MAT200: Logic Language and Proof

Lecture 20 - April 19 2021

Problem 4 (10 points)

Let X be any set. Let $\mathrm{Fun}(X \to \{0,1\})$ be the set of all functions from X to $\{0,1\}$.

(a) Suppose $X = \{1,2\}$. List all the elements of $\mathrm{Fun}(X \to \{0,1\})$.

(b) Now let X be a general set again.

For each of the following functions, determine if they are bijections. *Hint: To understand the definitions below, pick concrete examples for X, F and A and try to compute those examples.*

If it is a bijection, prove that your answer is correct by explicitly defining the inverse. If it is not a bijection (or not well defined), explain why not.

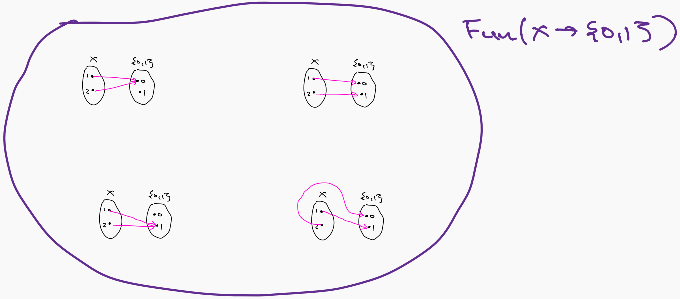
(a) $f_1 : \mathrm{Fun}(X \to \{0,1\}) \to \mathcal{P}(X)$, where $f_1(F) = \{x \in X : F(x) = 1\}$

(b) $f_2 : \mathrm{Fun}(X \to \{0,1\}) \to \mathcal{P}(X)$, where $f_2(F) = \{x \in X : F(x) = 0\}$

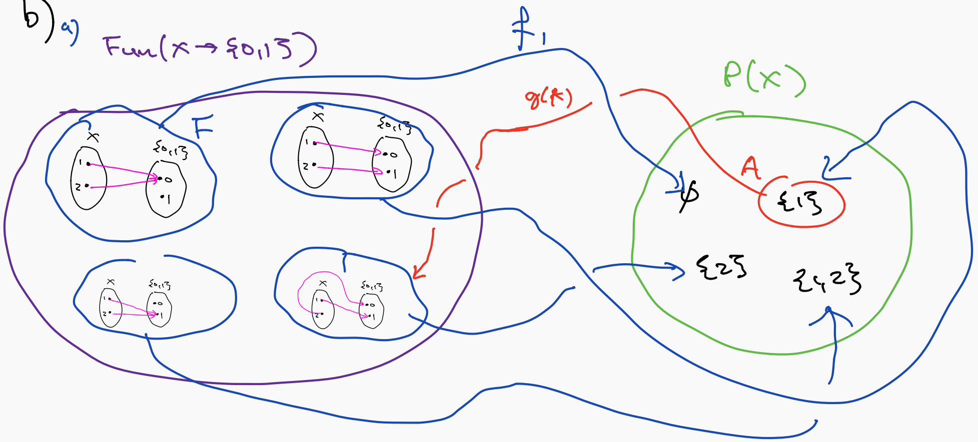
(c) $g : \mathcal{P}(X) \to \mathrm{Fun}(X \to \{0,1\})$ where $g(A)$ is the function

$$g(A) : X \to \{0,1\}, \qquad g(A)(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

a)



b) a)



Last time:

- Proof of irrationality of $\sqrt{2}$
- Could not extend proof to irrationality of $\sqrt{d}$ for d prime
  - (Could not prove the following fact: if a divides d^2 then a divides d.)

Remainder of class:

- Divisibility, primes, etc.

Last time:

- Proof of irrationality of $\sqrt{2}$
- Could not extend proof to irrationality of $\sqrt{d}$ for d prime
  - (Could not prove the following fact: if a divides d^2 then a divides d .)

Remainder of class:

- Divisibility, primes, etc.

Last time we used the following proof:

Theorem (needed for previous proof):
For integer n, if n^2 is divisible by 5, then n is divisible by 5.

Proof:

- Suppose n is not divisible by 5, then $n = 5q + r$ where $1 \leq r \leq 4$.
- Then $n^2 = 25q^2 + 5qr + r^2$.
- Therefore the remainder of n^2 on division by 5 is the same as the remainder of r^2 .
  - There are only 4 possibilities: $r^2 = 1,4,9,16$.
  - In all four possibilities, r^2 not divisible by 5.

How do we know this?

We're using: Every integer n can be written uniquely in the form $n = 5q + r$, where $q \in \mathbb{Z}$, $r \in \{1,2,3,4\}$.

Theorem: Let $a \in \mathbb{Z}, b \in \mathbb{N}$. Then there exists unique $q, r \in \mathbb{Z}$, such that $0 \leq r \leq b$ and $a = bq + r$.

Explanation:

E.g. if $a=7$, $b=2$ then $q=3$, $r=1$

because

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

This the only (q,r) pair that works,

$$7 = 2q + r$$

Only $q=3$, $r=1$ works.

Running example: $a=7$, $b=2$

$$A = \{0, 1, 2, 3, 4, 5, 6, 7 \ldots\}$$

So $A = \{0,1,2,3\}$.

Proof:

Suppose $a \geq 0$, let

$$A = \{k \in \mathbb{Z} : k \geq 0 \text{ and } bk \leq a\}$$

Let

$q = \max A$

$r = a - bq$.

Then

* $r \geq 0$ because $bq \leq a$
* $r < b$, because if not, $a - bq = r \geq b$,

so $a - b(q+1) \geq 0$

so $b(q+1) \leq a$,

which contradicts the fact that $q = \max A$.

