Mini-Quiz Mar. 2

Your name: Michael Plasmeier

Circle the name of your TA:

Ali   Nick   Oscar   (Oshani)

- This quiz is **closed book**. Total time is 25 minutes.
- Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Please keep your entire answer to a problem on that problem's page.
- GOOD LUCK!

T/R

DO NOT WRITE BELOW THIS LINE

Problem	Points	Grade	Grader
1	5	5	AK
2	5	0	AK
3	5	2	AK
4	5	0	NS
Total	20	7	NS

Problem 1 (5 points).
Set equalities such as the one below can be proved with a chain of *iff*s starting with "$x \in$ left-hand-set" and ending with "$x \in$ right-hand-set," as done in class and the text. A key step in such a proof involves invoking a propositional equivalence. State a propositional equivalence that would do the job for this set equality:

$$\overline{A - B} = (\overline{A} - \overline{C}) \cup (B \cap C) \cup ((\overline{A} \cup B) \cap \overline{C})$$

Do not simplify or prove the propositional equivalence you obtain.

For example, to prove $A \cup (B \cap A) = A$, we would have the following "iff chain":

$x \in A \cup (B \cap A)$ iff $x \in A$ OR $x \in (B \cap A)$
iff $x \in A$ OR ($x \in B$ AND $x \in A$)
iff $x \in A$ (Since P OR (Q AND P) is equivalent to P.)

5

$x \in \overline{A - B}$ IFF $x \notin A - B$
IFF NOT($x \in A$ AND $x \notin B$)

$x \in (\overline{A} - \overline{C})$ IFF $x \notin A$ AND NOT($x \in C$)
$x \in (B \cap C)$ IFF $x \in B$ And $x \in C$
$x \in ((\overline{A} \cup B) \cap \overline{C})$ IFF ($x \notin A$ or $x \in B$) AND $x \notin C$)

right side = ($x \notin A$ AND $x \in C$) or [$x \in B$ AND $x \in C$)
Or (($x \notin A$ or $x \in B$) And ($x \notin C$)

See online solution.

Problem 2 (5 points).
Let A and B denote two countably infinite sets:

$$A = \{a_0, a_1, a_2, a_3, \ldots\}$$
$$B = \{b_0, b_1, b_2, b_3, \ldots\}$$

✓ programatically ?

Show that their product, $A \times B$, is also a countable set by showing how to list the elements of $A \times B$. You need only show enough of the initial terms in your sequence to make the pattern clear — a half dozen or so terms usually suffice.

$A \times B = f(a(), b())$

(a_0, b_0)	(a_1, b_0)	(a_2, b_0)	$(a_{\ldots}, b_0)$
(a_0, b_1)	(a_1, b_1)	(a_2, b_1)	$(a_{\ldots}, b_1)$
(a_0, b_2)	(a_1, b_2)	(a_2, b_2)	$(a_{\ldots}, b_2)$
$(a_0, b_{\ldots})$	$(a_0, b_{\ldots})$	$(a_2, b_{\ldots})$	$(a_{\ldots}, b_{\ldots})$

Build matrix like this
Matrix of ∞ size

We want a list, not a matrix!

These are contable, because each a_0, b_0 is Countable

⓪

well then just read across... Silly
- went over in review session
- but should be partial at least

Good student

Problem 3 (5 points).
The nth Fibonacci number, F_n, is defined recursively as follows:

$$F_n = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F_{n-1} + F_{n-2} & \text{if } n \geq 2 \end{cases}$$

These numbers satisfy many unexpected identities, such as

$$F_0^2 + F_1^2 + \cdots + F_n^2 = F_n F_{n+1} \tag{1}$$

Equation (1) can be proved to hold for all $n \in \mathbb{N}$ by induction, using the equation itself as the induction hypothesis, $P(n)$.

Hyp: $P(n) = F_0^2 + F_1^2 + \ldots + F_n^2 = F_n F_{n+1}$

(a) Prove the **base case** ($n = 0$).

$F_n = 0$

$F_0^2 = F_0 F_1$

$0^2 = 0 \cdot 1$

$0 = 0$

(2)

(b) Now prove the **inductive step**.

