. Is -9 a factor of 54?
5. Suppose a and b are positive integers and $a|b$. Is $a \leq b$?

Class Discussion.

Elementary Number Theory (cont)

The divisibility of integers is defined in Coq's Coq.ZArith.ZArith library.

```
1  Require Import Coq.ZArith.ZArith.
2  Require Import Coq.ZArith.Znumtheory.
3
4  Example exmp1: (3 | 6)%Z.
5   apply (Zdivide_intro 3 6 2).
6   reflexivity.
7  Qed.
8
9  Open Scope Z_scope.
0
1  Example eg_3_2_3a: forall a b : Z, (2 | 4*a + 4*b).
2   intros.
3   apply (Zdivide_intro _ _ (2*a+2*b)).
4   ring. (* solves equations *)
5  Qed.
```

Elementary Number Theory (cont)

However, proving using computer is very difficult due to the "constructive" nature, e.g. $3 \nmid 5$ cannot be "proved" in Coq without using modulo.

Elementary Number Theory (cont)

Theorem 3.2.4 (Properties of Divisibility): For integers a, b, c, the following hold:

(a) $a|0$, $1|a$, $a|a$.

(b) $a|1$ iff $a = \pm 1$.

(c) If $a|b$ and $c|d$, then $ac|bd$.

(d) If $a|b$ and $b|c$, then $a|c$. (Transitivity of Divisibility)

(e) $a|b$ and $b|a$ iff $a = \pm b$.

(f) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

(g) If $a|b$ and $a|c$, then $a|(bx + cy)$ for arbitrary integers x and y.

Discuss some Proving Techniques in class.

Elementary Number Theory (cont)

Definition of Prime and Composite

A **prime (number)** is a natural number greater than 1 that is not a product of two smaller natural numbers. A natural number greater than 1 that is not prime is called a **composite number**.

Example: 0 and 1 are **not** prime numbers.

Example: 5 is prime because the only ways of writing it as a product of natural number is 1×5 or 5×1, involve 5 itself.

Example: 4 is composite because it is a product of two smaller numbers: 2×2.

Elementary Number Theory (cont)

Theorem 3.2.6 (Divisibility by a Prime): Any integer $n > 1$ is divisible by a prime number.

Proof

$n = 2$ is divisible by the prime number 2.
Let $n > 2$, and suppose the result is true for all positive integers $1 < k < n$. We want to show that n is divisible by a prime number.
If n is prime, then n is divisible by a prime number n.
If n is not prime, then it is composite. Therefore, n has a positive divisor m such that $m \neq 1$ and $m \neq n$. Plainly, m can't be larger than n, so $1 < m < n$. By induction, m is divisible by some prime number p. Now, $p|m$ and $m|n$, so $p|n$. This proves that n is divisible by a prime number, and completes the induction step.
Hence, then result is true for all integers greater than 1 by strong induction (Slide 167).

Elementary Number Theory (cont)

Definition 3.2.8: Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is that integer d with the following properties:

1. d is a common divisor of both a and b, i.e. $d|a$ and $d|b$.
2. For all integers c, if $c|a$ and $c|b$, then $c \leq d$.

Elementary Number Theory (cont)

Example 3.2.9: The positive divisors of -12 are 1, 2, 3, 4, 6, 12, whereas those of 30 are 1, 2, 3, 5, 6, 10, 15, 30; hence,

- the positive common divisors of -12 and 30 are 1, 2, 3, 6.
- Because 6 is the largest of these integers, it follows that $\gcd(-12, 30) = 6$.

Similarly, $\gcd(-5, 5) = 5$, $\gcd(8, 17) = 1$, $\gcd(-8, -36) = 4$.

Note that $\gcd(-12, 30) = 6 = (-12)2 + 30 \cdot 1$, $\gcd(-8, -36) = 4 = (-8)4 + (-36)(-1)$.

Elementary Number Theory (cont)

The following theorem indicates that $\gcd(a, b)$ can be represented as a linear combination of a and b.

Theorem 3.2.10

Given integers a and b, not both of which are zero, there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

Corollary 3.2.12

If a and b are given integers, not both zero, then the set $T = \{ax + by | x \in \mathbb{Z} \wedge y \in \mathbb{Z}\}$ is precisely the set of all multiples of $d = \gcd(a, b)$.

Elementary Number Theory (cont)

Definition 3.2.13

Integers a and b, not both of which are zero, are called *relatively prime* if $\gcd(a, b) = 1$. Integers $a_1, a_2, a_3, \cdots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ for all integers i and j with $1 \leq i, j \leq n$, and $i \neq j$.

Theorem 3.2.14

Let a and b be integers, not both zero. Then a and b are relatively prime iff there exist integers x and y such that $1 = ax + by$.

Elementary Number Theory (cont)

Corollary 3.2.16: If $a|c$ and $b|c$, with $\gcd(a, b) = 1$, then $ab|c$.

Proof (Direct Proof)

Inasmuch as $a|c$ and $b|c$, integers r and s can be found such that $c = ar = bs$. Now the relation $\gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y. Multiplying the last equation by c, it appears that

$$c = c \cdot 1 = c(ax + by) = acx + bcy.$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

or, as a divisibility statement, $ab|c$.

Elementary Number Theory (cont)

Theorem 3.2.17 (Euclid's Lemma) If $a|bc$, with $\gcd(a, b) = 1$, then $a|c$.

Proof

Since $\gcd(a, b) = 1$, there are some x and y such that $1 = ax + by$.
Multiplication of this equation by c produces

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Because $a|ac$ and $a|bc$, it follows that $a|(acx + bcy)$, which can be recast as $a|c$.

If a and b are not relatively prime, then the conclusion of Euclid's lemma may fail to hold. E.g. $12|9 \cdot 8$, but $12 \nmid 9$ and $12 \nmid 8$.

Elementary Number Theory (cont)

Theorem 3.2.18: Let a, b be integers, not both zero. For a positive integer d, $d = \gcd(a, b)$ iff

(a) $d|a$ and $d|b$.

(b) Whenever $c|a$ and $c|b$, then $c|d$.

Proof

$\Rightarrow$: Suppose that $d = \gcd(a, b)$. Certainly, $d|a$ and $d|b$, so that (a) holds. In light of Theorem 3.2.10 (Slide 27), d is expressible as $d = ax + by$ for some integers x, y. Thus, if $c|a$ and $c|b$, then $c|(ax + by)$, or rather $c|d$. In short, condition (b) holds.

$\Leftarrow$: Let d be any positive integer satisfying the stated conditions. Given any common divisor c of a and b, we have $c|d$ from hypothesis (b). The implication is that $d \geq c$, and consequently d is the greatest common divisor of a and b.

Elementary Number Theory (cont)

Theorem 3.2.1: If p is a prime and $a, b \in \mathbb{Z}$ such that $p|ab$, then $p|a$ or $p|b$.

Proof

Assume $p \nmid a$. Then $\gcd(a, p) = 1$. By Euclid's Lemma, $p|b$.

Unique Factorisation Theorem for the Integers

Given any integer $n > 1$, there is a positive integer k, distinct prime numbers $p_1, p_2, \cdots, p_k$, and there are positive integers e_1, e_2, $\cdots$, e_k such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

and any other expression of n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Elementary Number Theory (cont)

Definition 3.2.21

Given any integer $n > 1$, the *standard factored form* of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}, \quad p_1 < p_2 < \cdots < p_k,$$

where k is a positive integer; $p_1, p_2, \cdots, p_k$ are prime numbers; $e_1, e_2, \cdots, e_k$ are positive integers.

Example 3.2.23: Write 3300 in standard factored form.

Solution

$3300 = 100 \cdot 33 = 4 \cdot 25 \cdot 3 \cdot 11 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11 = 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1$

Elementary Number Theory (cont)

Quotient-Remainder (QR) Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = qd + r, \quad 0 \leq r < d.$$

Definition 3.2.25: With the notation of in the QR Theorem, r is called the ***modulo*** of the division of n by d. If $r = 0$, we say that n is a ***multiple*** of d, or that n is *divisible by* d, or d is a *divisor of* n, or that d *divides* n, or that d is a ***factor*** *of* n. The number q is called the ***quotient*** of n by d and is denoted n div d.
We can also define the operator mod: $n \mod d = r$.

Elementary Number Theory (cont)

In computer, it is convenient to transform the problems of divisibility from the set of integers $\mathbb{Z}$ to the set of real numbers $\mathbb{R}$. The two operations, floor and ceiling, that relates $\mathbb{Z}$ and $\mathbb{R}$ are defined below.

Definition 3.2.28

Given any real number x, the *floor* and *ceiling* of x, denoted $\lfloor x \rfloor$ and $\lceil x \rceil$, are defined respectively as follows:

$$\lfloor x \rfloor := \text{the unique integer } n \text{ such that } n \leq x < n + 1;$$
$$\lceil x \rceil := \text{the unique integer } n \text{ such that } n - 1 < x \leq n.$$

Elementary Number Theory (cont)

Example 3.2.30: Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the following values of x.

1. 25/4
2. 0.999
3. $0.999\cdots$
4. -2.01
5. $\lfloor -\frac{1}{2} \rfloor + \lfloor \frac{2}{3} \rfloor$.

Elementary Number Theory (cont)

Theorem 3.2.34

$\forall x \in \mathbb{R}, \forall m \in \mathbb{Z}, \lfloor x + m \rfloor = \lfloor x \rfloor + m.$

Exercise 3.2.32: If k is an integer, simplify $\lfloor k \rfloor$ and $\lfloor k + \frac{1}{2} \rfloor$ as an expression of k.

Exercise 3.2.33: Is the statement "for all real numbers x and y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$" true or false?