So we've found q and r

For uniqueness, suppose

$$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2$$

and suppose $q_1 \geq q_2$ (otherwise we could switch labels).

$$0 \leq r_1 = a - bq_1 \leq a - bq_2 = r_2 < b.$$

so $0 \leq (a - bq_2) - (a - bq_1) < b$

so $0 \leq b(q_1 - q_2) < b$.

So $0 \leq q_1 - q_2 < 1$, so $q_1 - q_2 = 0$. QED.

Theorem: Let n be an integer and suppose n is a perfect square. Then there exists $p \in \mathbb{Z}$ such that $n = 3p$ or $3p + 1$.

Examples:

$36 = 3 \cdot 12$

$49 = 3 \cdot 16 + 1$

$100 = 3 \cdot 33 + 1$

$n^2 = 3q + 2$ impossible.

Proof: Suppose n is a perfect square, then $n = a^2$ for some integer a.

a) There are 3 cases:

* if $a = 3q$, $a^2 = 9q^2$ $\Rightarrow n = 3\underbrace{(3q^2)}_{p}$

* if $a = 3q+1$, $a^2 = 9q^2 + 6q + 1$ $\Rightarrow n = 3\underbrace{(3q^2 + 2q)}_{p} + 1$

* if $a = 3q + 2$, $a^2 = 9q^2 + 12q + 4$ $\Rightarrow n = 3\underbrace{(q^2 + 4q + 1)}_{p} + 1$

QED.

By division theorem

(We don't have to worry about $a = 3q + 7$) $a = 3q + 8$ etc.

where $0 \le r < b$

- Suppose $a = bq + r$. Then r is said to be the *remainder when a is divided by q.*
- $q\,|\,a$ means q divides a, that is (there exists $b \in \mathbb{Z}$ such that $a = qb$).
- $a \nmid b$ means a does not divide b.
- " $a \equiv b \mod m$ " means $m\,|\,(a - b)$.

Example:

What is remainder when -7 divided 3?

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

$= -3 \cdot 3 + 2$

remainder:

a) -1

b) 2

a) Yes

b) No.

Examples:

$3 \equiv 7 \mod 4$

$(3-7 = -4$ and $4 | -4)$

$3 \equiv 103 \mod 4$

$(3-103 = -100$ and $4 | -100)$.

$a \equiv 0 \mod m$ means $m | a$

because $a - 0 = a$.

Theorem: If r is the remainder of a divided by q, then $a \equiv r \mod q$.

Proof: Will be on the homework.

Examples:

$7 = 2 \cdot 3 + 1$

q

remainder.

$7 \equiv 1 \mod 3$

Check: $7 - 1 = 6$, $3 | 6$.

- Suppose $a = bq + r$. Then r is said to be the *remainder when a is divided by q.*
- $q \mid a$ means q divides a, that is (there exists $b \in \mathbb{Z}$ such that $a = qb$).
- $a \nmid b$ means a does not divide b.
- $a \equiv b \mod m$ means $m \mid (a - b)$.

GCD

Suppose $(a, b) \in \mathbb{Z}^2 - \{(0,0)\}$

The greatest common divisor of a and b is the unique positive integer d such that

1) d is a common divisor: $d \mid b$ and $d \mid a$

2) d is larger than any other common divisor: If $c \mid a$ and $c \mid b$ then $c \leq d$

We use gcd(a,b) to denote the gcd of a and b.

Example: $\gcd(6, 15) = 3$

Check: 1) $3 \mid 6$ and $3 \mid 15$ ✓

2) Divisors of 6 : 1, 2, 3, 6 $\quad 1 \leq 3$ ✓

Divisors of 15 : 1, 3, 5, 15

Is gcd even well defined?

- What if there are no common divisors? ← 1 is always a common divisor.
- What if there is no largest common divisor?

Possible bad behaviour:

1 is a common divisor of a, b
2 is a common divisor of a, b
3 is a common divisor of a, b
4 is a common divisor of a, b.

This can't happen because a divisor of a is always less than a.
⋮
There's only finitely many divisors.

How to find gcd of 11033442 and 1102246?

Lemma 16.1.1: If $b \mid a$ then gcd(a,b)=b (1)

Lemma 16.1.2: For $(a, b) \neq (0,0)$, if $a = bq + r$, then $gcd(a, b) = gcd(b, r)$ (2)

Example application:

$$\gcd(72, 30) = \gcd(30, 12) \quad \text{by (2)}$$
$$= \gcd(12, 6) \quad \text{by (2)}$$
$$= 6 \quad \text{by (1).}$$

Example application:

~~gcd(72, 30)=~~

$$\gcd(232, 136) \stackrel{(2)}{=} \gcd(136, 96) \qquad 232 = 136 \times 1 + 96$$
$$\stackrel{(2)}{=} \gcd(96, 40)$$
$$\stackrel{(2)}{=} \gcd(40, 16)$$
$$\stackrel{(2)}{=} \gcd(16, 8)$$
$$\stackrel{(1)}{=} 8$$

Does this always work?

Do we always end up applying (1)?

Finding the gcd in this way is called the Euclidean algorithm.

Lemma 16.1.1: If $b \mid a$ then gcd(a,b)=b

Proof:

b is a common divisor:

$b \mid b$ and $b \mid a$.

Any common divisor c of a and b must be a divisor of b, so $c \leq b$.

So b is the largest common divisor.

Lemma 16.1.2: For $(a, b) \neq (0,0)$, if $a = bq + r$, then $gcd(a, b) = gcd(b, r)$

Next time.