CS 40
FOUNDATIONS OF CS

Summer 2024
Session A

Wednesday's learning goals

- Modular arithmetic and applications
- Finding the inverse of a number mod n
- Proof by contradiction

Modular arithmetic (on the clock)

Arithmetic on a ring of integers $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$

ring

$f_m : \mathbb{Z} \longrightarrow \mathbb{Z}_m$

$f_m(x) = x \mod m$

How many minutes past the hour?

$15 \mod 60 =$

$(15+60) \mod 60 = 15$

Obs: $(a+jm) \mod m = a \mod m$

Congruence (mod m): Practice notation

Definition: Let m be an integer greater than 1. Let a and b be any two integers. Then a is congruent to b (**mod** m), denoted as $a \equiv b$ (**mod** m) if and only if $a \bmod m = b \bmod m$

$(365 + 657)$ **mod** $60 = ((365 \bmod 60) + (675 \bmod 60)) \bmod 60$

$= (5 + 57) \bmod 60$

$= 62 \bmod 60 = 2$

$365 \equiv 5 \pmod{60}$

$657 \equiv 57 \pmod{60}$

$(365 \cdot 657)$ **mod** $60 = ((365 \bmod 60) \cdot (657 \bmod 60)) \bmod 60$

$= (5 \cdot 57) \bmod 60$

$= (5(60-3)) \bmod 60 = (5 \cdot 60 - 5 \cdot 3) \bmod 60$

$= -15 \bmod 60 = 45$

Theorems related to congruence

Theorem 2.1(i) Integers a, a', b, b' s.t

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

(i) $(a+b) \equiv (a'+b') \bmod m$ → will prove this statement later.

(ii) $(a-b) \equiv (a'-b') \bmod m$

(iii) $(ab) \equiv (a'b') \bmod m$

$a \equiv b \pmod m$ means $a \bmod m = b \bmod m$

$15 \equiv 75 \pmod{60}$

$75 \equiv 15 \pmod{60}$

$15 \equiv -45 \pmod{60}$

$(a + jm) \bmod m = a \bmod m$

Restate: $a + jm \equiv a \pmod m$

Theorem 1: $a, b, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

(i) $a \equiv a \pmod m$

(ii) $a \equiv b \pmod m$ iff $b \equiv a \pmod m$

(iii) If $a \equiv b \pmod m$ & $b \equiv c \pmod m$

then $a \equiv c \pmod m$

Computing Arithmetic Expressions mod m

Which of the following are true?

A. $(102 + 48) \bmod 5 = ((102 \bmod 5) + (48 \bmod 5)) \bmod 5$

B. $(7 \cdot 10) \bmod 5 = ((7 \bmod 5) \cdot (10 \bmod 5)) \bmod 5$

C. $(2^5) \bmod 3 = ((2 \bmod 3)^{(5 \bmod 3)}) \bmod 3$

D. More than one of the above

E. None of the above

$2^5 \bmod 3$

$= ((2 \bmod 3)^5) \bmod 3$

$= 2^5 \bmod 3$

$= 4 \cdot 8 \bmod 3$

$= 1 \cdot 2 \bmod 3 = 2$

Neat applications of theorems

What is 8^{1759} mod 7?

