Review for Final Exam

Part 1:

- Solving simple recurrence equations
- Sums of pth powers
- Proving formulas by induction
- Basic properties of
  - sets
  - logical statements
  - functions
- Set operators $\cap$, $\cup$, ^{c}
- Logical operators $\vee$, $\wedge$, $\neg$
- Venn diagrams and truth tables

Review: Recall that we define

$$S_p(n) := 1^p + 2^p + 3^p + \cdots + n^p = \sum_{k=1}^{n} k^p$$

We know some "closed formulas" for these:

- $S_0(n) = n$

- $S_1(n) = \frac{n(n+1)}{2}$

- $S_2(n) = \frac{n(n+1)(2n+1)}{6}$

- $S_3(n) = \frac{n^2(n+1)^2}{4}$

These formulas might not be easy to guess, but once we have the formula it is easy to prove by induction.

<u>Example</u>: Prove by induction that

$$S_2(n) = \frac{n(n+1)(2n+1)}{6} \quad \text{for } n \geq 1.$$

<u>Proof</u>: First we check the base case. The formula is correct when $n=1$ because $S_2(1) = 1^2 = 1$ and

$$\frac{1(1+1)(2\cdot1+1)}{6} = \frac{1\cdot2\cdot3}{6} = 1 \quad \checkmark$$

Now we fix an arbitrary $n \geq 1$ and assume that

$$S_2(n) = \frac{n(n+1)(2n+1)}{6}.$$

In this hypothetical case we want to show that we must also have

$$S_n(n+1) = \frac{(n+1)\big((n+1)+1\big)\big(2(n+1)+1\big)}{6}$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}.$$

To show this we note that

$$S_n(n+1) = \left(1^2 + \cdots + n^2\right) + (n+1)^2$$

$$= S_2(n) + (n+1)^2$$

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

$$= (n+1)\left[\frac{n(2n+1)}{6} + (n+1)\right]$$

$$= \frac{(n+1)}{6}\left[n(2n+1) + 6(n+1)\right]$$

$$= \frac{(n+1)}{6}\left[2n^2 + n + 6n + 6\right]$$

$$= \frac{(n+1)}{6}\left[2n^2 + 7n + 6\right]$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}.$$ ✓

We are done by induction.

[(1) The formula starts out true.
(2) If the formula is true at some point, then it remains true after that.]

Problem: Solve the recurrence

$$\boxed{\begin{array}{l} \bullet\ f_0 = 1 \\ \bullet\ f_n = f_{n-1} + n^2 + n \quad \text{for } n \geq 1 \end{array}}$$

Solution: We have.

$$f_0 = 1$$
$$f_1 = 1 + 1^2 + 1$$
$$f_2 = 1 + 1^2 + 1 + 2^2 + 2$$

$$f_3 = 1 + 1^2 + 1 + 2^2 + 2 + 3^2 + 3$$

$\vdots$

$$f_n = 1 + 1^2 + 1 + 2^2 + 2 + 3^2 + 3 + \cdots + n^2 + n$$

$$= 1 + (1 + 2 + 3 + \cdots + n) + (1^2 + 2^2 + 3^2 + \cdots + n^2)$$

$$= 1 + \frac{n(n+1)}{2} + \frac{n(n+1)(2n+1)}{6}$$

$$= 1 + \frac{1}{2}n^2 + \frac{1}{2}n + \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

$$= \frac{1}{3}n^3 + n^2 + \frac{2}{3}n + 1$$

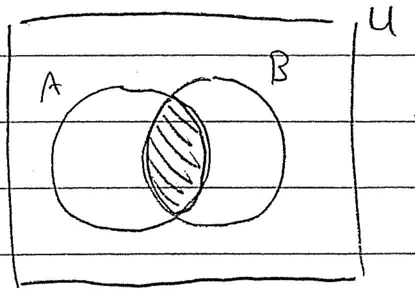
Given sets $A, B \subseteq U$ recall the Boolean set operations