Theorem 3.2.35

For any integer n,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even,} \\ \frac{n-1}{2}, & \text{if } n \text{ is odd.} \end{cases}$$

Elementary Number Theory (cont)

Example 3.2.26: For each values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

1. $n = 54, d = 4 \rightarrow r = 2$
2. $n = 54, d = -4 \rightarrow r = 2$
3. $n = -54, d = -4 \rightarrow r = 2$
4. $n = -54, d = 70 \rightarrow r = 16$

The r follows Raymond T. Boute's definition:

$$r = n - |d| \left\lfloor \frac{n}{|d|} \right\rfloor.$$

Example 3.2.27:

1. Compute 32 div 9 and 32 mod 9?
2. What day of the week will it be 1 year from today?

Elementary Number Theory (cont)

Example 3.2.26 in Racket

1. (modulo 54 4) $\rightarrow$ 2; (remainder 54 4) $\rightarrow$ 2
2. (modulo 54 -4) $\rightarrow$ -2; (remainder 54 -4) $\rightarrow$ 2
3. (modulo -54 -4) $\rightarrow$ -2; (remainder -54 -4) $\rightarrow$ -2
4. (modulo -54 70) $\rightarrow$ 16; (remainder -54 70) $\rightarrow$ -54

Elementary Number Theory (cont)

You can find out what is going on by referring to `https://en.wikipedia.org/wiki/Modulo_operation`:

- modulo follows Donald Knuth's definition to be

$$r = n - \left\lfloor \frac{n}{d} \right\rfloor d$$

E.g. $r = -54 - \lfloor -54/70 \rfloor \times 70 = -54 - (-70) = 16$

- remainder is defined to be

$$r = n - truncate(\frac{n}{d})d$$

E.g.
$r = -54 - truncate(-54/70)70 = -54 - 0 = -54$

Elementary Number Theory (cont)

Consider the integer $d = 2$ in the Quotient-Remainder Theorem, the modulo r will either be 0 or 1. This leads to the notions of even and odd.

Definition of Even

An integer n is **even** if it is divisible by two, i.e. $n \bmod 2 = 0$ or $n = 2k$ for some integer k.
The sets of even numbers is usually denoted as $2\mathbb{Z} := \{2k : k \in \mathbb{Z}\}$.

Definition of Odd

An integer n is **odd** if it is not divisible by two, i.e. $n \bmod 2 = 1$ or $n = 2k + 1$ for some integer k.

Elementary Number Theory

The definition of even and odd are defined in Coq's BinInt module.

```
1 Definition Even a := exists b, a = 2*b.
2 Definition Odd a := exists b, a = 2*b+1.
```

I only know how to prove the simplest example.

```
1  Require Import BinInt.
2  Open Scope Z_scope.
3  Example eg1: Z.Even 4.
4  exists 2; simpl; reflexivity.
5  Qed.
6  Example eg2: forall n : Z, Z.Even (4*n).
7  intro n.
8  exists (2*n).
9  simpl.   (* Integer n can be =0, >0, <0 *)
0  destruct n.
1  reflexivity. reflexivity. reflexivity.
2  Qed.
```

Outline

Modular Arithmetic (cont)

We now further the study of modular arithmetic using the notion of congruence, which is an equivalence relation over $\mathbb{Z}$.

Definition 3.5.1

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. We say a and b are *congruent modulo n* provided that $n|(a-b)$. We write $a \equiv b \pmod{n}$ or $a \equiv_n b$ which means $a - b = kn$ for some integer k.
When $n \nmid (a-b)$, we say that a is *incongruent to b modulo n*, and in this case we write $a \not\equiv b \pmod{n}$.

Remark: Note that $\equiv$ for number theory is different from the logical equivalence found in mathematical logic.

Modular Arithmetic (cont)

Example 3.5.3

For $n = 7$,
$3 \equiv 24 \pmod 7$, $-31 \equiv 11 \pmod 7$, $-15 \equiv -64 \pmod 7$ because $3 - 24 = (-3)7$, $-31 - 11 = (-6)7$, and $-15 - (-64) = 7 \cdot 7$.
$25 \not\equiv 12 \pmod 7$, because 7 fails to divide $25 - 12 = 13$.

Exercise 3.5.4:

1. Is $12 \equiv 7 \pmod 5$?
2. Is $-6 \equiv -8 \pmod 4$?
3. Is $0 \equiv -6 \pmod 3$?

Class Discussion.

Modular Arithmetic (cont)

Theorem 3.5.5

Let a, b, and $n > 1$ be any integers. The following statements are all equivalent:

1. $n|(a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (nonnegative) remainder when divided by n
5. $a \mod n = b \mod n$

Modular Arithmetic (cont)

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$a = qn + r, \quad 0 \leq r < n.$$

Then, by definition of congruence, $a \equiv r \pmod{n}$. Because there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, ..., n - 1$; in particular, $a \equiv 0 \pmod{n}$ iff $n|a$. The set of n integers

$$0, 1, 2, ..., n - 1$$

is called the set of *least nonnegative residues modulo* n.

Modular Arithmetic (cont)

Basic Arithmetic Theorem of Congruences

Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod{n}$.

(b) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

(e) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.

(f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Discuss Some Proofs.

Modular Arithmetic (cont)

Corollary 3.5.12

The congruence relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$ and the map

$$\{0, 1, \cdots, n-1\} \to \mathbb{Z}/\equiv_n, \quad r \mapsto \bar{r} = r + n\mathbb{Z}$$

is a bijection.

A special case of this Corollary is the Example 3.3.29 which will be discussed in the next topic (Relation).
In mathematics, $\mathbb{Z}/\equiv_n$ is denoted $\mathbb{Z}/n\mathbb{Z}$.

Modular Arithmetic (cont)

Proof of the Corollary: From the Basic Arithmetic Theorem (a), (b) and (c), we know that $\equiv_n$ is reflexive, symmetric and transitive. Therefore $\equiv_n$ is an equivalence relation.
The map is well-defined since for every $r = 0, 1, \cdots, n-1$, there is a set $r + n\mathbb{Z}$ corresponding to it.
To show that it is bijection, we show that it is an injection: assume $\bar{r} = \bar{s}$ with $0 \leq r, s < n$. Then, by definition, $r \equiv s \pmod{n}$, so $n|r - s$ and $|r - s| < n$, therefore $r = s$.
To show that the map is a surjection: Let $\bar{a} \in \mathbb{Z}/\equiv_n$, by definition, $\bar{a} = \{a + nk : k \in \mathbb{Z}\}$, by Quotient-Remainder Theorem, there is an $r \in \{0, 1, \cdots, n-1\}$ such that $a = r + nm$, hence $r \equiv_n a$ and by definition, $\bar{r} = \bar{a}$.

Modular Arithmetic (cont)

Example 3.5.14: Calculate $144^4 \mod 713$
Solution: Instead of writing like the left, writing like the right is much nicer.

$$
\begin{aligned}
& 144^4 \mod 713 \\
&= (144^2)^2 \mod 713 \\
&= [144^2 \mod 713]^2 \mod 713 \\
&= [20736 \mod 713]^2 \mod 713 \\
&= [59]^2 \mod 713 \\
&= 3481 \mod 713 = 629
\end{aligned}
$$

$$
\begin{aligned}
144^4 &= (20736)^2 \\
&\equiv_{713} (59)^2 \\
&= 3481 \\
&\equiv_{713} 629
\end{aligned}
$$

Modular Arithmetic (cont)

Example 3.5.15: Calculate $12^{43} \mod 713$.

Example 3.5.16: Show that 41 divides $2^{20} - 1$.

Example 3.5.17: Find the remainder obtained upon dividing the sum below by 12:

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

Class Discussion.

Modular Arithmetic (cont)

When we have a number to the power of the power of some number, we need the following theorem to simplify the calculation.

Fermat's Little Theorem

If p is any prime number and a is any integer, then $a^p \equiv a \pmod{p}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Modular Arithmetic (cont)

Example 3.5.20: Calculate $7^{11^{13}} \mod 17$

Solution

Since 17 is a prime number, we know that

$$7^{16} \equiv 1 \pmod{17}$$

What we need to calculate is

$$11^{13} = 11^{8+4+1} = 11^8 \cdot 11^4 \cdot 11 \equiv 9^4 \cdot 9^2 \cdot 11 = 11 \pmod{16}$$

where $11^2 \equiv 9 \pmod{16}$ and $9^2 \equiv 1$.
Therefore $11^{13} = 16k + 11$ for some integer k and

$$7^{11^{13}} = 7^{16k+11} = (7^{16})^k \cdot 7^{11} \equiv 1^k \cdot 7^{11} = 1977326743 \equiv 14 \pmod{17}.$$

Using Racket (modulo (expt 7 (expt 11 13)) 17) will take forever.

Outline

Euclidean Algorithm

In mathematics, the *Euclidean algorithm* (also called *Euclid's algorithm*) is an efficient method for computing the **greatest common divisor** of two integers. It is named after the Greek mathematician Euclid, who described it in Books VII and X of his Elements.

Euclidean Algorithm (cont)

The algorithm has many theoretical and practical applications:

- A key element of a public-key encryption method called “RSA algorithm”
- Use to solve Diophantine equations, such as finding numbers that satisfy multiple congruences (Chinese remainder theorem) or multiplicative inverses of a finite field.
- Use in the construction of continued fractions, in the Sturm chain method for finding real roots of a polynomial, and in several modern integer factorisation algorithms.
- A basic tool for proving theorems in modern number theory, such as Lagrange’s four-square theorem and the fundamental theorem of arithmetic (unique factorisation).

Euclidean Algorithm (cont)

The Euclidean algorithm is based on the following two lemmas.

Lemma 3.5.21

If r is a positive integer, then $\gcd(r, 0) = r$.

Lemma 3.5.22

If a and b are any integers with $b \neq 0$ and q and r are nonnegative integers such that $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Euclidean Algorithm (cont)

Theorem 3.5.23: Euclidean Algorithm

1. Let $A > B \geq 0$.
2. If $B = 0$ then $\gcd(A, B) = A$.
   Else divide A by B to obtain a quotient q and a remainder r as follows:

   $$A = Bq + r, \quad \text{where } 0 \leq r < B$$

   Thus, $\gcd(A, B) = \gcd(B, r)$.
3. Repeat step 2., but use B instead of A and r instead of B. The repetitions are guaranteed to terminate eventually with $r = 0$.

Euclidean Algorithm (cont)

Example 3.5.24: Use the Euclidean algorithm to find $\gcd(330, 156)$.