?

$F_0^2 + F_1^2 + \ldots + F_n^2 + (F_{n+1})^2 = F_n F_{n+1} (F_{n+1})$

$F_0^2 + F_1^2 + (F_{n-1} + F_{n-2})^2 + (F_n + F_{n-1})^2 = F_n (F_{n+1})^2$

$\ldots + F_{n-1}^2 + F_{n-1}F_{n-2} + F_{n-2}^2 + \frac{F_n^2 + F_n F_{n-1}}{F_n} + (F_{n-1})^2 = \frac{F_n (F_{n+1})}{F_n}$

$\ldots + F_n + F_{n-1} + \frac{(F_{n-1})^2}{F_n} = (F_{n+1})^2$

Shift time

$\frac{F_{n-1} + F_{n-2}}{F_n} + \frac{(F_{n-2})^2}{F_{n-1}} = F_n^2$

$F_n + \frac{(F_{n-2})^2}{F_{n-1}} = F_n^2$

(0)

Problem 4 (5 points).

The set, M, of strings of brackets is recursively defined as follows:

Base case: $\lambda \in M$.

Constructor cases: If $s, t \in M$, then

- $[\, s \,] \in M$, and
- $s \cdot t \in M$.

The set, RecMatch, of strings of matched brackets was defined recursively in class. Recall the definition:

Base case: $\lambda \in$ RecMatch.

Constructor case: If $s, t \in$ RecMatch, then $[\, s \,]\, t \in$ RecMatch.

Fill in the following parts of a proof by structural induction that

$$\text{RecMatch} \subseteq M. \tag{2}$$

(a) State an **induction hypothesis** suitable for proving (2) by structural induction.

P(n) ::= RecMatch ⊆ M ∀s,t ∈ M ✗ see sols

If P(b) is true for each base case element b ∈ R for all 2 argument constructors c [P(r) and P(s) ⇒ P(c(r,s))] for all r, s ∈ R then P(c) is true for all r ∈ R

(b) State and prove the **base case(s)**.

✗ Base case s = λ

There are no [] in base case, so base case of RecMatch definition that λ ∈ RecMatch

λ ∈ M ?

(c) Prove the **inductive step**.

✗ If s,t ∈ RecMatch, then [s]t ∈ RecMatch

Proof by cases

[s]t ∈ M

then remove the brackets on the outside, recursively

[s']t ∈ M

then remove brackets on the inside, recursively

want to show [s]t ∈ M,

As a matter of fact, M = RecMatch, though we won't prove this. An advantage of the RecMatch definition is that it is *unambiguous*, while the definition of M is ambiguous.

(d) Give an example demonstrating that M is ambiguously defined.

X We don't know what is in M. It could be an empty set or it could be a set where [ ] do not match. no. see sols.

(e) Briefly explain what advantage unambiguous recursive definitions have over ambiguous ones. (Remember that "ambiguous definition" has a technical mathematical meaning which does not imply that the ambiguous definition is unclear.)

We know that we have proved for all cases. There are no cases that can be considered that might lead to a different outcome. X

did not study end well

Solutions to Mini-Quiz Mar. 2

Problem 1 (5 points).
Set equalities such as the one below can be proved with a chain of *iff*s starting with "$x \in$ left-hand-set" and ending with "$x \in$ right-hand-set," as done in class and the text. A key step in such a proof involves invoking a propositional equivalence. State a propositional equivalence that would do the job for this set equality:

$$\overline{A - B} = (\overline{A} - \overline{C}) \cup (B \cap C) \cup ((\overline{A} \cup B) \cap \overline{C})$$

Do not simplify or prove the propositional equivalence you obtain.

