CS311H
Discrete Math for CS: Honors

Prof: Peter Stone
TA: Matthew Hausknecht
Proctor: Sudheesh Katkam

Department of Computer Science
The University of Texas at Austin

Good Morning, Colleagues

Good Morning, Colleagues

Are there any questions?

Logistics

- Keeping up and posting on piazza is **required**

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*
  - But we've shown some fully formal examples
  - On HW and test you need to be fully formal

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*
  - But we've shown some fully formal examples
  - On HW and test you need to be fully formal
  - If you're not sure what that means, go to office hours

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*
  - But we've shown some fully formal examples
  - On HW and test you need to be fully formal
  - If you're not sure what that means, go to office hours
- If you need a nametag, email me

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*
  - But we've shown some fully formal examples
  - On HW and test you need to be fully formal
  - If you're not sure what that means, go to office hours
- If you need a nametag, email me
- Bring in chairs?

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*
  - But we've shown some fully formal examples
  - On HW and test you need to be fully formal
  - If you're not sure what that means, go to office hours
- If you need a nametag, email me
- Bring in chairs? (but then return them)

Logistics

- Keeping up and posting on piazza is **required**
- Due to time constraints, some proofs in the videos and class aren't fully formal: *proof sketches*
  - But we've shown some fully formal examples
  - On HW and test you need to be fully formal
  - If you're not sure what that means, go to office hours
- If you need a nametag, email me
- Bring in chairs? (but then return them)
- Second homework **due at start of class**

Some questions

- How do you do proof by exhaustive cases?

Some questions

- How do you do proof by exhaustive cases?
  - First establish all the *possible* solutions

Some questions

- How do you do proof by exhaustive cases?
  - First establish all the *possible* solutions
  - Then examine them one by one

Prove that. . .

- Every odd integer is the difference of two squares using **direct proof**.

Prove that. . .

- Every odd integer is the difference of two squares using **direct proof**.
  - Is the converse true? That is, is the difference of two squares always an odd integer?

Prove that...

- Every odd integer is the difference of two squares using **direct proof**.
  - Is the converse true? That is, is the difference of two squares always an odd integer?

Prove by Contradiction

- There are no positive integer solutions to equation $x^2 - y^2 = 1$

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.
6. Combining 4 and 5, $d(q - q') > r' - r$

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.
6. Combining 4 and 5, $d(q - q') > r' - r$— Contradicts 3.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.
6. Combining 4 and 5, $d(q - q') > r' - r$— Contradicts 3.
7. Therefore $q = q'$ (step 2)

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.
6. Combining 4 and 5, $d(q - q') > r' - r$— Contradicts 3.
7. Therefore $q = q'$ (step 2) $\Rightarrow r' - r = 0$ (step 3).

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.
6. Combining 4 and 5, $d(q - q') > r' - r$— Contradicts 3.
7. Therefore $q = q'$ (step 2) $\Rightarrow r' - r = 0$ (step 3).
8. Therefore $r = r'$.

Uniqueness of Quotients and Remainders

Thm: Let a be an integer, d positive integer. Then there are *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$

d is divisor, q quotient, r remainder.
Will just prove uniqueness, you can try existence

1. Assume $\exists q, r, q', r'$ where this holds.
2. Assume $q \neq q'$. then WLOG assume $q > q'$.
3. Then we have $d(q - q') = (r' - r)$.
4. Since $q > q'$ we have $d(q - q') \geq d$. (Both are integers)
5. Since $d > r'$ and $r \geq 0$ we have that $d > r' - r$.
6. Combining 4 and 5, $d(q - q') > r' - r$— Contradicts 3.
7. Therefore $q = q'$ (step 2) $\Rightarrow r' - r = 0$ (step 3).
8. Therefore $r = r'$.QED.

Prove:

- Between every two rational numbers there is an irrational number.

Prove:

- Between every two rational numbers there is an irrational number.
- $(1/2) \times (3/4) \times (5/6) \times ... \times (99/100) < (1/10)$

Prove:

- Between every two rational numbers there is an irrational number.