Solution

$$\begin{aligned}
\gcd(330, 156) &= \gcd(156, 18) && [330 = 156(2) + 18] \\
&= \gcd(18, 12) && [156 = 18(8) + 12] \\
&= \gcd(12, 6) && [18 = 12(1) + 6] \\
&= \gcd(6, 0) && [12 = 6(2) + 0] \\
&= 6
\end{aligned}$$

Racket Check: (gcd 336 156)

Euclidean Algorithm (cont)

Exercise: Use the Euclidean algorithm to find $\gcd(155, -275)$

Racket: (gcd 155, –275) $\rightarrow$ 5

Euclidean Algorithm (cont)

Definition 3.5.25

An integer d is said to be a *linear combination of integers a and b* if there exist integers s and t such that $as + bt = d$.

Theorem 3.5.26

For all integers a and b, not both zero, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Euclidean Algorithm (cont)

Example 3.5.27: Express $\gcd(330, 156)$ as a linear combination of 330 and 156.

Solution

From Example 3.5.24 (Slide 60),

$$\begin{aligned}
6 &= 18 - 12 = 18 - [156 - 8(18)] \\
&= 18 + (-1)(156) + 8(18) \\
&= 9(18) + (-1)(156) \\
&= 9[330 - 2(156)] + (-1)(156) \\
&= 9(330) + (-18)(156) + (-1)(156) \\
&= 9(330) + (-19)(156)
\end{aligned}$$

Hence $\gcd(330, 156) = 9(330) + (-19)(156)$.

Euclidean Algorithm (cont)

Example 3.5.28: Show that 660 and 43 are relatively prime, and find a linear combination of 660 and 43 that equals 1.

Solution

$$
\begin{aligned}
&\gcd(660, 43) \\
&= \gcd(43, 15) && [660 = 43(15) + 15 \Rightarrow 15 = 660 - 43(15)] \\
&= \gcd(15, 13) && [43 = 15(2) + 13 \Rightarrow 13 = 43 - 15(2)] \\
&= \gcd(13, 2) && [15 = 13(1) + 2 \Rightarrow 2 = 15 - 13] \\
&= \gcd(2, 1) && [13 = 2(6) + 1 \Rightarrow 1 = 13 - 2(6)] \\
&= \gcd(1, 0) && [2 = 1(2) + 0] \\
&= 1
\end{aligned}
$$

hence 660 and 43 are relatively prime.

Euclidean Algorithm (cont)

Solution of Example 3.5.28 (cont)

An expression of 1 as a linear combination of 660 and 43 is

$$\begin{aligned}
1 &= 13 - 2(6) \\
&= 13 - [15 - 13](6) \\
&= 7(13) - 6(15) \\
&= 7[43 - 15(2)] - 6(15) \\
&= 7(43) - 20(15) \\
&= 7(43) - 20[660 - 43(15)] \\
&= (-20)(660) + 307(43)
\end{aligned}$$

Euclidean Algorithm (cont)

Theorem 3.5.29

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof

$$ca \equiv cb \pmod{n} \Rightarrow \exists k(c(a-b) = ca - cb = kn)$$

Knowing that $\gcd(c, n) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$. When these values are substituted in the displayed equation and the common factor d cancels

$$r(a-b) = ks.$$

Hence, $s|r(a-b)$ and $\gcd(r, s) = 1$. Euclid's lemma yields $s|a-b$, which may be recast as $a \equiv b \pmod{s}$ or $a \equiv b \pmod{n/d}$.

Euclidean Algorithm (cont)

Theorem 3.5.29 gets its maximum force when the requirement that $\gcd(c, n) = 1$ is added, for then the cancellation may be accomplished without a change in modulus.

Corollary 3.5.30

If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Corollary 3.5.31

If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is prime, then $a \equiv b \pmod{p}$.

Euclidean Algorithm (cont)

Example 3.5.32:

$$33 \equiv 15 \pmod 9 \Rightarrow 3 \cdot 11 \equiv 3 \cdot 5 \pmod 9$$
$$\Rightarrow 11 \equiv 5 \pmod 3$$

since $\gcd(3, 9) = 3$ and Theorem 3.5.29 (Slide 66)

$$-35 \equiv 45 \pmod 8 \Rightarrow 5 \cdot (-7) = 5 \cdot 9 \pmod 8$$
$$\Rightarrow -7 = 9 \pmod 8$$

since $\gcd(5, 8) = 1$.

Euclidean Algorithm (cont)

Corollary 3.5.33

For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integers s such that $as \equiv 1 \pmod{n}$. The integer s is called the *inverse of a modulo n*.

Example 3.5.34: Find an inverse for 43 modulo 660. That is, find an integer s such that $43s \equiv 1 \pmod{660}$.

Solution

From Example 3.5.28,

$$307(43) + (-20)(660) = 1 \Rightarrow 307(43) = 1 + 20(660)$$
$$\Rightarrow 307(43) \equiv 1 \pmod{660}$$

So 307 is an inverse for 43 modulo 660.

Euclidean Algorithm (cont)

Example: Find a positive inverse for 3 modulo 40. That is, find a positive integer s such that $3s \equiv 1 \pmod{40}$.

Answer: $s = 27$

Class Discussion.

Outline

Linear Congruences

Can we solve equations associated with "modular arithmetic"?
The simple equation is the *linear congruence equation*:

$$ax \equiv b \pmod{n}.$$

By a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b \pmod{n}$.

Linear Congruences

By definition,

$$ax_0 \equiv b \pmod{n} \Leftrightarrow n|(ax_0 - b) \Leftrightarrow \exists y_0(ax_0 - b = ny_0).$$

Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b \pmod{n}$ is identical with that of obtaining all solutions of the linear Diophantine equation

$$ax - ny = b.$$

Linear Congruences (cont)

Note that any "two" solutions are regarded "equivalent". E.g. $x = 3$ and $x = -9$ both satisfy the congruence $3x \equiv 9 \pmod{12}$; because $3 \equiv -9 \pmod{12}$, they are not counted as different solutions.

Hence, when we refer to the number of solutions of $ax \equiv b \pmod{n}$, we mean the number of incongruent integers satisfying this congruence.

Theorem 3.5.35

The linear congruence $ax \equiv b \pmod{n}$ has a solution iff $d|b$, where $d = \gcd(a, n)$. If $d|b$, then it has d "different" solutions modulo n (called incongruent).

Linear Congruences (cont)

Proof

Note that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. It can be solved iff $d|b$; moreover, if it is solvable and x_0, y_0 is a specific solution, then any other solution has the form

$$x = x_0 + \frac{n}{d}t, \quad y = y_0 + \frac{a}{d}t$$

for some choice of t.

Linear Congruences (cont)

Proof (cont)

Among the various integers satisfying the first of these formulae, consider those that occur when t takes on the successive values $t = 0, 1, 2, ..., d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \cdots, x_0 + \frac{(d-1)n}{d}.$$

We claim that these integers are incongruent modulo n, and all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}, \quad 0 \leq t_1 < t_2 \leq d - 1.$$

Linear Congruences (cont)

Proof (cont)

Then we would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$$

Now $\gcd(n/d, n) = n/d$, by Theorem 3.5.29 (Slide 66) the factor n/d could be cancelled leading to

$$t_1 \equiv t_2 \pmod{d}$$

which is to say that $d|t_2 - t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

Linear Congruences (cont)

Proof (cont)

It remains to argue that any other solution $x_0 + (n/d)t$ is congruent modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d - 1$. Hence

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r \pmod{n}$$

with $x_0 + (n/d)r$ being one of our d selected solutions.

Linear Congruences (cont)

The proof of Theorem 3.5.35 points that: If x_0 is any solution of $ax \equiv b \pmod{n}$, then the $d = \gcd(a, n)$ incongruent solutions are given by

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \cdots, x_0 + (n-1)\frac{n}{d}.$$

Linear Congruences (cont)

Corollary 3.5.36

If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution modulo n.

Given relatively prime integers a and n, the congruence $ax \equiv 1 \pmod{n}$ has a unique solution. This solution is called the *(multiplicative) inverse of a modulo n*.

Linear Congruences (cont)

Example 3.5.37: Solve the linear congruence $18x \equiv 30 \pmod{42}$.

Solution

Because $\gcd(18, 42) = 6$ and 6 surely divides 30, Theorem 3.5.35 (Slide 74) guarantees the existence of exactly six solutions, which are incongruent modulo 42. By inspection, one solution is found to be $x = 4$.
The six solutions are as follows:

$$x \equiv 4 + (42/6)t = 4 + 7t \pmod{42}, \quad t = 0, 1, ..., 5$$

or, plainly enumerated,

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Linear Congruences (cont)

Example 3.5.38: Solve the linear congruence $9x \equiv 21 \pmod{30}$.

Answer: $x = 9, 19, 29 \pmod{30}$

Class Discussion.

Outline

Chinese Remainder Theorem

Having considered a single linear congruence, it is natural to turn to the problem of solving a *system of simultaneous linear congruences*:

$$\begin{aligned} c_1 x &\equiv b_1 \pmod{m_1}, \\ c_2 x &\equiv b_2 \pmod{m_2}, \\ &\cdots, \\ c_r x &\equiv b_r \pmod{m_r}. \end{aligned}$$

Chinese Remainder Theorem (cont)

Assume that the moduli m_k are relatively prime in pairs. The system will has a solution if each individual congruence is solvable, i.e. $d_k | b_k$ for each k, where $d_k = \gcd(c_k, m_k)$. When these conditions are satisfied, the factor d_k can be cancelled in the kth congruence to produce a new system having the same set of solutions as the original one:

$$\begin{aligned} c_1' x &\equiv b_1' \pmod{n_1}, \\ c_2' x &\equiv b_2' \pmod{n_2}, \\ &\cdots, \\ c_r' x &\equiv b_r' \pmod{n_r} \end{aligned}$$

where $n_k = m_k / d_k$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$; in addition, $\gcd(c_i', n_i) = 1$.

Chinese Remainder Theorem (cont)

The solutions of the individual congruences assume the form

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned} \tag{1}$$

Thus, the problem is reduced to one of finding a simultaneous solution of a system of congruences of this simpler type.