properties: $8 \equiv 1 \pmod 7$

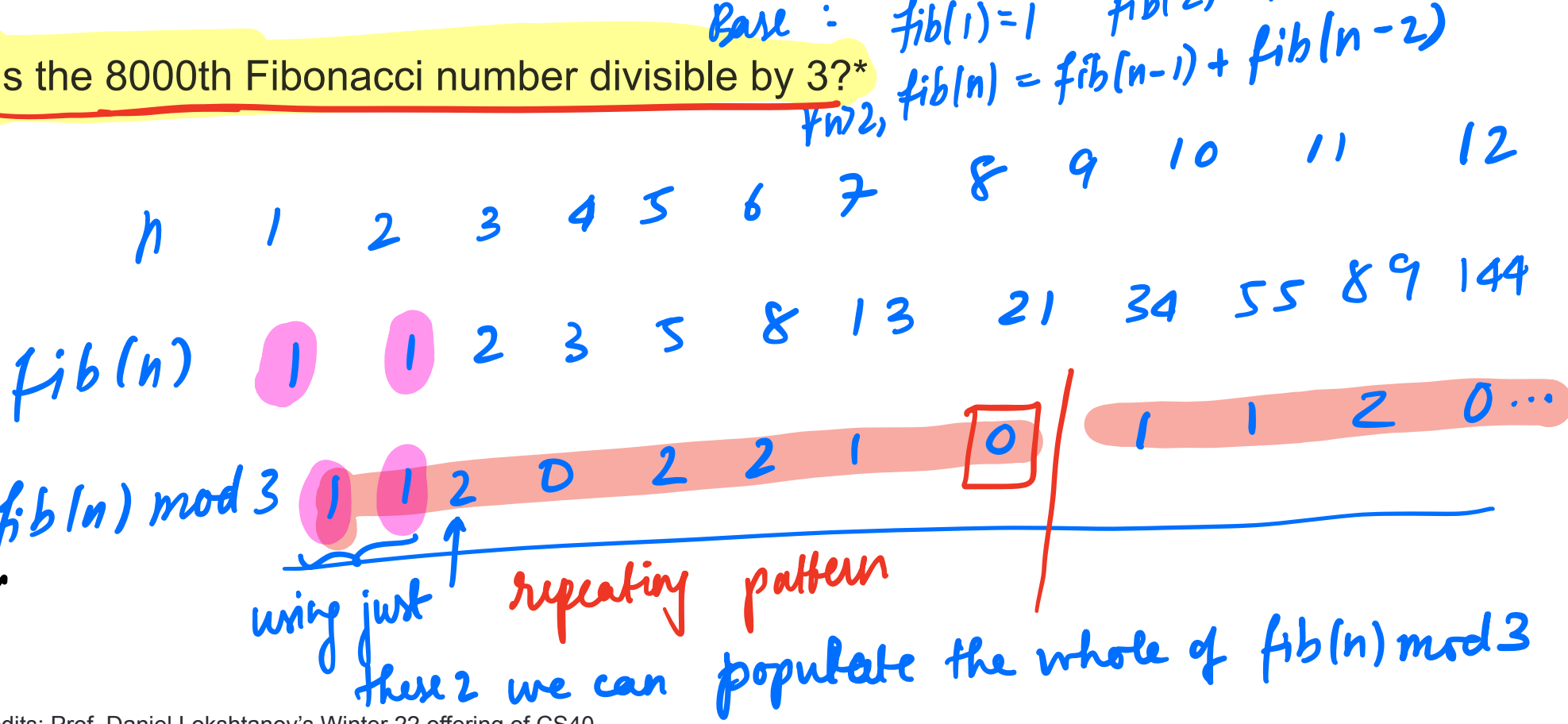
$8^{1759} \equiv 1^{1759} \pmod 7$

by defn of $\equiv$: $8^{1759} \bmod 7 = 1 \bmod 7$

$= 1$

Neat applications of theorems

Is the 8000th Fibonacci number divisible by 3?*



*credits: Prof. Daniel Lokshtanov's Winter 22 offering of CS40.

$$fib(n) \bmod 3 = (fib(n-1) + fib(n-2)) \bmod 3$$

$$= (fib(n-1) \bmod 3 + fib(n-2) \bmod 3) \bmod 3$$

In order to compute $fib(n) \bmod 3$ $n > 2$

do not need to know $fib(n)$

just knowing $fib(n-1) \bmod 3$ & $fib(n-2) \bmod 3$ is enough

---

Application 2: Division by 11 test

12331 ⟶ is it divisible by 11?