$$A \cap B := \{ x \in U : x \in A \overset{\text{"AND"}}{\wedge} x \in B \}$$

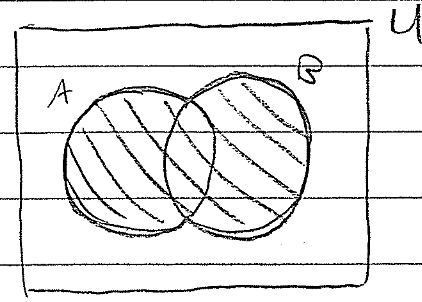
$$A \cup B := \{ x \in U : x \in A \overset{\text{"OR"}}{\vee} x \in B \}$$

$$A^c := \{ x \in U : \overset{\text{"NOT"}}{\neg}\, x \in A \}$$

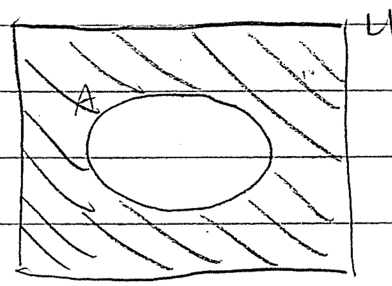
We can draw these sets with Venn diagrams



$A \cap B$



$A \cup B$



A^c

We can use Venn diagrams to prove basic properties of $\cap$, $\cup$, ^{c}.

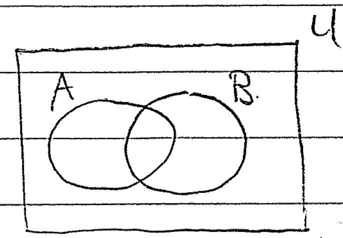
Example: Use Venn diagrams to show that for all sets $A, B \subseteq U$ we have

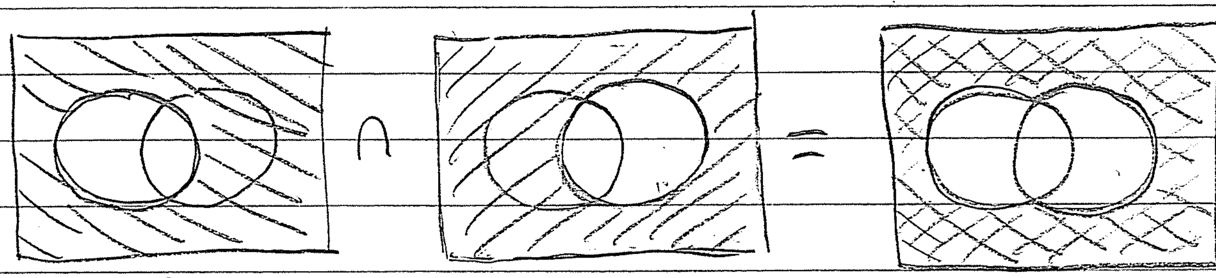
$$(A \cup B)^c = A^c \cap B^c.$$

[Remark: This is called

"de Morgan's identity"]

Proof: consider





$A^c \qquad\qquad B^c \qquad\qquad (A \cup B)^c$

We can also think about Venn diagrams as truth tables.

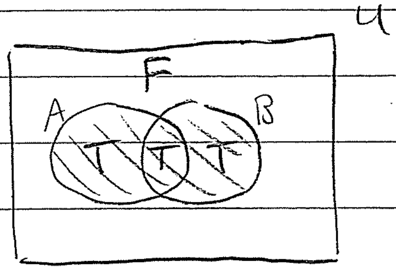
Let $P =$ "$x \in A$" and $Q =$ "$x \in B$", so that

$P \wedge Q =$ "$x \in A$ AND $x \in B$" $=$ "$x \in A \cap B$"
$P \vee Q =$ "$x \in A$ OR $x \in B$" $=$ "$x \in A \cup B$"
$\neg P \wedge Q =$ "$x \notin A$ AND $x \in B$" $=$ "$x \in A^c \cap B$"
$P \wedge \neg Q =$ "$x \in A$ AND $x \notin B$" $=$ "$x \in A \cap B^c$"