For example, to prove $A \cup (B \cap A) = A$, we would have the following "iff chain":

$$\begin{aligned} x \in A \cup (B \cap A) \quad & \text{iff} \quad x \in A \text{ OR } x \in (B \cap A) \\ & \text{iff} \quad x \in A \text{ OR } (x \in B \text{ AND } x \in A) \\ & \text{iff} \quad x \in A \qquad \text{(since } P \text{ OR } (Q \text{ AND } P) \text{ is equivalent to } P\text{).} \end{aligned}$$

Solution. The stated set equality holds iff membership in $\overline{A - B}$ implies and is implied by membership in $(\overline{A} - \overline{C}) \cup (B \cap C) \cup ((\overline{A} \cup B) \cap \overline{C})$. That is, the set equality holds iff, for all x,

$$x \in \overline{A - B} \quad \text{iff} \quad x \in (\overline{A} - \overline{C}) \cup (B \cap C) \cup ((\overline{A} \cup B) \cap \overline{C}).$$

Define three propositions describing the membership of x in each of the sets A, B, and C:

$$\begin{aligned} P &::= x \in A \\ Q &::= x \in B \\ R &::= x \in C \end{aligned}$$

Now, express membership in $\overline{A - B}$ in terms of P, Q, and R:

$$\begin{aligned} & x \in \overline{A - B} \\ & \quad \text{iff} \quad \text{NOT}(x \in (A \cap \overline{B})) \\ & \quad \text{iff} \quad \text{NOT}(x \in A \text{ AND } x \in \overline{B}) \\ & \quad \text{iff} \quad \text{NOT}(x \in A \text{ AND NOT}(x \in B)) \\ & \quad \text{iff} \quad \text{NOT}(P \text{ AND NOT}(Q)) \end{aligned}$$

Then express membership in

$$(\overline{A} - \overline{C}) \cup (B \cap C) \cup ((\overline{A} \cup B) \cap \overline{C})$$

in terms of P, Q, and R:

$$x \in (\overline{A} - \overline{C}) \cup (B \cap C) \cup ((\overline{A} \cup B) \cap \overline{C})$$

$$\text{iff} \quad x \in (\overline{A} - \overline{C}) \text{ OR } x \in (B \cap C) \text{ OR } x \in ((\overline{A} \cup B) \cap \overline{C})$$

$$\text{iff} \quad x \in \left(\overline{A} \cap \overline{\overline{C}}\right) \text{ OR } x \in (B \cap C) \text{ OR } \left(x \in \left(\overline{A} \cup B\right) \text{ AND } x \in \overline{C}\right)$$

$$\text{iff} \quad x \in \left(\overline{A} \cap C\right) \text{ OR } x \in (B \cap C) \text{ OR } \left(x \in \left(\overline{A} \cup B\right) \text{ AND } x \in \overline{C}\right)$$

$$\text{iff} \quad \left(x \in \overline{A} \text{ AND } x \in C\right) \text{ OR } (x \in B \text{ AND } x \in C) \text{ OR } \left(\left(x \in \overline{A} \text{ OR } x \in B\right) \text{ AND } x \in \overline{C}\right)$$

$$\text{iff} \quad (\text{NOT } (x \in A) \text{ AND } x \in C) \text{ OR } (x \in B \text{ AND } x \in C) \text{ OR } ((\text{NOT } (x \in A) \text{ OR } x \in B) \text{ AND NOT } (x \in C))$$

$$\text{iff} \quad \left(\overline{P} \text{ AND } R\right) \text{ OR } (Q \text{ AND } R) \text{ OR } \left(\left(\overline{P} \text{ OR } Q\right) \text{ AND } \overline{R}\right)$$

So the stated set equality holds if and only if the following two propositional formulas are equivalent

$$\text{NOT } \left(P \text{ AND } \overline{Q}\right)$$

and

$$\left(\left(\overline{P} \text{ AND } R\right) \text{ OR } (Q \text{ AND } R) \text{ OR } \left(\left(\overline{P} \text{ OR } Q\right) \text{ AND } \overline{R}\right)\right).$$

Notice that you were **not** expected to write out a proof like this. We've written this out to remind you how the propositional equivalence would be used in such a proof.

The point is that there is a clear correspondence between the set equality and the needed propositional equivalence in such proofs, and once you've recognized this, you can read off the propositional equivalence from the set equality without having to go through any long derivation.

■

Problem 2 (5 points).
Let A and B denote two countably infinite sets:

$$A = \{a_0, a_1, a_2, a_3, \ldots\}$$
$$B = \{b_0, b_1, b_2, b_3, \ldots\}$$

Show that their product, $A \times B$, is also a countable set by showing how to list the elements of $A \times B$. You need only show enough of the initial terms in your sequence to make the pattern clear — a half dozen or so terms usually suffice.