Test: Check if the difference of sum of alternate digits is divisible by 11

$1+3+1 - (2+3)$

$= 5 - 5$

$= 0$ is divisible by 11

$\therefore$ 12331 is divisible by 11

Why it works?

$$12331 = 1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 3 \cdot 10 + 1$$

$$(12331) \bmod 11 = (1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 3 \cdot 10 + 1) \bmod 11$$

$$
\begin{cases}
1 \pmod{11} \equiv 1 \\
10 \pmod{11} \equiv -1 & (\because 10 \bmod 11 = -1 \bmod 11 = 10) \\
10^2 \pmod{11} \equiv 1 \\
10^3 \pmod{11} \equiv -1 & (\because 10^3 \bmod 11 = -1 \bmod 11) \\
10^4 \pmod{11} \equiv 1
\end{cases}
$$

$-1 \bmod 11$

$-1 = q \cdot 11 + 91$ *

$\boxed{-1 = (-1) \cdot 11 + 10}$

$= -1 \bmod 11$

$$
(12331) \bmod 11 = (1 \cdot 10^4 + \boxed{2 \cdot 10^3} + 3 \cdot 10^2 + \boxed{3 \cdot 10} + 1) \bmod 11
$$

$$
= (1 \bmod 11 \cdot 10^4 \bmod 11 + 2 \bmod 11 \cdot 10^3 \bmod 11 + \cdots)
$$

$$
= (1 - 2 + 3 - 3 + 1) \bmod 11
$$

$$
= ((1 + 3 + 1) - (2 + 3)) \bmod 11
$$

$$
= (5 - 5) \bmod 11
$$

$$
= 0
$$

$\therefore$ 12331 is divisible by 11.

Proof of congruence theorems

Theorem 2: For $a, b, a', b' \in \mathbb{Z}$ and positive integer m, if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:

(i) $(a + b) \equiv (a' + b') \pmod{m}$

(ii) $(a - b) \equiv (a' - b') \pmod{m}$

(iii) $(a \cdot b) \equiv (a' \cdot b') \pmod{m}$

} Exercise try to prove for (ii) & (iii)

Informally: can bring mod "inside" and do it first, for addition and for multiplication.

Proof: We will prove 2(i)

T.S.T : For $a, b, a', b' \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

if $a \equiv a' \pmod m$ (Recall that this means $a \bmod m = a' \bmod m$)

$b \equiv b' \pmod m$

we want to show

$$(a+b) \equiv (a'+b') \pmod m$$

(ie) we want to show

$$(a+b) \bmod m = (a'+b') \bmod m$$

Since, $a \equiv a' \pmod m$, $a \bmod m = a' \bmod m$

$\therefore a = qm + r_a$ & $a' = q'm + r_a$ for some $q, q', r_a \in \mathbb{Z}$ (same r)

(Similarly) $b \equiv b' \pmod m$, $b \bmod m = b' \bmod m$

$\therefore b = pm + r_b$ & $b' = p'm + r_b$ for some $p, p', r_b \in \mathbb{Z}$

Now,

$$\begin{aligned}(a+b) \bmod m &= (qm + r_a + pm + r_b) \bmod m \\ &= ((q+p)m + r_a + r_b) \bmod m \\ &= (r_a + r_b) \bmod m\end{aligned}$$

$$(a'+b') \bmod m = (q'm + r_a + p'm + r_b) \bmod m = (r_a + r_b) \bmod m$$

Thus,

$$(a+b) \bmod m = (a'+b') \bmod m = (r_a + r_b) \bmod m$$

$\therefore (a+b) \equiv (a'+b') \pmod m$ by defn of $\equiv$

This completes the proof

Application: Pseudorandom numbers

$x_{n+1} = (7x_n + 4) \bmod 9, \text{ with } x_0 = 3.$

a c m

$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$

$x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$

$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$

$x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$

$x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$

$x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$

$x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$

$x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$

$x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$

repeats from here

General recursive generator

$x_{n+1} = (ax_n + c) \bmod m.$

seeds

$2 \le a < m,$

$0 \le c < m,$

$0 \le x_0 < m$

The sequence generated is 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,...
It repeats after generating 9 terms.

Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Multiplicative inverse mod m (key step in the RSA cryptosystem)

co-prime = gcd(x, m) = 1

$\bar{x}\,x \bmod m = 1$

$\bar{x}$ is the modular inverse of x

inverse:

$x\,\bar{x} = 1$

$inv(x) = \frac{1}{x}$

Multiplicative inverses don't always exist

For example, there is no multiplicative inverse of 2 mod 6.

Multiplicative inverse of x mod m exists
if and only if x and m are relatively prime.