$\vdots$

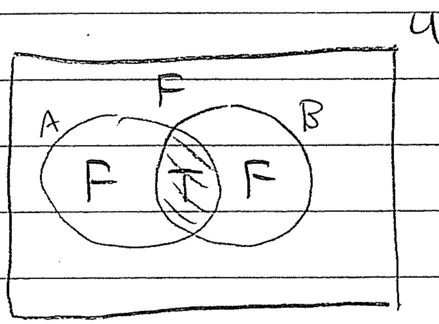
etc.

Examples :



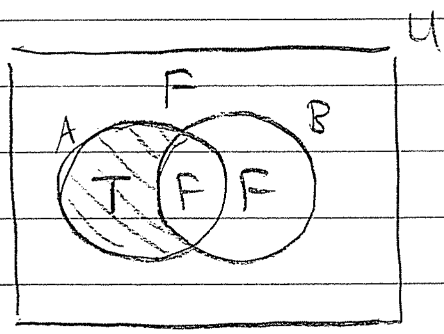
$A \cup B$

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F



$A \cap B$

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F



$A \cap B^c$

P	Q	$P \wedge \neg Q$
T	T	F
T	F	T
F	T	F
F	F	F

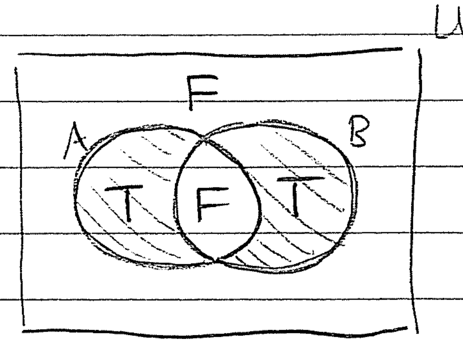
Problem: Let P, Q be logical statements and let $\varphi(P,Q)$ be the logical statement defined by the following truth table

P	Q	$\varphi(P,Q)$
T	T	F
T	F	T
F	T	T
F	F	F

Find a formula for $\varphi(P,Q)$ in terms of the Boolean operations $\wedge, \vee, \neg$.

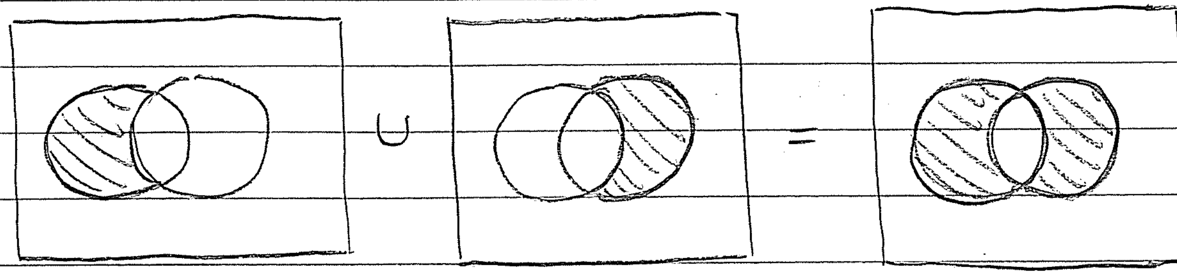
Solutions: It helps to consider the associated Venn diagram.

If $P = $ "$x \in A$" and $Q = $ "$x \in B$" then we have



$\varphi(P,Q)$

What set does this correspond to?



$A \cap B^c$ $\quad\cup\quad$ $A^c \cap B$ $\quad=\quad$ $(A \cap B^c) \cup (A^c \cap B)$.

We conclude that

$$\begin{aligned}\varphi(P,Q) &= \text{“}x \in (A \cap B^c) \cup (A^c \cap B)\text{”} \\ &= \text{“}x \in A \cap B^c \vee x \in A^c \cap B\text{”} \\ &= \text{“}(x \in A \wedge \neg x \in B) \vee (\neg x \in A \wedge x \in B)\text{”} \\ &= (P \wedge \neg Q) \vee (\neg P \wedge Q).\end{aligned}$$

“(P AND NOT Q) OR (NOT P AND Q)”

Let's check that the formula works by building it up piece by piece.