3.5.39: Chinese Remainder Theorem

Suppose $n_1, n_2, \cdots, n_r$ are pairwise relatively prime positive integers and $a_1, a_2, \cdots, a_r$ are any integers. The system of congruences (1) have a simultaneous solution that is unique modulo n, where $n = n_1 n_2 \cdots n_r$. When $r = 3$, let $N_1 = n_2 n_3$, $N_2 = n_1 n_3$, $N_3 = n_1 n_2$, then $\gcd(N_i, n_i) = 1$ for $i = 1, 2, 3$. There exists an integer y_i, an inverse of N_i modulo n_i such that $N_i y_i \equiv 1 \pmod{n_i}$. The solution to (1) is

$$x \equiv a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 \pmod{n}$$

where $n = n_1 n_2 n_3$.

Refer to UECM2383 for the proof.

Chinese Remainder Theorem (cont)

Example 3.5.40: In the first century, the Chinese mathematician Sūn Zi asked the following question in the book "Sūn Zǐ Suàn Jīn": There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

Solution

This puzzle can be translated into the following question: What are the solutions of the systems of congruences

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Chinese Remainder Theorem (cont)

Solution of Example 3.5.40 (cont)

Let $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, $a_1 = 2$, $a_2 = 3$, $a_3 = 2$.
Then $N_1 = n_2 n_3 = (5)(7) = 35$,
$N_2 = n_1 n_3 = (3)(7) = 21$, $N_3 = n_1 n_2 = (3)(5) = 15$
and

$$\gcd(35, 3) = 1 \Rightarrow 35 = 3(11) + 2 \Rightarrow 2 = 35 - 3(11)$$

$$3 = 2(1) + 1 \Rightarrow 1 = 3 - 2 = \cdots = 12(3) + (-1)(35)$$

Hence $(-1)(35) \equiv 1 \pmod 3$, -1 is an inverse for 35 modulo 3 and 2 is a positive integer that is an inverse for 35 modulo 3.

Chinese Remainder Theorem (cont)

Solution of Example 3.5.40 (cont)

Similarly, the inverse for 21 modulo 5 is found to be 1 and the inverse for 15 modulo 7 is found to be 1. Thus $y_1 = 2$, $y_2 = 1$, $y_3 = 1$. The solution to this system are those x such that

$$\begin{aligned} x &= a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 \\ &= (2)(35)(2) + (3)(21)(1) + (2)(15)(1) = 233 \equiv 23 \pmod{105} \end{aligned}$$

It follows that 23 is the smallest positive integer that is a simultaneous solution. We conclude that 23 is the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

Chinese Remainder Theorem (cont)

Example 3.5.41: Solve the linear congruence

$$17x \equiv 9 \pmod{276}.$$

Solution

Because $276 = 3 \cdot 4 \cdot 23$, this is equivalent to finding a solution for the system of congruences

$$\begin{cases} 17x \equiv 9 \pmod{3} \\ 17x \equiv 9 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 10 \pmod{23} \end{cases}$$

Chinese Remainder Theorem (cont)

Solution of Example 3.5.41 (cont)

Note that if $x \equiv 0 \pmod 3$, then $x = 3k$ for any integer k. We substitute into the second congruence of the system and obtain

$$3k \equiv 1 \pmod 4$$

Multiplication of both sides of this congruence by 3 gives us

$$k \equiv 9k \equiv 3 \pmod 4$$

so that $k = 3 + 4j$, where j is an integer. Then

$$x = 3(3 + 4j) = 9 + 12j.$$

Chinese Remainder Theorem (cont)

Solution of Example 3.5.41 (cont)

For x to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}$$

or $204j \equiv -144 \pmod{23}$, which reduces to $3j \equiv 6 \pmod{23}$; in consequence, $j \equiv 2 \pmod{23}$. This yields $j = 2 + 23t$, with t an integer, whence

$$x = 9 + 12(2 + 23t) = 33 + 276t.$$

All in all, $x \equiv 33 \pmod{276}$ provides a solution to the system of congruences and, in turn, a solution to $17x \equiv 9 \pmod{276}$.

Outline

Applications

Modular arithmetic has applications in

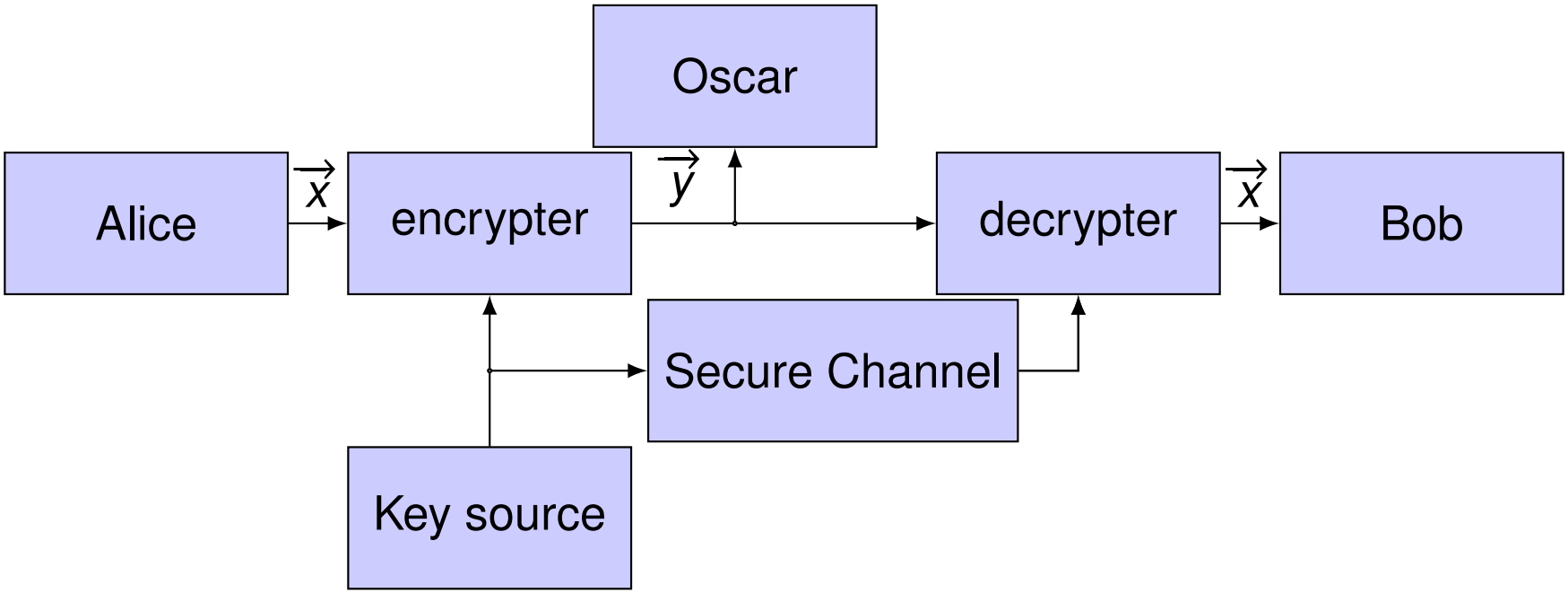
- UECM2383 Elementary Number Theory → UECM3383 Cryptology → Computer Security for various business transactions.
- Random Number Generation: SSIF → Operations Research → Stochastic Process in Finance and Engineering
- UECM3373 Coding Theory (geometry of numbers) → check digit to identification numbers, in order to recognize transmission errors or forgeries.
- Computer Graphics: Computational Geometry (solving systems of polynomials) → computational algebraic numbers.

Applications (cont)

Cryptography is the study of methods for sending secret messages. It involves *encryption*, in which a message, called *plaintext*, is converted into a form, called *ciphertext*, that may be sent over channels possibly open to view by outside parties. The receiver of the ciphertext uses *decryption* to convert the ciphertext back into plaintext.

Applications (cont)

Pictorially, we have



Applications (cont)

Definition 3.6.1: A *cryptosystem* is a tuple $(\mathscr{P}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$ where

1. $\mathscr{P}$ is a finite set of possible plaintexts;
2. $\mathscr{C}$ is a finite set of possible ciphertexts;
3. $\mathscr{K}$ is a set of possible keys called the *keyspace*;
4. For each $k \in \mathscr{K}$, there is an encryption rule and a decryption rule respectively as follows:

$$e_K : \mathscr{P} \to \mathscr{C}, \quad d_K : \mathscr{C} \to \mathscr{P}$$

such that $d_K(e_K(x)) = x$ for every $x \in \mathscr{P}$. The set of e_K is denoted $\mathscr{E}$ and the set of d_K is denoted $\mathscr{D}$.

Remark: When $\mathscr{P} = \mathscr{C}$, then each encryption function is in fact a permutation.

Applications (cont)

We will investigate three *classical (or private-key, symmetric-key) cryptosystem* and one public-key cryptosystem, the RSA cryptosystem. For simplicity, we will just investigate Latin characters A to Z ignoring the difference between capital and small letters. We assume each letter of the alphabet is coded by its position relative to the others as follows:

$$\mathtt{A}=0,\ \mathtt{B}=1,\ \mathtt{C}=2,\ \mathtt{D}=3,\ \cdots,\ \mathtt{X}=23,\ \mathtt{Y}=24,\ \mathtt{Z}=25.$$

Applications (cont)

Definition 3.6.3: Shift Cipher

Let $\mathscr{P} = \mathscr{C} = \mathscr{K} = \mathbb{Z}_{26}$. For $0 \leq k \leq 25$, define

$$e_k(x) = (x + k) \mod 26, \quad d_k(y) = (y - k) \mod 26$$

for every x, y in $\mathbb{Z}_{26}$. Then $(\mathscr{P}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$ is called a *shift cipher*.

Applications (cont)

An encryption system once used by Julius Caesar, and now called the Caesar cipher, encrypts messages by changing each letter of the alphabet to the one three places farther along, with X wrapping around to A, Y to B, and Z to C.

If the numerical version of the plaintext for a letter is denoted M and the numeric version of the ciphertext is denoted C, then

$$C = (M + 3) \mod 26$$

The receiver of such a message can easily decrypt it by using the formula

$$M = (C - 3) \mod 26$$

Applications (cont)

Example 3.6.5a: Use the Caesar cipher to encrypt the message HOW ARE YOU.