How to find multiplicative inverse

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication: *Closure, Associativity, Commutativity, Identity, Distributivity, Additive Inverses* *BUT NOT DIVISION: Multiplicative inverses don't always exist*

Finding Multiplicative inverses mod m (when they exist)

Theorem 5.5.2: Expressing gcd(x, y) as a linear combination of x and y.

Let x and y be integers, then there are integers s and t such that

$$\gcd(x, y) = sx + ty$$

How to find this Extended Euclid's algorithm

$$\gcd(6,14) = 2 = (-2)\cdot 6 + 1\cdot 14$$

Use this Theorem to find mul inverse mod m. ($x\bar{x} \bmod m = 1$)

Qs: Give one x, y s.t $\gcd(x, y) = 1$

$\gcd(3, 5) = 1$

$$1 = 2 \cdot 5 - 3 \cdot 3$$

Find mul inverse of 3 mod 5

↓

Let mul inverse of 3 mod 5 be $\bar{x}$

$$\bar{x} \cdot 3 \bmod 5 = 1$$

$$1 \bmod 5 = (2 \cdot 5 - 3 \cdot 3) \bmod 5$$

$$1 = (-3 \cdot 3) \bmod 5$$

↑ $\bar{x} = -3$

because $(-3 \cdot 3) \bmod 5 = 1$

Finding inverses mod m

Extended Euclid Algo

- Find an inverse of 3 modulo 7.
  - Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
  - Write gcd(3, 7) as $s \cdot 3 + t \cdot 7$

    $$1 = -2 \cdot 3 + 1 \cdot 7$$

  - Hence, –2 is an inverse of 3 modulo 7.
  - To get a value within $\mathbb{Z}_7$ add 7

↳ here it'll be 5

$5 \cdot 3 \bmod 7 = 15 \bmod 7 = 1$

Finding inverses: Extended Euclid's

- **Example**: Find an inverse of 31 modulo 43.
- **Solution**: First use the Euclidian algorithm to show that gcd(31,43) = 1.

$43 = 1 \cdot 31 + 12$

$31 = 2 \cdot 12 + 7$

$12 = 1 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$\gcd(x, y) = \gcd(y \bmod x, x)$

$x < y$

↳ express 1 as linear comb of 31, 43

how?

Finding inverses: Extended Euclid's

- **Example**: Find an inverse of 31 modulo 43.
- **Solution**: First use the Euclidian algorithm to show that gcd(31,43) = 1.
- Working Backwards to express gcd(x, y) as a linear combination of x and y

$43 = 1 \cdot 31 + 12$ → $12 = 43 - 1 \cdot 31$

$31 = 2 \cdot 12 + 7$ → $7 = 31 - 2 \cdot 12$

$12 = 1 \cdot 7 + 5$ → $5 = 12 - 1 \cdot 7$

$7 = 1 \cdot 5 + 2$ → $2 = 7 - 1 \cdot 5$

$5 = 2 \cdot 2 + 1$ → $1 = 5 - 2 \cdot 2$

$2 = 2 \cdot 1 + 0$ →

rearranging eqn

y mod x

$1 = 5 - 2 \cdot 2$ (substitute)

$= 5 - 2 \cdot (7 - 1 \cdot 5)$ (simplify)

$= 3 \cdot 5 - 2 \cdot 7$ (subs)

$= 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7$ (simplify)

$= 3 \cdot 12 - 5 \cdot 7$ (subs)

$= 3 \cdot 12 - 5 \cdot (31 - 2 \cdot 12)$ (simplify)

$= 13 \cdot 12 - 5 \cdot 31$ (subs)

$= 13 \cdot (43 - 1 \cdot 31) - 5 \cdot 31$

$1 = 13 \cdot 43 - 18 \cdot 31$

1 as linear combn of 31 & 43

multiplicative inverse of 31 mod 43 is -18

also $-18+43=25$

both -18 & 25 are multiplicative inverses

Wed/Thursday's learning goals

- Proof by contradiction
- Strong induction
- Distinguish between and use as appropriate each of structural induction, mathematical induction, and strong induction
- Use insights from proofs to develop new algorithms

New! Proof by Contradiction (Rosen 1.7 p86)
To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

Prove p assuming ~p first the contradicting some true statement we show it should have been p

Example: From a few classes back.