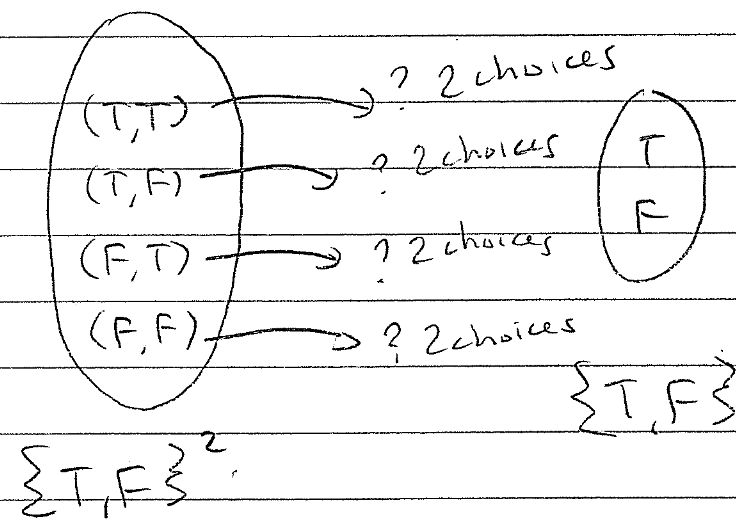
P	Q	$\neg P$	$\neg Q$	$P \wedge \neg Q$	$\neg P \wedge Q$	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$
T	T	F	F	F	F	F
T	F	F	T	T	F	T
F	T	T	F	F	T	T
F	F	T	T	F	F	F

✓

Let $P, Q \in \{T, F\}$ be logical statements. We can think of a statement $\varphi(P,Q) \in \{T,F\}$ as a <u>function</u> from the set

$$\{T,F\}^2 := \{(T,T), (T,F), (F,T), (F,F)\}$$

to the set $\{T,F\}$:



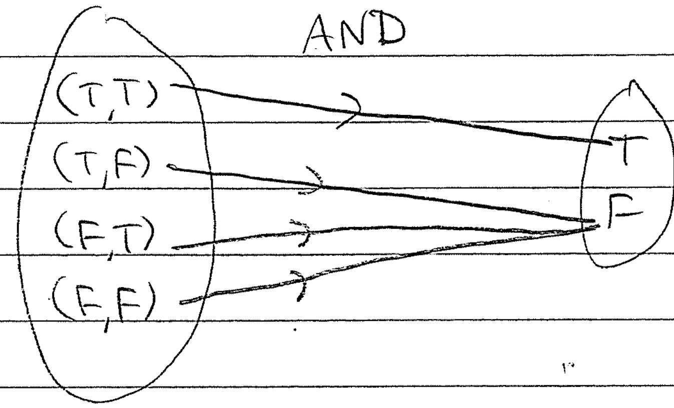
How many such functions are there?

Each arrow has 2 choices for its target so the total number of choices is

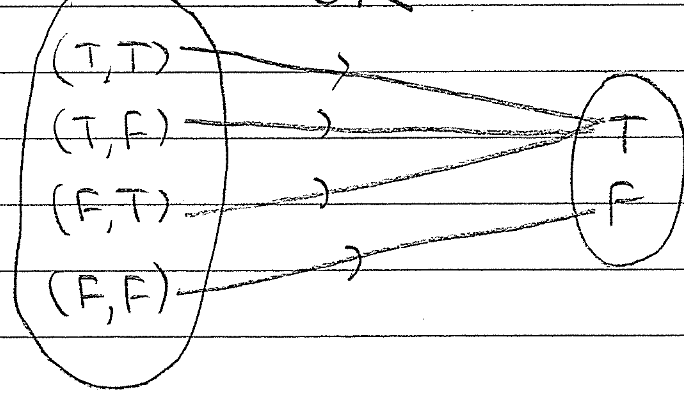
$$2 \times 2 \times 2 \times 2 = 2^4 = 16.$$

We have named two of these functions:

AND



OR



Most of the other 14 also have names. We'll see them later.