Solution. The elements of $A \times B$ can be arranged as follows:

$$\begin{array}{ccccc}
(a_0, b_0) & (a_0, b_1) & (a_0, b_2) & (a_0, b_3) & \ldots \\
(a_1, b_0) & (a_1, b_1) & (a_1, b_2) & (a_1, b_3) & \ldots \\
(a_2, b_0) & (a_2, b_1) & (a_2, b_2) & (a_2, b_3) & \ldots \\
(a_3, b_0) & (a_3, b_1) & (a_3, b_2) & (a_3, b_3) & \ldots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Traversing this grid along successive lower-left to upper-right diagonals yields the required list:

$$(a_0, b_0), (a_1, b_0), (a_0, b_1), (a_2, b_0), (a_1, b_1), (a_0, b_2), (a_3, b_0), (a_2, b_1), (a_1, b_2), (a_0, b_3), \ldots$$

Obviously, travelling in the opposite direction along each diagonal yields an equally acceptable list:

$$(a_0, b_0), (a_0, b_1), (a_1, b_0), (a_0, b_2), (a_1, b_1), (a_2, b_0), (a_0, b_3), (a_1, b_2), (a_2, b_1), (a_3, b_0), \ldots$$

■

Problem 3 (5 points).
The nth Fibonacci number, F_n, is defined recursively as follows:

$$F_n = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F_{n-1} + F_{n-2} & \text{if } n \geq 2 \end{cases}$$

These numbers satisfy many unexpected identities, such as

$$F_0^2 + F_1^2 + \cdots + F_n^2 = F_n F_{n+1} \tag{1}$$

Equation (1) can be proved to hold for all $n \in \mathbb{N}$ by induction, using the equation itself as the induction hypothesis, $P(n)$.

(a) Prove the **base case** ($n = 0$).

Solution.

$$\sum_{i=0}^{0} F_i^2 = (F_0)^2 = 0 = (0)(1) = F_0 F_1$$

Therefore, $P(0)$ is true. ■

(b) Now prove the **inductive step**.

Solution. We need to prove that $P(n)$:

$$\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$$

implies $P(n+1)$:

$$\sum_{i=0}^{n+1} F_i^2 = F_{n+1} F_{n+2}$$

Proof.

$$\begin{aligned} \sum_{i=0}^{n+1} F_i^2 &= \sum_{i=0}^{n} F_i^2 + F_{n+1}^2 \\ &= F_n F_{n+1} + F_{n+1}^2 && \text{By } P(n). \\ &= F_{n+1}(F_n + F_{n+1}) \\ &= F_{n+1} F_{n+2} && \text{By the definition of the Fibonacci sequence.} \end{aligned}$$

■

Problem 4 (5 points).
The set, M, of strings of brackets is recursively defined as follows:
Base case: $\lambda \in M$.
Constructor cases: If $s, t \in M$, then

- $[\, s \,] \in M$, and
- $s \cdot t \in M$.

The set, RecMatch, of strings of matched brackets was defined recursively in class. Recall the definition:

Base case: $\lambda \in$ RecMatch.

Constructor case: If $s, t \in$ RecMatch, then $[\,s\,]\,t \in$ RecMatch.

Fill in the following parts of a proof by structural induction that

$$\text{RecMatch} \subseteq M. \tag{2}$$

(a) State an **induction hypothesis** suitable for proving (2) by structural induction.

Solution.

$$P(x) ::= x \in M$$

■

(b) State and prove the **base case(s)**.

Solution. Base case ($x = \lambda$): By definition of M, the empty string is in M.

■

(c) Prove the **inductive step**.

Solution. *Proof.* **Constructor case** ($x = [\,s\,]\,t$ for $s, t \in$ RecMatch): By structural induction hypothesis, we may assume that $s, t \in M$. By the first constructor case of M, it follows that $[s] \in M$. Then, by the second constructor case of M, it follows that $[\,s\,]\,t \in M$.