A says "I am a knave or B is a knight"

B says nothing

p: A is a knight q: B is a knight

Goal: Prove p

Proof by contradiction

Suppose $\sim p$,

Then the statement

I am a knave or B is a knight

$\sim p \vee q$ is False

Since $\sim p$, A is a knave

& the statement is false

we have $\sim(\sim p \vee q)$ is True [∵ knaves lies]

But $\sim(\sim p \vee q) = p \wedge \sim q$

$= F \wedge \sim q$

$= F$

This contradicts that $\sim(\sim p \vee q)$ is True

∴ our assumption $\sim p$ is false

∴ p is True

New! Proof by Contradiction (Rosen 1.7 p86)
To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

Theorem: There is no greatest prime number.

New! Proof by Contradiction (Rosen 1.7 p86)
To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = "Every positive integer greater than 1 is a product of (one or more) primes."

↳ we will show this later today

Assume r is true

To show: $(r \wedge \neg r)$

r is True (We will prove it later today)
To show: r is False (under assumption).

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = ”Every positive integer greater than 1 is a product of primes.”

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

Idea: Use assumption to build a number that is not a product of primes

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = ”Every positive integer greater than 1 is a product of primes.”

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

largest prime

We can name all primes (since there are finitely many integers between 2 and n_{BIG})

$n_1, n_2, \ldots, n_{BIG}$

Consider the number **$C = (n_1\ n_2 \cdots n_{BIG}) + 1$**. This is a positive integer greater than 1.

Lemma: C does not have any prime factors and thus is not a product of primes.

In particular C cannot be expressed as product of primes.

C is a witness to ~r

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = "Every positive integer greater than 1 is a product of primes."

r

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

Lemma: There is an integer, C, that is not a product of primes.

$\Rightarrow \Leftarrow$ to r shows ~r

Since assuming that there is a greatest prime guarantees $(r \wedge \neg r)$ assumption must be **false**. Thus, its negation is true.

Recap

Proof by contradiction can be useful in proving negations of existentials.

In a proof by contradiction, we are proving a conditional claim $\neg p \to (r \wedge \neg r)$ where the hypothesis is the **negation of the statement we are trying to prove** and the conclusion is up to us to figure out!

Mathematical induction

$\forall n \in \mathbb{Z}^{\geq b}, P(n)$

Base case: $P(b)$

Induction case:

$\forall n \in \mathbb{Z}^{\geq b} \; (P(n) \rightarrow P(n+1))$

New approach: Strong induction

$\forall n \in \mathbb{Z}^{\geq b}, P(n)$

Base case: $P(b)$

$\vdots$

$P(b+j)$

Inductive case:

$\forall n \in \mathbb{Z}^{\geq b+j} \; (P(b) \wedge P(b+1) \wedge P(b+2) \cdots \wedge P(n)) \longrightarrow P(n+1)$

Mathematical induction

To prove a universal quantification where the element comes from the set of integers >= b, prove two cases:

Base case:

1. Prove the property is true about the number b

Inductive case

2. Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for n+1.

only for n

New approach: Strong induction

To prove a universal quantification where the element comes from the set of integers >= b:

1. Pick j basis cases and prove the property is true about b, …, b+j

can have many basis cases

2. Consider an arbitrary integer n that is >= b+j, assume (as the **strong induction hypothesis**) that the property holds for each of b, …, n, and use this and other facts to prove that the property holds for n+1.

n ≥ b+j

assume for b .... n

Theorem (Rosen p336): Every positive integer *greater than 1* is a product of (one or more) primes.

Proof by strong induction, with $b = 2$ and $j = 0$.

Basis step: WTS property is true about 2.

want to show

$(b=2)$ $2 = 1 \cdot 2 \rightarrow$ 2 is a product of primes by so the statement is true for 2.

Recursive step: Consider an arbitrary integer $n \geq 2$. Assume (as the IH) that the property is true about each of $2, \ldots, n$. WTS that the property is true about $n+1$.