You should also remember the definitions of injective/surjective/bijective functions.

Review for Final Exam

Part 2:

- "Abstract" Boolean Algebra
  - proving formulas using algebraic manipulation instead of Venn diagrams or truth tables. (e.g. using de Morgan's Law)

- Properties of the Boolean functions

  $\oplus$, $\Rightarrow$, $\Leftrightarrow$, $\uparrow$,

- Basic Notions of counting
  - Let A, B be finite sets. The size of the Cartesian product is

$$\#(A \times B) = \#A \times \#B$$

- The number of functions from A to B is

$$\# B^{\# A}$$

<u>Example</u>: The number of Boolean functions in n variables,

$$\varphi : \{T, F\}^n \to \{T, F\},$$

is $\#\{T,F\}^{\#(\{T,F\}^n)} = \#\{T,F\}^{(\#\{T,F\})^n}$

$$= 2^{2^n}.$$

- Subsets of U = Functions $U \to \{T, F\}$.

There is a natural bijection between subsets of U and functions $U \to \{T, F\}$ given by sending the subset $A \subseteq U$ to the function $f_A : U \to \{T, F\}$ defined by

$$f_A(x) = \begin{cases} T & x \in A \\ F & x \notin A \end{cases}$$

The inverse sends the function $f : U \to \{T, F\}$ to the subset

$$\{x \in U : f(x) = T\}.$$

We conclude that the number of subsets of U equals the number of functions $U \to \{T, F\}$, i.e.,

$$\#\{T, F\}^{\# U} = 2^{\# U}.$$

- Subsets = Binary Strings.

We can also encode a subset $A \subseteq U$ as a binary string with $\# A$ "1"s and $\# U - \# A$ "0"s.

Example

$$\{2, 6, 7\} \subseteq \{1, \ldots, 7\} \leftrightarrow 0100011$$

- Counting Subsets

Let $\# \mathcal{U} = n$. The total # of subsets of $\mathcal{U}$ is 2^n, but how many subsets of each size?

Let $\binom{n}{k}$ = # subsets of size k.

☆ <u>Theorem</u>: $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

<u>Proof</u>: Instead we count binary strings of length n with k "1"s. By counting the permutations of symbols

$$1_1, 1_2, \ldots, 1_k, 0_1, 0_2, \ldots, 0_{n-k}$$

in <u>two different ways</u>, we find that

$$n! = \binom{n}{k} \cdot k!(n-k)!$$

Hence

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

//

- The Binomial Theorem
  - says that for all numbers a & b and all integers $n \geq 0$, we have

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

- Pascal's Triangle.
  - is defined by the following recurrence

$$\boxed{\begin{array}{l} \bullet\ f(0,k) = \begin{cases} 1 & k=0 \\ 0 & k\neq 0 \end{cases} \\[2ex] \bullet\ f(n,k) = f(n-1,k) + f(n-1,k-1) \quad \forall\, n,k \in \mathbb{Z},\ n \geq 1 \end{array}}$$

$k =$ 0 1 2 3 4 . . .

$n = 0$ 0 0 0 0 1 0 0 0 0

1   0 0 0 1 1 0 0 0

2   0 0 1 2 1 0 0

3   0 1 3 3 1 0

4   1 4 6 4 1

etc.

Theorem : $f(n,k) = \binom{n}{k}$.

This is proved in two steps

1. Show that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

2. Use induction to show that
$$f(n,k) = \binom{n}{k}.$$

Discussion of HW 4 :

A standard deck of cards contains 26 red and 26 black cards.

A "hand" of cards consists of 5 cards.