Solution

First translate the letters of HOW ARE YOU into their numeric equivalents:

$$7\ 14\ 22\ 0\ 17\ 4\ 24\ 14\ 20$$

Next encrypt the message by adding 3 to each number.

$$10\ 17\ 25\ 3\ 20\ 7\ 1\ 17\ 23$$

Finally, substitute the letters that correspond to these numbers. The encrypted messages becomes KRZ DUH BRX

Applications (cont)

Example 3.6.5b: Use the shift cipher with key 3 to decrypt the message `L DP ILQH`.

Solution

First translate the letters of `L DP ILQH` into their numeric equivalents:

$$11\ \ 3\ \ 15\ \ 8\ \ 11\ \ 16\ \ 7$$

Next decrypt the message by subtracting 3 from each number.

$$8\ \ 0\ \ 12\ \ 5\ \ 8\ \ 13\ \ 4$$

Then translate back into letters to obtain the original message: `I AM FINE`

Applications (cont)

When a private key cryptosystem is used, a pair of people who wish to communicate in secret must have a separate key. Since anyone knowing this key can both encrypt and decrypt messages easily, these two people need to securely exchange the key.
Shift ciphers can be broken by what we call a *brute force attack*. It only takes 25 trials to guess the private key, hence, this is a useless cryptosystem in an information society.

Applications (cont)

Definition 3.6.7: Affine Cipher

Let $\mathscr{P} = \mathscr{C} = \mathbb{Z}_{26}$ and $\mathscr{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$. For each permutation $(a, b) \in \mathscr{K}$, define

$$e_{a,b}(x) = (ax + b) \mod 26,$$
$$d_{a,b}(y) = a^{-1}(y - b) \mod 26.$$

Since $\gcd(a, 26) = 1$, a can only take values from 1,3,5,7,9,11,15, 17,19,21,23,25.

Applications (cont)

Example 3.6.8: Encipher "ITS COOL" using an affine cipher with $a = 5$ and $b = 8$.

Solution

Using $e_{5,8}(x) = (5x + 8) \mod 26$, we fill in the following table

plaintext	I	T	S	C	O	O	L
x	8	19	18	2	14	14	11
$5x + 8$	48	103	98	18	78	78	63
$(5x + 8) \mod 26$	22	25	20	18	0	0	11
ciphertext	W	Z	U	S	A	A	L

Applications (cont)

Example 3.6.9: Decipher "HPCCXAQ" using an affine cipher with $a = 5$ and $b = 8$.

Solution

Since $5x \equiv 1 \pmod{26}$ is solved with $x \equiv 21 \pmod{26}$, hence $5^{-1} \equiv 21 \pmod{26}$. Therefore, the decrypter

$$d_{5,8}(y) = 21(y - 8) \mod 26$$

and so filling in our table gives

ciphertext	H	P	C	C	X	A	Q
y	7	15	2	2	23	0	16
$y - 8$	-1	7	-6	-6	15	-8	8
$21(y - 8)$	-21	147	-126	-126	315	-168	168
$21(y - 8) \mod 26$	5	17	4	4	3	14	12
plaintext	F	R	E	E	D	O	M

Applications (cont)

A substitution cipher is one in which letters are represented by other letters; it can be decriphered by someone knowing the order of the cipher alphabet used. It is defined formally as follows.

Definition 3.6.10: Substitution Cipher

Let $\mathscr{P} = \mathscr{C} = \mathbb{Z}_{26}$ and $\mathscr{K}$ be the set of all possible permutations of the 26 symbols in $\mathscr{P}$. For each substitution $\sigma \in \mathscr{K}$, define

$$e_\sigma(x) = \sigma(x), \quad d_\sigma(y) = \sigma^{-1}(y).$$

Remark: There are 26! permutations. Hence, finding the right private key may be difficult.

Applications (cont)

Example 3.6.11: Consinder the following permutation for substitution cipher:

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ R & Z & B & U & Q & K & F & C & P & Y & E & V & L & S & N & G & W & O & X & D & J & I & A & H & T & M \end{pmatrix}$$

Encode the word “HARDWORKING”.

Solution

The ciphertext is “CROUANOEPSF”.

Applications (cont)

Substitution ciphers are fairly easy to "crack" — the problem is that in English (or any language), certain letters are far more likely to appear. In English, for example, the letter "E" is far more likely to appear than the letter "Z". In fact, we have the following English letter frequency table

A	8.2%	F	2.2%	K	0.8%	P	1.9%	U	2.8%	Z	0.1%
B	1.5%	G	2.0%	L	4.0%	Q	0.1%	V	1.0%		
C	2.8%	H	6.1%	M	2.4%	R	6.0%	W	2.3%		
D	4.3%	I	7.0%	N	6.7%	S	6.3%	X	0.1%		
E	12.7%	J	2.2%	O	7.5%	T	9.1%	Y	2.0%		

The approximate percentages for the first few letters in the list below are:

E: 12.7%, T: 9.1%, A: 8.2%, O: 7.5%

and the percentages for the last few are:

J: 0.2%, Q: 0.1%, Z: 0.1%.

Applications (cont)

RSA is a popular public-key encryption method used in electronic commerce. In what follows, we will investigate how to encrypt and decrypt a message using RSA cryptography. First, we define RSA formally.

Definition 3.6.13: RSA Cryptosystem

Let $n = pq$, where p and q different prime numbers. Let $\mathscr{P} = \mathscr{C} = \mathbb{Z}_n$, define

$$\mathscr{K} = \{(n, p, q, a, b) : ab \equiv 1 \pmod{\phi(n)}\}.$$

For every $k \in \mathscr{K}$, we define

$$e_k(x) = x^b \mod n, \quad d_k(y) = y^a \mod n$$

Applications (cont)

Definition 3.6.13: RSA Cryptosystem (cont)

Here $x, y \in \mathbb{Z}_n$ and ϕ is the *Euler phi function*, which is an arithmetic function that counts the number of positive integers less than or equal to n that are relatively prime to n. It is found mathematically to be

$$\phi(n) = n \prod_{\substack{p|n \\ p \text{ is prime}}} \left(1 - \frac{1}{p}\right).$$

The values n and b comprise the *public key* and the values p, q and a form the *private key*.

Applications (cont)

Example 3.6.14: Find the number of integers relatively prime to 36.

Solution

$$\phi(36) = \phi(2^2 3^2) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12.$$

In words, this says that the distinct prime factors of 36 are 2 and 3; half of the thirty-six integers from 1 to 36 are divisible by 2, leaving eighteen; a third of those are divisible by 3, leaving twelve coprime to 36. And indeed there are twelve: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, and 35.

Applications (cont)

Theorem 3.6.15

When p and q are prime numbers,
$\phi(pq) = (p-1)(q-1)$.

To encrypt a message using the RSA cipher, a person needs to know the value of pq and of another number b, both of which are made publicly available. But only a person who knows the individual values of p, q and a can decrypt an encrypted message.

Applications (cont)

Example 3.6.16: Suppose Alice decides to set up an RSA cipher. She chooses two prime numbers, say $p = 5$ and $q = 11$, and computes $n = pq = 55$. She then chooses a positive integer b that is relatively prime to $(p-1)(q-1)$. In this case, $(p-1)(q-1) = 4(10) = 40$, so she may take $b = 3$ is relatively prime to 40. The two numbers $n = 55$ and $b = 3$ are the public key, which she may distribute widely. To decrypt the message, Alice needs to find the decryption key, a number a that is a positive inverse to b modulo $(p-1)(q-1)$. In this case, the key is

$$k = (55, 5, 11, a, 3).$$

1. Bobs wants to send Alice the message `HA`. Find the ciphertext for his message.
2. Find the value of a and decrypt the ciphertext 17.

Applications (cont)

Example 3.6.16 Solution

1. Bob will send his message in two blocks, one for the `H` and another for the `A`. The letters `H` and `A` are encoded as `7` and `0` respectively. The corresponding ciphertext is computed as follows:

$$e(7) = 7^3 \mod 55 = 343 \mod 55 = 13,$$
$$e(0) = 0^3 \mod 55 = 0.$$

Accordingly, Bob sends Alice the message: `13 0`.

Applications (cont)

Example 3.6.16 Solution (cont)

2. The integer a needs to satisfy

$$ab = 3a \equiv 1 \pmod{\phi(55)}$$

Here, $\phi(55) = (p-1)(q-1) = 40$. Using modular arithmetic, we can find

$$a \equiv 3^{-1} \equiv 27 \pmod{40}.$$

and then compute

$$\begin{aligned} d(17) &\equiv 17^{27} = 17^{16+8+2+1} \equiv 17^{16+8+2+1} \pmod{55} \\ &\equiv (16 \cdot 26 \cdot 14 \cdot 17) \pmod{55} \\ &\equiv 99008 \equiv 8 \pmod{55} \end{aligned}$$

Applications (cont)

Example 3.6.16 Solution (cont)

2. where
$$\begin{cases} 17^2 \mod 55 = 17^2 \mod 55 = 14 \\ 17^4 \mod 55 = (14)^2 \mod 55 = 31 \\ 17^8 \mod 55 = (31)^2 \mod 55 = 26 \\ 17^{16} \mod 55 = (26)^2 \mod 55 = 16. \end{cases}$$

Thus the plaintext of Bob's message is 8. The letter corresponding to 8 is `I`.

In reality, RSA is used in setting up a secure communication channel. These days, a key length of at least 4096 bits is required.

```
openssl req -out CSR.csr -new -newkey rsa:4096 -nodes
        -keyout privateKey.key
```

Applications (cont)

Real-world crypto issues:

- Block ciphers: encrypts blocks of a fixed length instead of alphabets. It is a generalisation of the substitution cipher. The number of permutations of the set of blocks of a cipher with a 128 bit block size is $(2^{128})!$.
  The most popular block cipher is AES (Advanced Encryption Standard). The older block cipher is DES (deprecated due to poor security).