Case 1: $n+1$ is prime:
$\rightarrow$ We can write $n+1$ in terms of itself

Case 2: $n+1$ is not prime:
$\Rightarrow n+1$ can be written as product of two nos a, b
$n+1 = a \cdot b$ where $2 \leq a < n+1$, $2 \leq b < n+1$

By Induction Hypothesis, a can be written as product of one or more primes

$a = p_1 p_2 \cdots p_k$

III by b can be written as one or more primes / product of

$$b = p_1' p_2' \cdots p_m'$$

$\therefore$ $n+1 = ab = p_1 p_2 \cdots p_l p_1' p_2' \cdots p_m'$

can be written as product of one or more primes.

This completes the proof

Change making

For which nonnegative integers n can we make change for n with coins of value 5 cents and 3 cents?

Which of the following is true?

A. The greedy algo works for all n>0
B. Some other algo works for all n>0
C. The greedy algo works for large enough n
D. Some other algo works for large enough n
E. None of the above

Can you make change $\forall n \in \mathbb{Z}^+$ using 5 cents & 3 cents? NO

ex: 2 cents ✗

$\exists c \in \mathbb{Z}^+$ s.t. $\forall n \geq c$, $n = 5x + 3y$ for some $x, y \in \mathbb{Z}^+$

(Exercise

Change making algorithm in pseudocode

```
1  procedure change(c_1, c_2, ..., c_r : values of denominations of coins, where c_1 > c_2 > ... > c_r ; n : a positive integer)
2
3  for i := 1 to r
4    d_i := 0 {d_i counts the number of coin of denomination c_i used}
5    while n ≥ c_i
6      d_i := d_i + 1 {Add a coin of denomination c_i}
7      n := n − c_i
8
9  return d_1, d_2, ..., d_r {d_i the number of coins of denomination c_i in the change for i=1, 2, ..., r}
```

Restating: We can make change for _____, we cannot make change for _____, and

_____ ⋆

A $\forall n \in \mathbb{Z}^{\geq 8}\ \exists x \in \mathbb{Z}^{\geq 8}\ \exists y \in \mathbb{Z}^{\geq 8}\ \ (5x + 3y = n)$

B $\forall n \in \mathbb{Z}^{\geq 8}\ \exists x \in \mathbb{N}\ \exists y \in \mathbb{N}\ \ (5x + 3y = n)$

Proving this using both strong induction & induction.

C $\exists n \in \mathbb{Z}^{\geq 8}\ \forall x \in \mathbb{Z}^{\geq 8}\ \forall y \in \mathbb{Z}^{\geq 8}\ \ (5x + 3y = n)$

D $\exists n \in \mathbb{Z}^{\geq 8}\ \forall x \in \mathbb{N}\ \forall y \in \mathbb{N}\ \ (5x + 3y = n)$

$\mathbb{Z}^{\geq 8} = \{x \in \mathbb{Z} \mid x \geq 8\}$

Mathematical induction

To prove a universal quantification where the element comes from the set of integers >= b, prove two cases:

1. Prove the property is true about the number b

2. Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for n+1.

Proof by mathematical induction, with $b = 8$

Basis step: WTS property is true about 8

Since $8 = 5 + 3$ ✓

The claim is true for $n = 8$

Inductive step: To show that claim is true for $n+1$ assuming claim is true for n.

→ $n+1 > 9$

Since claim is true for n, let $n = 5x + 3y$, $x, y \in \mathbb{Z}^+$

ex: $9 = 5 + 3$
↳ $x \neq 0$

Case (i) $x \neq 0$

want $x', y' \in \mathbb{Z}^+$ s.t

$$n+1 = 5x' + 3y'$$

How to set x' & y' in terms of x & y?

Let $x' = x - 1$, $y' = y + 2$

Then, $5(x') + 3y'$

$= 5(x-1) + 3(y+2)$

$= 5x + 3y - 5 + 6$

$= 5x + 3y + 1$ [$\because n = 5x + 3y$ by inductive hypothesis]

$= n + 1$

$\therefore$ $n+1 = 5x' + 3y'$ for some $x', y' \in \mathbb{Z}^+$

Case (ii) $x = 0$

Here $n = 3y$ [since $n+1 > 9$ & $n = 3y$, $y \geq 3$]

Want x', y' s.t $n+1 = 5x' + 3y'$

How to set x' & y' in terms of y?