■

As a matter of fact, $M =$ RecMatch, though we won't prove this. An advantage of the RecMatch definition is that it is *unambiguous*, while the definition of M is ambiguous.

(d) Give an example demonstrating that M is ambiguously defined.

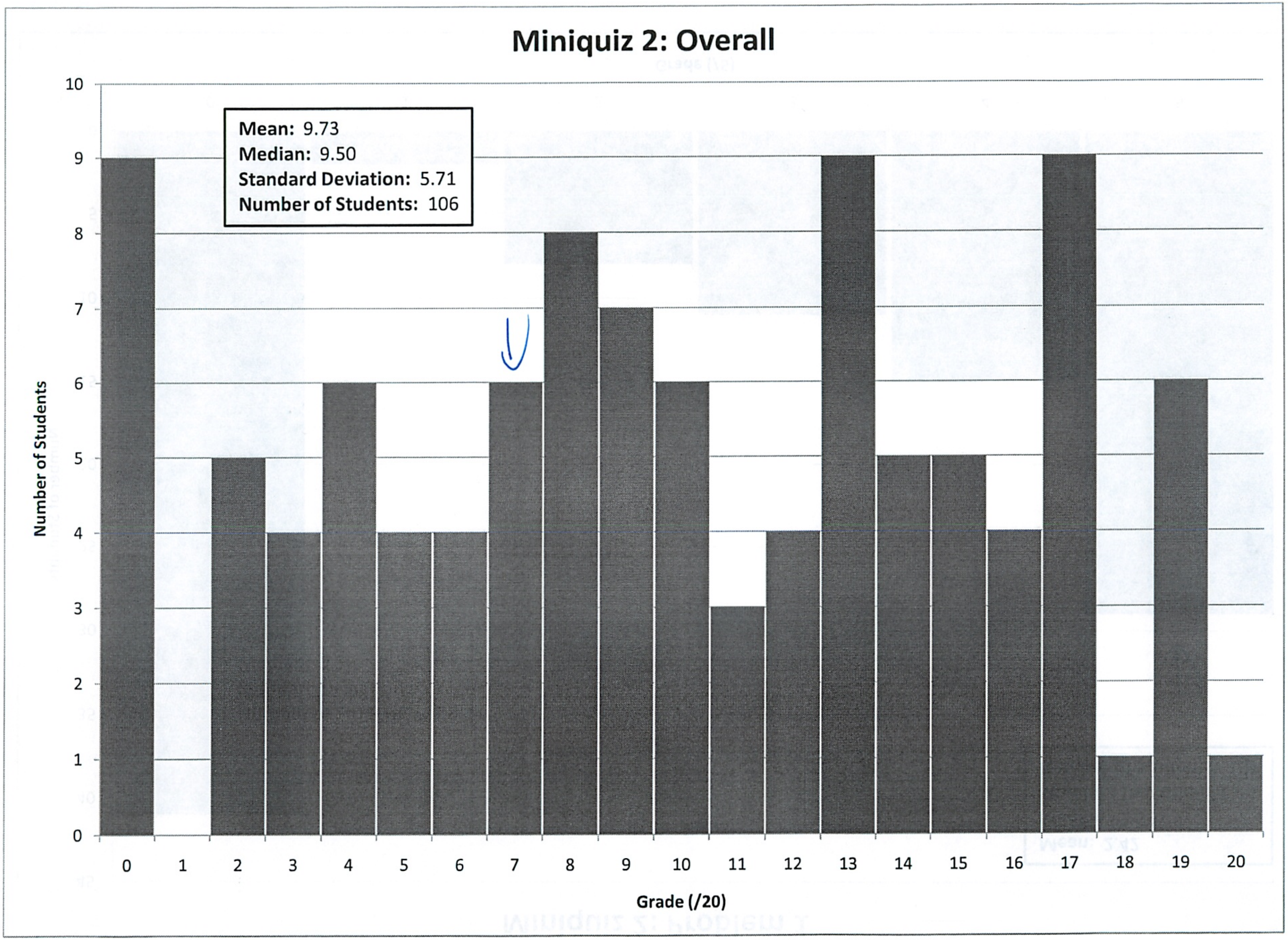
Solution. Consider derivations of the empty string. This could be derived directly from the base case λ, or by starting with λ and then constructing $\lambda\lambda$ through the second constructor case.