Applications (cont)

Real-world crypto issues (cont):

- Stream ciphers: The most common native stream cipher in common use on desktop and mobile devices is RC4. Salsa20 and ChaCha are the newer state of art stream ciphers.
- Key exchange protocols attempt to solve a problem that Alice and Bob, have to agree on a secret value over an insecure communication channel. Using Diffie-Hellman (discrete logarithms or elliptic curves), we can agree on shared secrets across an insecure Internet.
- https runs over TLS (Transport Layer Security).

Outline

1. Logic for Equality
2. Theory of Numbers
   - Elementary Number Theory
   - Modular Arithmetic
   - Euclidean Algorithm
   - Linear Congruences
   - Chinese Remainder Theorem
   - Applications of Number Theory
3. **Method of Proofs**
   - Direct, Contrapositive, Contradiction
   - Two Classical Theorems
   - Mathematical Induction

Methods of Proofs

To prove something, we need to start from somewhere. For mathematics, the 'somewhere' is set theory. For this topic, the 'somewhere' is the 'axioms' of natural numbers and integers.

But how to we know the rules associated with sets are 'true'???

Mathematicians have discovered that it is impossible to prove a rich mathematical system (i.e. a system which includes number theory as part of the theory) cannot be proven to be 'true' if it is consistent (i.e. there is no contradicting statements).

Note: Week 5 pre-recorded video tried to explore this.

Methods of Proofs (cont)

Disproof by counterexample: In reality, if you suspect that a mathematical statement is wrong, try to find a counterexample (to axioms or derived theorems, etc.).

If we believe the mathematical statement to be true, we can use a relevant proving techniques below:

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Mathematical induction

Disproof by Counterexample

To disprove a statement means to show that it is false. Consider the disproving a universal statement of the form

$$\forall x(P(x) \to Q(x)) \tag{2}$$

Since $\forall x(P(x) \to Q(x)) \equiv F$, that means

$$\begin{aligned} \sim \forall x(P(x) \to Q(x)) \equiv & \exists x \sim (P(x) \to Q(x)) \\ \equiv & \exists x P(x) \wedge \sim Q(x)) \equiv T \end{aligned}$$

Hence, to disprove (2) becomes finding a value of x for which $P(x)$ is true and $Q(x)$ is false. Such an x is called a *counterexample*.

Disproof by Counterexample (cont)

Example 1.14.1: Disprove the statement "for real numbers n, if n is even, then $\frac{n+2}{2}$ is even" by finding a counterexample.

Solution

Formally, we have

$$\forall n(\text{even}(n) \rightarrow \text{even}(\frac{n+2}{2})).$$

To disprove this statement, we find a counter-example of n: Let $n = 4$. 4 is even but $\frac{4+2}{2} = 3$ is not even.

Disproof by Counterexample (cont)

Example 1.14.2: Disprove the following statement by finding a counterexample:

For all real numbers a and b, if $a^2 = b^2$ then $a = b$.

Solution

Formally, the statement can be expressed as $\forall a \forall b(a^2 = b^2 \rightarrow a = b))$ To disprove it, we show that its negation

$$\sim \forall a \forall b(a^2 = b^2 \rightarrow a = b)) \equiv \exists a \exists b \sim (a^2 = b^2 \rightarrow a = b)$$
$$\equiv \exists a \exists b(a^2 = b^2 \wedge a \neq b).$$

is true, i.e. we can find a and b such that $a^2 = b^2$ but $a \neq b$: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, so $a^2 = b^2$. But $a = 1 \neq b = -1$.

Disproof by Counterexample (cont)

Example 1.14.3: Disprove the following statement

For real numbers a and b, if $a > b$ then $a^2 > b^2$.

Solution

Let $a = -1$, $b = -2$. Then $a > b$ but $a^2 = 1 < b^2 = 4$.

Example 1.14.4: Disprove the following statement

For integers m and n, if $2m + n$ is even, then m and n are both even.

Solution

Let $m = 1$ and $n = 2$. Then $2m + n = 4$ is even but $m = 1$ is not even.

Disproof by Counterexample (cont)

Disproving a universal statement is normally not too difficult as demonstrated above. The key technique is to find a counterexample. However, disproving an existential statement would be more complicate because we would have to prove that its negation, which is a universal statement, is true. This leads to direct proof, proof by contradiction, etc.

Disproof by Counterexample (cont)

Show that there is no positive integer n such that $n^2 + 3n + 2$ is prime.

Proof (by Direct Proof)

The negation of the statement is "$\forall$ positive integers n, $n^2 + 3n + 2$ is not prime."
Suppose n is any positive integer.
$n^2 + 3n + 2 = (n + 1)(n + 2)$. Note that $n + 1 > 1$ and $n + 2 > 1$ are integers because they are sums of integers and $n \geq 1$.
Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime.

Outline

Direct / Contrapositive / Contradiction Proofs

Let $A_1, \cdots, A_n$ and $T_1, \cdots, T_m$ be the axioms (and definitions) and theorems of the mathematical objects respectively that we are investigating. Let ϕ and ψ be two formulae. Then the conditional proposition can be represented as

$$A_1, \cdots, A_n, T_1, \cdots, T_m \vdash (\phi \rightarrow \psi). \tag{3}$$

When ϕ is "empty", i.e. there is no constraint, (3) can be written as

$$A_1, \cdots, A_n, T_1, \cdots, T_m \vdash \psi. \tag{4}$$

Direct proof

Formally, the *direct proof* of (3) can be expressed as

$$A_1 \wedge \cdots \wedge A_n \wedge T_1 \wedge \cdots \wedge T_m \wedge \phi \Rightarrow \psi.$$

However, the argument (3) can be further classified into existential statement and universal statements. To prove an existential statement, we either find a special value s, which satisfies the formula (quantified statement). This technique is called the *constructive direct proof of existence* and is demonstrated in the examples below.

Direct proof (cont)

Example 1.13.1: Prove that "there is an even integer n that can be written in 2 ways as a sum of 2 prime numbers."

Proof

Let $n = 10$. Then 10 = 5 + 5 = 3 + 7 and 3, 5 and 7 are all prime numbers. Let $P(n)$ be the predicate "n is prime". Then take $n = 10$, $p_1 = p_2 = 5$, $p_3 = 3$, $p_4 = 7$ and

$$\begin{array}{ll} & \underline{10 = 2 \cdot 5} \wedge \underline{5 \neq 3 \wedge 5 \neq 7 \wedge 5 \neq 7} \\ & \underline{\wedge P(5) \wedge P(5) \wedge P(3) \wedge P(7)} \wedge \underline{10 = 5 + 5 \wedge 10 = 3 + 7)} \\ \hline \therefore & \exists n,\ (\underline{\exists k(n = 2k)} \wedge \underline{\exists p_1 \exists p_2 \exists p_3 \exists p_4 (p_1 \neq p_3 \wedge p_1 \neq p_4 \wedge p_2 \neq p_4} \\ & \underline{\wedge P(p_1) \wedge P(p_2) \wedge P(p_3) \wedge P(p_4)} \wedge \underline{n = p_1 + p_2 \wedge n = p_3 + p_4}) \end{array}$$

Due to the complexity of formal proofs, we do not use formal proofs in deriving results in mathematics.

Direct proof (cont)

Example 1.13.4: Suppose r and s are integers. Prove that "there is an integer k such that $22r + 18s = 2k$".

Proof

Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers and
$2k = 2(11r + 9s) = 22r + 18s$.

Direct proof (cont)

It is possible to prove an existential statement indirectly without finding the value that matches the predicate. This is called the *non-constructive proof* and is demonstrated below.

Example 1.13.6

Prove that "There exist irrational numbers x and y s.t. x^y is rational".

Direct proof (cont)

Proof of Example 1.13.6:
Consider the number $\sqrt{2}^{\sqrt{2}}$, it can either be (i) rational or (ii) irrational, but not both by definition.

Case (i)

Let $x = y = \sqrt{2}$, then x^y is rational.

Case (ii)

Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, so both are irrational (the proof of $\sqrt{2}$ being irrational is given in Theorem 160). Then, $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$. Thus, x^y is rational.

Direct proof (cont)

To prove a universal statement, we have to verify that the predicate is true for all possible values. When the number of possible values are finite and not large, we can verify all of them as demonstrated in the following example.

However, when there are infinitely many values, we need to rely on the axioms and theorems characterising the mathematical object we studied or apply the principle of mathematical induction when the problem is related to $\mathbb{N}$.

Direct proof (cont)

Example 1.13.7: Use the method of exhaustion to prove the following statements:

1. If n is even and $4 \leq n \leq 20$, then n can be written as a sum of 2 prime numbers.

Proof

4=2+2	8=3+5	12=5+7	16=5+11	20=7+13
6=3+3	10=5+5	14=11+3	18=7+11	

2. Every even positive integer n which are less than 26 can be written as a sum of less than or equal to 3 perfect squares.

Solution

$2 = 1^2 + 1^2$	$8 = 2^2 + 2^2$	$14 = 3^2 + 2^2 + 1^2$	$20 = 4^2 + 2^2$
$4 = 2^2$	$10 = 3^2 + 1^2$	$16 = 4^2$	$22 = 3^2 + 3^2 + 2^2$
$6 = 1^2 + 1^2 + 2^2$	$12 = 2^2 + 2^2 + 2^2$	$18 = 3^2 + 3^2$	$24 = 4^2 + 2^2 + 2^2$

Direct proof (cont)

The following are examples where the values are infinite. The statement is shown to be true based on the axioms governing the values.

Example 1.13.9: Show that: Given any number, add 5, multiply by 4, subtract 6, divide by 2 and subtract twice the original number, then the final result is 7.

Proof

Let x be the given number (x is particular because it represents a single quantity but it is also arbitrarily chosen or generic because it can represent any number whatsoever). Then

$$\begin{aligned}&[(((x+5)\times 4)-6)\div 2]-2x=[((4x+20)-6)\div 2]-2x\\ =&[(4x+14)\div 2]-2x=[2x+7]-2x=7\end{aligned}$$

Thus no matter what number is given, the result will always be 7.

Direct proof (cont)

Example 1.13.10: Prove that the sum of any two even integers is even.