Here $x' = 2$ $y' = y - 3$ $[y' \geq 0$ since $y \geq 3]$

$$5x' + 3y'$$

$$= 5 \cdot 2 + 3(y-3)$$

$$= 10 - 9 + 3y$$

$$= 1 + 3y$$

$$= 1 + h$$

$\therefore$ $\boxed{h+1 = 2 \cdot 5 + (y-3)3}$ ★

This proves the claim for case (ii)

Combining case (i) & (ii) proves the inductive case.

Mathematical induction

To prove a universal quantification where the element comes from the set of integers >= b, prove two cases:

1. Prove the property is true about the number b

2. Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for n+1.

Proof of $\star$ by mathematical induction $(b = 8)$

Basis step: WTS property is true about 8

Inductive step: Consider an arbitrary $n \geq 8$. Assume (as the IH) that there are nonnegative integers x, y such that $n = 5x + 3y$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$. We consider two cases, depending on whether any 5 cent coins are used for n.

Key insight: can write "+1" in terms of 5 and 3. How?

Mathematical induction

To prove a universal quantification where the element comes from the set of integers >= b, prove two cases:

1. Prove the property is true about the number b

2. Consider an arbitrary integer k greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for k, and use this and other facts to prove that the property holds for k+1.

Inductive step: Consider an arbitrary $n \geq 8$. Assume (as the IH) that there are nonnegative integers x, y such that $n = 5x + 3y$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$. We consider two cases, depending on whether any 5 cent coins are used for n.

Case 1: Assume .
Define $x' =$
and $y' =$
(both in $\mathbb{N}$ by case assumption).
Calculating:

$$5x' + 3y' \overset{\text{by def}}{=} \overset{\text{rearranging}}{=} \overset{\text{IH}}{=}$$

Case 2: Assume .
Therefore $n = 3y$ and $n \geq 8$, by case assumption. Therefore, $y \geq 3$ Define $x' = 2$ and $y' = y - 3$ (both in $\mathbb{N}$ by case assumption). Calculating:

$$5x' + 3y' \overset{\text{by def}}{=} 5(2) + 3(y-3) = 10 + 3y - 9 \overset{\text{rearranging}}{=} 3y + 10 - 9 \overset{\text{IH and case}}{=} n + 10 - 9 = n + 1$$

Prove the claim by strong induction:

Claim: $\forall n \geq \mathbb{Z}^{\geq 8} \; \exists x \in \mathbb{Z}^+ \exists y \in \mathbb{Z}^+ \; n = 5x + 3y$

Base case: $(n = 8, 9, 10)$

$8 = 5 + 3$

$9 = 3 \cdot 3$

$10 = 2 \cdot 5$

The claim is true for $n = 8, 9, 10$

Inductive case: Let $n+1 \in \mathbb{Z}^{>10}$

Assume by IH that the claim is true $\forall n' \in \{8, \ldots, n\}$

(i.e) $\forall n' \in \{8, \ldots, n\} \; \exists x \in \mathbb{Z}^+ \exists y \in \mathbb{Z}^+ \; n' = 5x + 3y$

strong induction

Complete the proof?

$\forall n > 10, \quad n - 2 > 8$

and by IH $\quad n - 2 = 5x + 3y$ for some $x, y \in \mathbb{Z}^+$

$5x + 3y + 3$

$= n - 2 + 3$

$= n + 1$

$\therefore \boxed{n + 1 = 5x + 3(y+1)}$ ★

This completes the proof.

New approach: Strong induction

To prove a universal quantification where the element comes from the set of integers >= b:

1. Pick j basis cases and prove the property is true about b, …, b+j

2. Consider an arbitrary integer n that is >= b+j, assume (as the **strong induction hypothesis**) that the property holds for each of b, …, n, and use this and other facts to prove that the property holds for n+1.