The number of possible hands is

$$\binom{52}{5} = \frac{52!}{5!\,47!} = \frac{52 \cdot 51 \cdot \overset{10}{\cancel{50}} \cdot 49 \cdot \overset{2}{\cancel{48}} \cdot 47!}{\cancel{5} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1 \cdot 47!}$$

$$= 52 \cdot 51 \cdot 10 \cdot 49 \cdot 2 = 2{,}598{,}960.$$

The number of hands with 2 red and 3 black cards is

$$\binom{26}{2}\binom{26}{3} = \frac{26!}{2!\,24!}\,\frac{26!}{3!\,23!}$$

choose 2 red cards

choose 2 black cards

$$= \frac{\overset{13}{\cancel{26}}\cdot 25}{\cancel{2}}\cdot\frac{\overset{13}{\cancel{26}}\cdot 25\cdot \overset{8}{\cancel{24}}}{\cancel{3}\cdot\cancel{2}}$$

$$= 13\cdot 25\cdot 13\cdot 25\cdot 8$$

$$= 845{,}000.$$

In general, the number of hands with k red cards and $5-k$ black cards is

$$\binom{26}{k}\binom{26}{5-k}$$

choose k red cards

choose $n-k$ black cards.

Since every hand has <u>some</u> number of red cards, we get

$$\binom{52}{5} = \sum_k \binom{26}{k}\binom{26}{5-k}.$$

$$= \binom{26}{0}\binom{26}{5} + \binom{26}{1}\binom{26}{4} + \binom{26}{2}\binom{26}{3}$$

$$+ \binom{26}{3}\binom{26}{2} + \binom{26}{4}\binom{26}{1} + \binom{26}{5}\binom{26}{0}$$

More generally, suppose we have a deck of cards with R red cards and B black cards, and suppose a "hand" consists of n cards.

The total # of possible hands is

$$\binom{R+B}{n}.$$

The number of hands with k red cards is

$$\binom{R}{k}\binom{B}{n-k}$$

choose k red cards — choose $n-k$ black cards

Since every hand has <u>some</u> number of red cards we get

$$\binom{R+B}{n} = \underbrace{\sum_k \binom{R}{k}\binom{B}{n-k}}_{\text{some terms may be zero if } R<n \text{ or } B<n.}$$

<u>Example</u>: $R=2$, $B=4$, $n=4$.

$$\binom{2+4}{4} = \binom{2}{0}\binom{4}{4} + \binom{2}{1}\binom{4}{3} + \binom{2}{2}\binom{4}{2} + \binom{2}{3}\binom{4}{1} + \binom{2}{4}\binom{4}{0}$$

$$15 = 1\cdot 1 + 2\cdot 4 + 1\cdot 6 + 0\cdot 4 + 0\cdot 1$$

$$15 = 1 + 8 + 6 + 0 + 0 \qquad ✓$$

Later we will interpret this in terms of probability: Suppose you are dealt 4 cards from a deck with 2 red and 4 black cards.

What is the <u>probability</u> that you get exactly one red card?

P(one red card)

$$= \frac{\text{\# ways to get one red card}}{\text{total \# possible hands}}$$

$$= \frac{\binom{2}{1}\binom{4}{3}}{\binom{6}{4}} = \frac{2 \cdot 4}{15} = \frac{8}{15} = 0.5333\ldots$$

The probability of getting exactly one red card is 53.3%

Review for Final Exam

Part 3: Properties of Z

- Theorem: Given $a, b, q, r \in \mathbb{Z}$ with $a = qb + r$ we have that

$$\gcd(a, b) = \gcd(b, r)$$

Proof: Show that the sets of common divisors are equal.

$$\mathrm{Div}(a, b) = \mathrm{Div}(b, r),$$

hence their max. elements are equal.
(This was Problem 1 on Exam 1) ///

- Euclidean Algorithm.