Proof

Suppose m and n are any even integers.[a]
By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s.
Then $m + n = 2r + 2s = 2(r + s)$.
Let $k = r + s$. k is an integer because it is a sum of integers.
Hence $m + n = 2k$ where k is an integer.
It follows by definition of even that $m + n$ is even.

[a] Note that m and n are arbitrarily chosen.

Direct proof (cont)

Example 1.13.11: Prove that the sum of any two odd integers is even.

Proof

Suppose m and n are any odd integers.
By definition of odd, $m = 2r + 1$ and $n = 2s + 1$ for some integers r and s.
Then
$m+n = (2r+1)+(2s+1) = 2r+2s+2 = 2(r+s+1)$.
Let $k = r + s + 1$. Note that k is an integer because it is a sum of integers.
Hence $m + n = 2k$ where k is an integer.
It follows by definition of even that $m + n$ is even.

Direct proof (cont)

Example 1.13.12: Prove that the products of any two even integers is even.

Proof

Suppose m and n are any even integers.
By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s.
Then $mn = (2r) \cdot (2s) = 2(2rs)$.
Let $k = 2rs$. Note that k is an integer because it is a product of integers.
Hence $mn = 2k$ where k is an integer.
It follows by definition of even that mn is even.

Direct proof (cont)

Example 1.13.13: Prove that for all integers n, if n is odd, then n^2 is odd.

Proof

Suppose n is any odd integer. By definition of odd, $n = 2s + 1$ for some integer s.
Then $n^2 = (2s + 1)^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$
Let $k = 2s^2 + 2s$. Note that k is an integer because it is a sum of integers.
Hence $n^2 = 2k + 1$ where k is an integer.
It follows by definition of odd that n^2 is odd.

Direct proof (cont)

Theorem 1.13.15: Prove that the sum of any two rational numbers is rational.

Proof

Suppose r and s are rational numbers. By definition of rational number, $r = a/b$ and $s = c/d$ for some integers a, $b \neq 0$, c and $d \neq 0$. Thus

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Since the products and sums of integers are integers, $ad + bc$ and bd are integers. Since $b \neq 0$ and $d \neq 0$, $bd \neq 0$.
Therefore, $r + s$ is a ratio of integers and it is rational by definition.

Proof by Contraposition

Proof by contraposition or *contrapositive proof* is based on the logical equivalences of conditional statements introduced in Topic 1: $\phi \rightarrow \psi \equiv \sim \psi \rightarrow \sim \phi$. Formally, contrapositive proof of (3) can be expressed as

$$A_1 \wedge \cdots \wedge A_n \wedge T_1 \wedge \cdots \wedge T_m \wedge \sim \psi \Rightarrow \sim \phi.$$

The outline of the proof is given below:

1. Rewrite the statement to be proved in the contrapositive form
2. Prove the contrapositive form using direct proof.

Proof by Contraposition (cont)

Example 1.13.29: Prove that for all integers n, if n^2 is even then n is even.

Proof

In contrapositive form: For all integers n, if n is odd then n^2 is odd.

Suppose n is any odd integer. Then $n = 2k + 1$ for some integer k.

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ So n^2 is odd.

Proof by Contraposition (cont)

Example 1.13.31: Prove that for all integers n, if $3n + 2$ is odd then n is odd.

Proof

In contrapositive form: For all integers n, if n is even then $3n + 2$ is even.
Suppose n is any even integer. Then $n = 2k$ for some integer k. $3n + 2 = 6k + 2 = 2(3k + 1)$. Here $3k + 1$ is an integer. So $3n + 2$ is odd.

Proof by Contraposition (cont)

Example 1.13.32: Prove that for any natural numbers n, a and b, if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof

Suppose $a > \sqrt{n}$ and $b > \sqrt{n}$, then
$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$ which means $a \cdot b \neq n$.

Proof by Contradiction

Proof by contradiction is based on the logical equivalences of conditional statements introduced in Topic 1: $\phi \rightarrow \psi \equiv \sim \phi \vee \psi \equiv \sim (\phi \wedge \sim \psi)$. Formally, *proof by contradiction* for (3) can be expressed as

$$A_1 \wedge \cdots \wedge A_n \wedge T_1 \wedge \cdots \wedge T_m \wedge \phi \wedge \sim \psi \Rightarrow F.$$

Hence, to prove a statement by contradiction, we first need to suppose the negation of the conclusion of the statement is true. Then together with the premises and some axioms or theorem, we arrive at a logically contradicting statement. This means that the **negation of the conclusion** cannot be true, hence the conclusion must be true.

Proof by Contradiction (cont)

Example 1.13.17: For all integers m and n, if $mn = 1$ then $m = n = 1$ or $m = n = -1$.

Hypotheses: "m and n are integers and $mn = 1$".
Conclusion: "$m = n = 1$ or $m = n = -1$".

Proof by contradiction

Suppose "m and n are integers and $mn = 1$" is true but "$(m = 1 \wedge n = 1) \vee (m = -1 \wedge n = -1)$" is false.
So $((m \neq 1) \vee (n \neq 1)) \wedge ((m \neq -1) \vee (n \neq -1))$. This is logically equivalent to
$(m \neq 1 \wedge m \neq -1) \vee (n \neq 1 \wedge m \neq -1) \vee$
$(m \neq 1 \wedge n \neq -1) \vee (n \neq 1 \wedge n \neq -1)$.

Proof by Contradiction (cont)

Example 1.13.17: Proof by contradiction (cont)

We can classify into the following cases:

1. $m \neq 1 \wedge m \neq -1$:
   1. $m < -1$:
      1. $n = 0$: $mn = 0$. Contradicting with $mn = 1$.
      2. $n \leq -1$: $mn > 1$. Contradicting with $mn = 1$.
      3. $n \geq 1$: $mn < -1$. Contradicting with $mn = 1$.
   2. $m = 0$: $mn = 0$. Contradicting with $mn = 1$.
   3. $m > 1$:
      1. $n = 0$: $mn = 0$. Contradicting with $mn = 1$.
      2. $n \leq -1$: $mn < -1$. Contradicting with $mn = 1$.
      3. $n \geq 1$: $mn > 1$. Contradicting with $mn = 1$.
2. $n \neq 1 \wedge n \neq -1$: This is similar to case 1., the only difference is m and n are exchanged.

Proof by Contradiction (cont)

Example 1.13.17: Proof by contradiction (cont)

3. $n \neq 1 \wedge m \neq -1$:
   1. $n > 1 \wedge m > -1$: $mn = 0 \vee mn > 1$. Contradicting with $mn = 1$.
   2. $n > 1 \wedge m < -1$: $mn < -1$. Contradicting with $mn = 1$.
   3. $n < 1 \wedge m > -1$: $mn = 0 \vee mn < 0$. Contradicting with $mn = 1$.
   4. $n < 1 \wedge m < -1$: $mn = 0 \vee mn > 1$. Contradicting with $mn = 1$.
4. $m \neq 1 \wedge n \neq -1$: This is similar to case 3., the only difference is m and n are exchanged.

All situation leads to contradiction. Hence, the conclusion cannot be false and hence the statement is proved.

Proof by Contradiction (cont)

Example 1.13.18: Show that the rational number $\frac{1}{4}$ is not an integer.

Proof

Suppose $\frac{1}{4}$ is an integer. Then

$$4 \times \frac{1}{4} = 1$$

and 1 can be factorised into two integers different from 1 and -1. This is contradicting with Example 1.13.17 (Slide 150).

Proof by Contradiction (cont)

Example 1.13.19: Use proof by contradiction to prove that for all integers n, if n^2 is even then n is even.

Proof

Suppose there is an integer such that n^2 is even and n is not even. Hence, $n = 2k + 1$ for some integer k and

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

So n^2 is odd, which contradicts the supposition that n^2 is even.

Proof by Contradiction (cont)

Theorem 1.13.20: Using the method of proof by contradiction to show that "There is no integer that is both even and odd."

Proof

Suppose there is an integer n that is both even and odd. By definition of even, $n = 2a$ for some integer a. By definition of odd, $n = 2b + 1$ for some integer b. Hence

$$2a = 2b + 1 \Rightarrow 2(a - b) = 1, \quad a - b \in \mathbb{Z}.$$

This is a contradiction since 1 cannot be factorised as demonstrated in Example 1.13.17 (Slide 150).

Proof by Contradiction (cont)

Theorem 1.13.21: There is no greatest integer.

Proof

Suppose there is a greatest integer N. Then $n \leq N$ for every integer n.
Let $M = N + 1$. Now M is an integer since it is a sum of integers. Also $N < N + 1 = M$.
Thus M is an integer that is greater than N.
However, N is the greatest integer, so $M < N$. Hence $M < N \wedge N < M$ which is a contradiction.
Thus the supposition is false and "there is no greatest integer" is true.

Proof by Contradiction (cont)

Example 1.13.26: Use proof by contradiction to show that the sum of any rational number and any irrational number is irrational.

Proof

Suppose there is a rational number r and an irrational number s such that $r + s$ is rational.
By definition of rational, $r = a/b$ and $r + s = c/d$ for some integers a, b, c and d with $b \neq 0$ and $d \neq 0$. Then
$r + s = \frac{a}{b} + s = \frac{c}{d} \Rightarrow s = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$
Both $bc - ad$ and bd are integers and $bd \neq 0$. Thus s is rational.
This contradicts the supposition that s is irrational (by definition, irrational cannot be written as a ratio of integers).
Hence the sum of any rational number and any irrational number is irrational.

Proof by Contradiction (cont)

Example 1.13.27: Prove that $1 + 3\sqrt{2}$ is irrational.

Proof

Suppose $1 + 3\sqrt{2}$ is rational. Then

$$1 + 3\sqrt{2} = \frac{a}{b} \qquad (*)$$

for some integers a and $b \neq 0$. Rearranging (*), we have

$$3\sqrt{2} = \frac{a}{b} - 1 = \frac{a-b}{b} \Rightarrow \sqrt{2} = \frac{a-b}{3b}$$

Both $a - b$ and $3b \neq 0$ are integers. Hence $\sqrt{2}$ is rational, this contradicts with the fact that $\sqrt{2}$ is irrational as demonstrated in Theorem 1.13.24 (Slide 160).
Hence $1 + 3\sqrt{2}$ is irrational.