*Key insight: once we have enough basis cases, we can represent larger numbers using **one more** 3-cent coin than a smaller number*

New approach: Strong induction

To prove a universal quantification where the element comes from the set of integers >= b:

1. Pick j basis cases and prove the property is true about b, …, b+j

2. Consider an arbitrary integer n that is >= b+j, assume (as the **strong induction hypothesis** that the property holds for each of b, …, n, and use this and other facts to prove that the property holds for n+1.

Proof by strong induction, with $b = 8$ and $j = 2$.

Basis step: WTS property is true about $8, 9, 10$

New approach: Strong induction

To prove a universal quantification where the element comes from the set of integers >= b:

1. Pick j basis cases and prove the property is true about b, …, b+j

2. Consider an arbitrary integer n that is >= b+j, assume (as the **strong induction hypothesis** that the property holds for each of b, …, n, and use this and other facts to prove that the property holds for n+1.

Recursive step: Consider an arbitrary $n \geq 10$. Assume (as the IH) that the property is true about each of $8, 9, 10, \ldots, n$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$.

Algorithms: making change using 3 cent and 5 cent coins

Change making algorithm in pseudocode

```
1  procedure change(c1, c2, ..., cr: values of denominations of coins, where c1 > c2 > ... > cr; n: a positive integer)
2
3  for i := 1 to r
4    di := 0 {di counts the number of coin of denomination ci used}
5    while n ≥ ci
6      di := di + 1 {Add a coin of denomination ci}
7      n := n − ci
8
9  return d1, d2, ..., dr {di the number of coins of denomination ci in the change for i=1, 2, ..., r}
```

Recall: A different way to represent positive integers

Definition (Rosen p257): An integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Theorem (Rosen p336): Every positive integer *greater than 1* is a product of (one or more) primes.

Before proving theorem, let's try some example prime factorizations. Which of these match the definitions?

A. 3 = 3
B. 100 = (1)(2)(2)(5)(5)
C. 20 = (4)(5)
D. 9 = (3)(3)
E. All of the above.

Strong induction

To prove a universal quantification where the element comes from the set of integers >= b:

1. Pick j basis cases and prove the property is true about b, …, b+j

2. Consider an arbitrary integer n that is >= b+j, assume (as the **strong induction hypothesis**) that the property holds for each of b, …, n, and use this and other facts to prove that the property holds for n+1.

Key insight: a number is either prime or is the product of two smaller numbers.

Theorem (Rosen p336): Every positive integer *greater than 1* is a product of (one or more) primes.

Proof by strong induction, with $b = 2$ and $j = 0$.

proved earlier

Basis step: WTS property is true about 2.

Recursive step: Consider an arbitrary integer $n \geq 2$. Assume (as the IH) that the property is true about each of $2, \ldots, n$. WTS that the property is true about $n + 1$.

- A counterexample can be used to prove that $\forall x P(x)$ is **false**.
- A witness can be used to prove that $\exists x P(x)$ is **true**.
- **Proof by universal generalization**: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.
- To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.
- **Proof of Conditional by Direct Proof**: To prove that the implication $p \to q$ is true, we can assume p is true and use that assumption to show q is true.
- **Proof of Conditional by Contrapositive Proof**: To prove that the implication $p \to q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.
- **Proof by Cases**: To prove q when we know $p_1 \vee p_2$, show that $p_1 \to q$ and $p_2 \to q$.
- **Proof by Contradiction** To prove that a statement p is true, pick another statement r and if we can show that $\neg p \to (r \wedge \neg r)$ then we can conclude that p is true.
- **Proof by Structural Induction** To prove a universal quantification over a recursively defined set:

  Basis Step: Show the statement holds for elements specified in the basis step of the definition.
  Recursive Step: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

- **Proof by Mathematical Induction** To prove a universal quantification over the set of all integers greater than or equals some base integer b:

  Basis Step: Show the statement holds for b.
  Recursive Step: Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for $n + 1$.

- **Proof by Strong Induction** To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

  Basis Step: Show the statement holds for b, $b + 1$, $\ldots$, $b + j$.
  Recursive Step: Consider an arbitrary integer n greater than or equal to $b + j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b + 1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n + 1$.