Apply the previous theorem to compute greatest common divisors

Example: Compute gcd(12, 7).

$$\begin{array}{ll} & \gcd(12,7) \\ 12 = 1\cdot 7 + 5 & = \gcd(7,5) \\ 7 = 1\cdot 5 + 2 & = \gcd(5,2) \\ 5 = 2\cdot 2 + 1 & = \gcd(2,1) \\ 2 = 2\cdot 1 + 0 & = \gcd(1,0) = 1 \end{array}$$

- Extended Euclidean Algorithm.

We can extend the algorithm to solve for $x, y \in \mathbb{Z}$ in the equation

$$ax + by = d, \quad a, b, d \in \mathbb{Z}.$$

Example: Solve $12x + 7y = 2$.

Consider triples (x, y, r) such that $12x + 7y = r$. There are two obvious triples.

x	y	r
1	0	12
0	1	7

Now apply Euclidean Algorithm

x	y	r	
1	0	12	(1)
0	1	7	(2)
1	-1	5	(3) = (1) - 1(2)
-1	2	2	(4) = (2) - 1(3)
3	-5	1	(5) = (3) - 2(4)
-7	12	0	(6) = (4) - 2(5)

DONE.

Row (5) says.

$$12(3) + 7(-5) = 1.$$

Multiply by 2 to get

$$12(6) + 7(-10) = 2$$

Add k times row (6) to get

$$\begin{array}{rl} & 12(6) + 7(-10) = 2 \\ + & 12(-7k) + 7(12k) = 0 \\ \hline & 12(6-7k) + 7(-10+12k) = 2 \end{array}$$

The general solution to $12x + 7y = 2$ is

$(x, y) = (6 - 7k, -10 + 12k) \ \forall k \in \mathbb{Z}$.

- Bézout's Identity.

Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then $\exists\, x, y \in \mathbb{Z}$ such that

$$ax + by = d.$$

Proof: Extended Euclidean Algorithm ///

- Euclid's Lemma.

Let $p \in \mathbb{Z}$ be prime. Then $\forall a, b \in \mathbb{Z}$,

$$p \mid ab \implies p \mid a \text{ OR } p \mid b.$$

Proof: Assume $p \mid ab$ (say $ab = pk$) and assume $p \nmid a$. We will show that $p \mid b$.

Indeed, we have $\gcd(p, a) = 1$ (why?)

So $\exists\, x, y \in \mathbb{Z}$ with $px + ay = 1$. Multiply both sides by b to get

$$1 = px + ay$$
$$b = pbx + aby$$
$$b = pbx + pky$$
$$b = p(bx + ky) \Rightarrow p \mid b.$$

//

- Every $0 \neq n \in \mathbb{Z}$ can be written as $\pm$ a product of primes.

Proof: Suppose not. Then by Well-Ordering $\exists$ smallest $n \geq 1$ that is not a product of primes. Since n is not prime (why?) $\exists\, 1 < a, b < n$ with

$$n = ab.$$

But since $1 < a, b < n$, both a and b are products of primes. Hence so is n. Contradiction.

//

- Prime Factorization is Unique

Proof: Suppose not. By Well-Ordering, $\exists$ smallest $n > 1$ with two different prime factorizations

(*) $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$.

Since $p_1 \mid n = q_1 q_2 \cdots q_t$, Euclid's Lemma says $p_1 \mid q_i$ for some $1 \le i \le t$. Use cancellation to write

$$n' = \underbrace{p_2 p_3 \cdots p_s = q_1 \cdots q_{i-1} q_{i+1} \cdots q_t}_{\text{still different!}}$$

Now n' is smaller than n, but it still has two different prime factorizations. Contradiction //

Whew!

- Application of Unique Factorization.

Theorem: $\sqrt{2} \notin \mathbb{Q}$.

Proof: Suppose we have $\sqrt{2} = a/b$ with $a, b \in \mathbb{Z}$, hence

(*) $$a^2 = 2b^2.$$

In the prime factorizations of a^2 and b^2, each prime occurs with even multiplicity.

Hence the prime 2 occurs an even # of times on left side of (*) and an odd # of times on the right side of (*).

This contradicts uniqueness. ///

Next: Practice Induction