Outline

Proof by Contradiction (cont)

Theorem 1.13.24: $\sqrt{2}$ is irrational.

Proof

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors and $n \neq 0$ such that

$$\sqrt{2} = \frac{m}{n}.$$

This implies $$2 = \frac{m^2}{n^2} \Rightarrow 2n^2 = m^2$$

So m^2 is even and m must be even (otherwise it must be odd, but the square of odd number must be odd) and there is an integer k such that $m = 2k$. Hence

$$2n^2 = m^2 = 4k^2 \Rightarrow n^2 = 2k^2.$$

Now, n^2 is even and so n is even. This implies that both m and n have a common factor of 2, which contradicts the supposition that m and n have no common factors.

Proof by Contradiction (cont)

Theorem 1.13.25: For a positive integer k, if $\sqrt{k}$ is not integer, then $\sqrt{k}$ is irrational.

Proof of Theorem 1.13.25

Let $\sqrt{k}$ be a non-integer and rational. Then $E = \{b \in \mathbb{N}^* : \exists a(a \in \mathbb{N} \wedge \sqrt{k} = a/b)\} \neq \emptyset$ and by the Well-ordering principle, E contains the smallest value b_1.

Let $\sqrt{k} = a_1/b_1$, $a_1 > 0$, q be the largest positive integer no greater than $\sqrt{k}$, i.e. $\sqrt{k} - 1 < q < \sqrt{k}$. Then

$$\sqrt{k} = \frac{a_1}{b_1} = \frac{a_1(\sqrt{k} - q)}{b_1(\sqrt{k} - q)} = \frac{a_1\sqrt{k} - a_1 q}{b_1((\frac{a_1}{b_1}) - q)} = \frac{b_1\sqrt{k} \times \sqrt{k} - a_1 q}{a_1 - b_1 q} = \frac{b_1 k - a_1 q}{a_1 - b_1 q}$$

Proof by Contradiction (cont)

Proof of Theorem 1.13.25 (cont)

Let $a_2 = b_1 k - a_1 q$ and $b_2 = a_1 - b_1 q$. Since $q < \sqrt{k}$,

$$a_2 = b_1 k - a_1 q = a_1(\frac{b_1}{a_1} k - q) = a_1(\frac{k}{\sqrt{k}} - q) = a_1(\sqrt{k} - q) > 0$$

$$b_2 = a_1 - b_1 q = b_1(\frac{a_1}{b_1} - q) = b_1(\sqrt{k} - q)$$

This implies $b_2 - b_1 = b_1(\sqrt{k} - q) - b_1 = b_1(\sqrt{k} - q - 1) > 0 \Rightarrow b_2 > b_1$. The positive integer b_2 is smaller than b_1. This contradicts with the definition of b_1.

Theorem 2: Infinitude of Primes

Theorem 3.2.19: The set of prime numbers is infinite.

Proof

Suppose the set of prime numbers is finite. Then all the prime numbers can be listed, say, in ascending order:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \cdots,\ p_n.$$

Consider the integer

$$N = p_1 p_2 p_3 \cdots p_n + 1 > 1$$

By Theorem in Slide 24, N is divisible by some prime number p. Since p is prime, p must equal one of the prime numbers $p_1, p_2, p_3, \cdots, p_n$. Let $p = p_k$ for some $1 \leq k \leq n$ and

$p = p_k | (N = p_1 p_2 p_3 \cdots p_k \cdots p_n + 1) \Rightarrow p_k m = p_1 p_2 p_3 \cdots p_k \cdots p_n + 1 \Rightarrow$
$p_k (m - p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n) = 1$

for some integer m. This implies 1 can be factorised into two integers which are larger than 1, a contradiction.

Outline

Mathematical Induction

Mathematical induction is a method of proof developed to check conjectures about the outcomes of processes that occur repeatedly and according to definite patterns which are related to the linear order of natural numbers. It is a two-step process:

1. Basis Step: Show that the $P(a)$ is true for a particular integer a.
2. Inductive Step: Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.
   To perform this step, assume that the property is true for $n = k$ for some integer $k \geq a$. This supposition is called the *inductive hypothesis*.
   Then show that the property is true for $n = k + 1$.

Mathematical Induction (cont)

It is based on the following *principle of ordinary mathematical induction*.

Principle of Ordinary Mathematical Induction

Let $P(n)$ be a predicate that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement "for all integers $n \geq a$, $P(n)$" is true.

Mathematical Induction (cont)

Strong Form of Mathematical Induction

Let $P(n)$ be a predicate that is defined for integers $n \geq n_0$.

1. Verify that $P(n_0)$ is true.
2. Assume that $P(n_0), P(n_0+1), \cdots, P(k)$ are true.
3. Show that $P(k+1)$ is true.

Then the statement "for all integers $n \geq n_0$, $P(n)$" is true.

The idea behind the inductive step is to show that

$$[P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)] \Rightarrow P(k+1).$$

This form is used in the proof of Theorem 3.2.6 (Slide 24)

Mathematical Induction (cont)

Euler first noticed (in 1772) that the quadratic polynomial

$$P(n) = n^2 + n + 41$$

is prime for the 40 integers $n = 0, 1, 2, ..., 39$. However, it does not give a prime number for $n = 40$.
There are many functions which takes natural numbers with various properties. To show that the properties persist for all natural numbers, we need to prove it using the principle of mathematical induction.

Some Categories of Problems

The predicate $P(n)$ can be categorised to

- Properties of numbers (e.g. divisible by some number)
- Equalities
- Inequalities
- Combinatorics???
- ???

Induction with property of integers

Example 3.1.6: Use mathematical induction to prove that for all integers $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Proof

Let $P(n)$: "$3|2^{2n} - 1$".
Basis Step: Show that $P(1)$ is true.
$2^{2(1)} - 1 = 3$ is divisible by 3.
So $P(1)$ is true.

Induction with property of integers

Proof of Example 3.1.6 (cont)

Inductive Step:
Suppose $P(k)$ is true for an integer $k \geq 1$, that is $3|2^{2k} - 1$. We must show that $2^{2(k+1)} - 1$ is divisible by 3.
$3|2^{2k} - 1 \Rightarrow 2^{2k} - 1 = 3a$ for some integer a.

$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 3(2^{2k}) + (2^{2k} - 1)$$
$$= 3(2^{2k}) + 3a = 3(2^{2k} + a) \Rightarrow 3|2^{2(k+1)} - 1.$$

Thus $P(k+1)$ is true.
Hence, by mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

Equalites

Example 3.1.3: Use mathematical induction to prove that

$$\sum_{i=1}^{n} = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof

Let $P(n)$: "$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$".
Basis Step: Show that $P(1)$ is true.
LHS = 1, RHS = $\frac{1(1+1)}{2} = 1$.
So LHS of $P(1)$ = RHS of $P(1)$ and $P(1)$ is true.

Equalites (cont)

Proof of Example 3.1.3 (cont)

Inductive Step: Suppose $P(k)$ is true for an integer $k \geq 1$ that is

$$\sum_{i=1}^{k} i = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Show that $P(k+1)$ is true:

$$\begin{aligned}
\text{LHS of } P(k+1) &= \underbrace{1 + 2 + \cdots + k}_{\text{using assumption}} + k + 1 \\
&= \frac{k(k+1)}{2} + k + 1 = \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+1+1)}{2} = \text{RHS of } P(k+1).
\end{aligned}$$

So $P(k+1)$ is true. **By mathematical induction, $P(n)$ is true for all $n \geq 1$.**

Equalites (cont)

Example 3.1.2: Use mathematical induction to prove that the sum of the first n odd positive integers is n^2 for $n \geq 1$.

Hint: $P(n)$: "$1 + 3 + \cdots + (2n - 1) = n^2$".

Class Exercise.

Generalisation to arithmetic progression series:

$$a + (a + d) + \cdots + (a + (n - 1)d) = \frac{n(2a + (n - 1)d)}{2}.$$

Equalites (cont)

Example: Use mathematical induction to prove that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Class Exercise.

Equalites (cont)

Example 3.1.4: Use mathematical induction to prove that

$$\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

Class Exercise.

Jacob Bernoulli (1713) and Johann Faulhaber have noticed that

$$\sum_{i=1}^{n} i^p = \text{polynomial of } n \text{ to degree } p+1$$

Equalites (cont)

They derive the following formula:

$$\sum_{i=1}^{n} i^p = \frac{n^{p+1}}{p+1} + \frac{1}{2}n^p + \sum_{i=2}^{p} \frac{B_i}{i!} \frac{p!}{(p-i+1)!} n^{p-i+1}$$

where B_i are the Bernoulli numbers:

$$B_0 = 1,\ B_1 = 1/2,\ B_2 = 1/6,\ B_3 = 0,\ B_4 = -1/30, \ldots.$$

We find that the formulas in discrete mathematics is not as nice as in Calculus where

$$\int_0^n x^p dx = \frac{n^{p+1}}{p+1}.$$

Inequalites

Example 3.1.6: Use mathematical induction to prove that

$$2n + 1 < 2^n, \quad \text{for all integers } n \geq 3.$$

Proof

Let $P(n)$: "$2n + 1 < 2^n$".
Basis Step: Show that $P(3)$ is true.
LHS of $P(3) = 2(3) + 1 = 7$, RHS of $P(3) = 2^3 = 8$.
Hence LHS of $P(3) <$ RHS of $P(3)$ and so $P(3)$ is true.

Inequalites

Proof of Example 3.1.6 (cont)

Inductive Step: Suppose $P(k) := 2k + 1 < 2^k$ is true for some integer $k \geq 3$. Show that $P(k+1)$ is true:

$$\text{LHS of } P(k+1) = 2(k+1) + 1 = \underbrace{(2k+1)}_{\text{using assumption}} + 2$$

$$< 2^k + 2 < 2^k + \underbrace{2^k}_{k \geq 3 \Rightarrow 2 < 2^k} = 2(2^k)$$

$$= 2^{k+1} = \text{RHS of } P(k+1).$$

So $P(k+1)$ is true.
Hence, by mathematical induction, $P(n)$ is true for all integers $n \geq 3$.