- $(1/2) \times (3/4) \times (5/6) \times ... \times (99/100) < (1/10)$
  1. Define $A = (1/2) \times (3/4) \times (5/6) \times ... \times (99/100)$.

Prove:

- Between every two rational numbers there is an irrational number.

- $(1/2) \times (3/4) \times (5/6) \times \ldots \times (99/100) < (1/10)$
  1. Define $A = (1/2) \times (3/4) \times (5/6) \times \ldots \times (99/100)$.
  2. Define $B = (2/3) \times (4/5) \times (6/7) \times \ldots \times (98/99) \times 1$.

Prove:

- Between every two rational numbers there is an irrational number.

- $(1/2) \times (3/4) \times (5/6) \times ... \times (99/100) < (1/10)$
  1. Define $A = (1/2) \times (3/4) \times (5/6) \times ... \times (99/100)$.
  2. Define $B = (2/3) \times (4/5) \times (6/7) \times ... \times (98/99) \times 1$.
  3. Each of these consists of 50 terms, and each term in B is larger than the corresponding term in A.

Prove:

- Between every two rational numbers there is an irrational number.

- $(1/2) \times (3/4) \times (5/6) \times ... \times (99/100) < (1/10)$
  1. Define $A = (1/2) \times (3/4) \times (5/6) \times ... \times (99/100)$.
  2. Define $B = (2/3) \times (4/5) \times (6/7) \times ... \times (98/99) \times 1$.
  3. Each of these consists of 50 terms, and each term in B is larger than the corresponding term in A.
  4. Therefore $A < B \Rightarrow A^2 < AB$.

Prove:

- Between every two rational numbers there is an irrational number.

- $(1/2) \times (3/4) \times (5/6) \times ... \times (99/100) < (1/10)$
  1. Define $A = (1/2) \times (3/4) \times (5/6) \times ... \times (99/100)$.
  2. Define $B = (2/3) \times (4/5) \times (6/7) \times ... \times (98/99) \times 1$.
  3. Each of these consists of 50 terms, and each term in B is larger than the corresponding term in A.
  4. Therefore $A < B \Rightarrow A^2 < AB$.
  5. $AB = (1/2) \times (2/3) \times (3/4) \times (4/5) \times (5/6) \times (6/7) \times ... \times (98/99) \times (99/100) \times 1 = 1/100$.

Prove:

- Between every two rational numbers there is an irrational number.

- $(1/2) \times (3/4) \times (5/6) \times ... \times (99/100) < (1/10)$
  1. Define $A = (1/2) \times (3/4) \times (5/6) \times ... \times (99/100)$.
  2. Define $B = (2/3) \times (4/5) \times (6/7) \times ... \times (98/99) \times 1$.
  3. Each of these consists of 50 terms, and each term in B is larger than the corresponding term in A.
  4. Therefore $A < B \Rightarrow A^2 < AB$.
  5. $AB = (1/2) \times (2/3) \times (3/4) \times (4/5) \times (5/6) \times (6/7) \times ... \times (98/99) \times (99/100) \times 1 = 1/100$.
  6. So, $A^2 < 1/100 \Rightarrow A < 1/10$.

Prove that...

- Show that there is no rational number r for which $r^3 + r + 1 = 0$

Prove by direct proof:

- If a and b are real numbers, then $a^2 + b^2 \geq 2ab$.

Prove by direct proof:

- If a and b are real numbers, then $a^2 + b^2 \geq 2ab$.
- (Tricky problem) The number $100...01$ (with $3n - 1$ zeros where n is positive integer) is not a prime. (Hint: using identity $x^3 + 1 = (x + 1)(x^2 - x + 1)$.

Assignments for Tuesday

- Second homework **due at start of class**
- Modules 7,8 with associated readings

Assignments for Tuesday

- Second homework **due at start of class**
- Modules 7,8 with associated readings