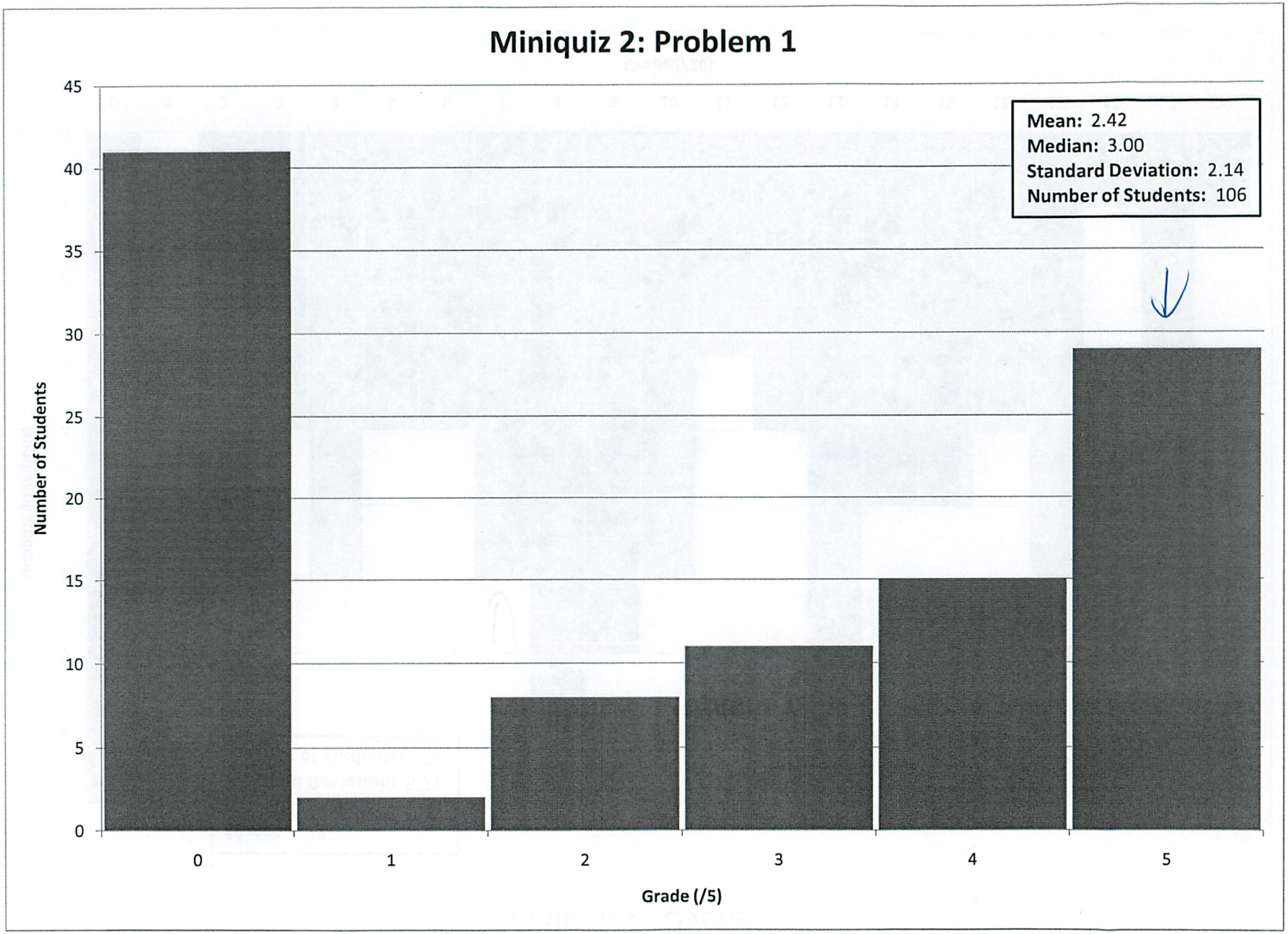
■

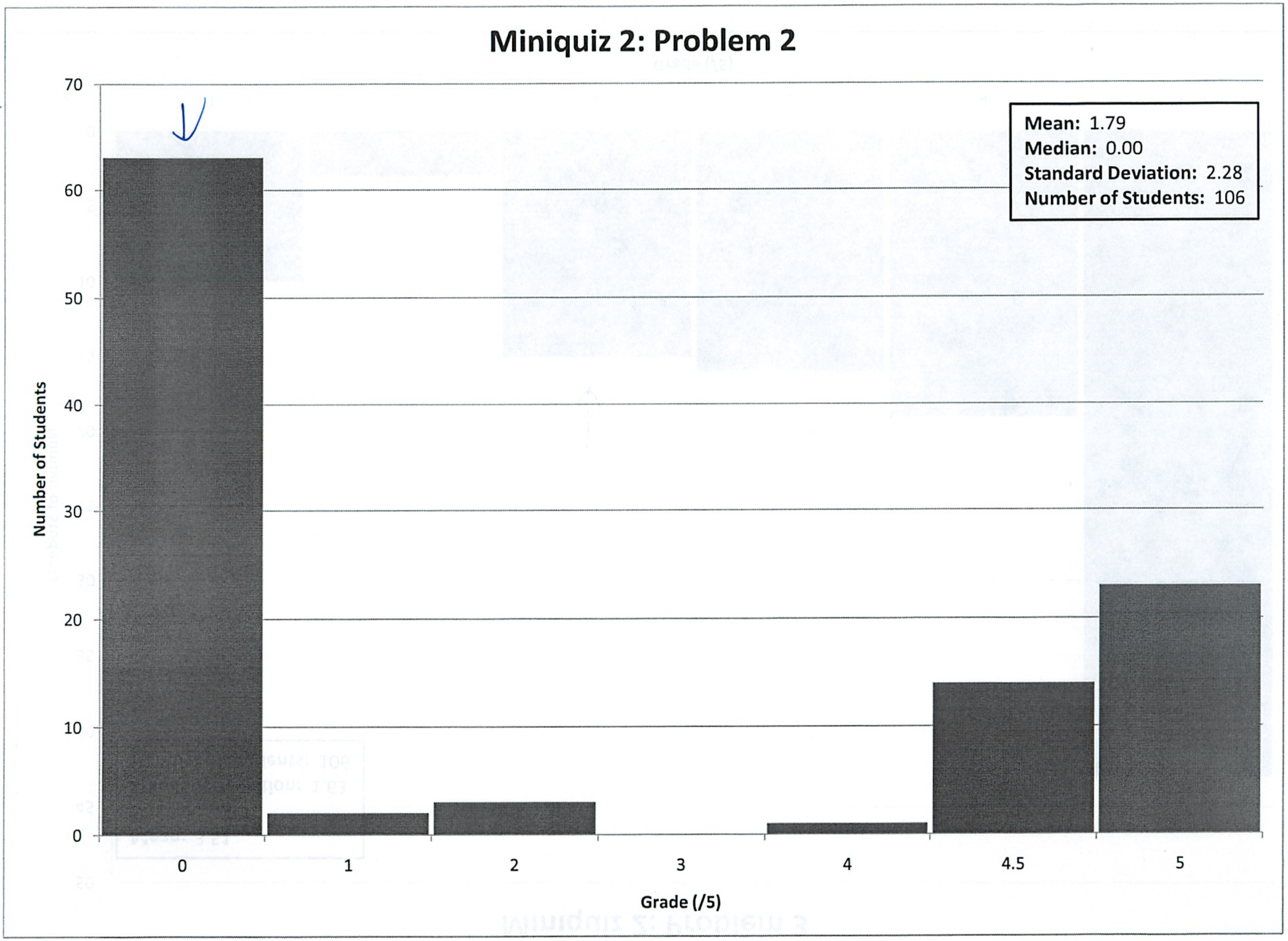
(e) Briefly explain what advantage unambiguous recursive definitions have over ambiguous ones. (Remember that "ambiguous definition" has a technical mathematical meaning which does not imply that the ambiguous definition is unclear.)

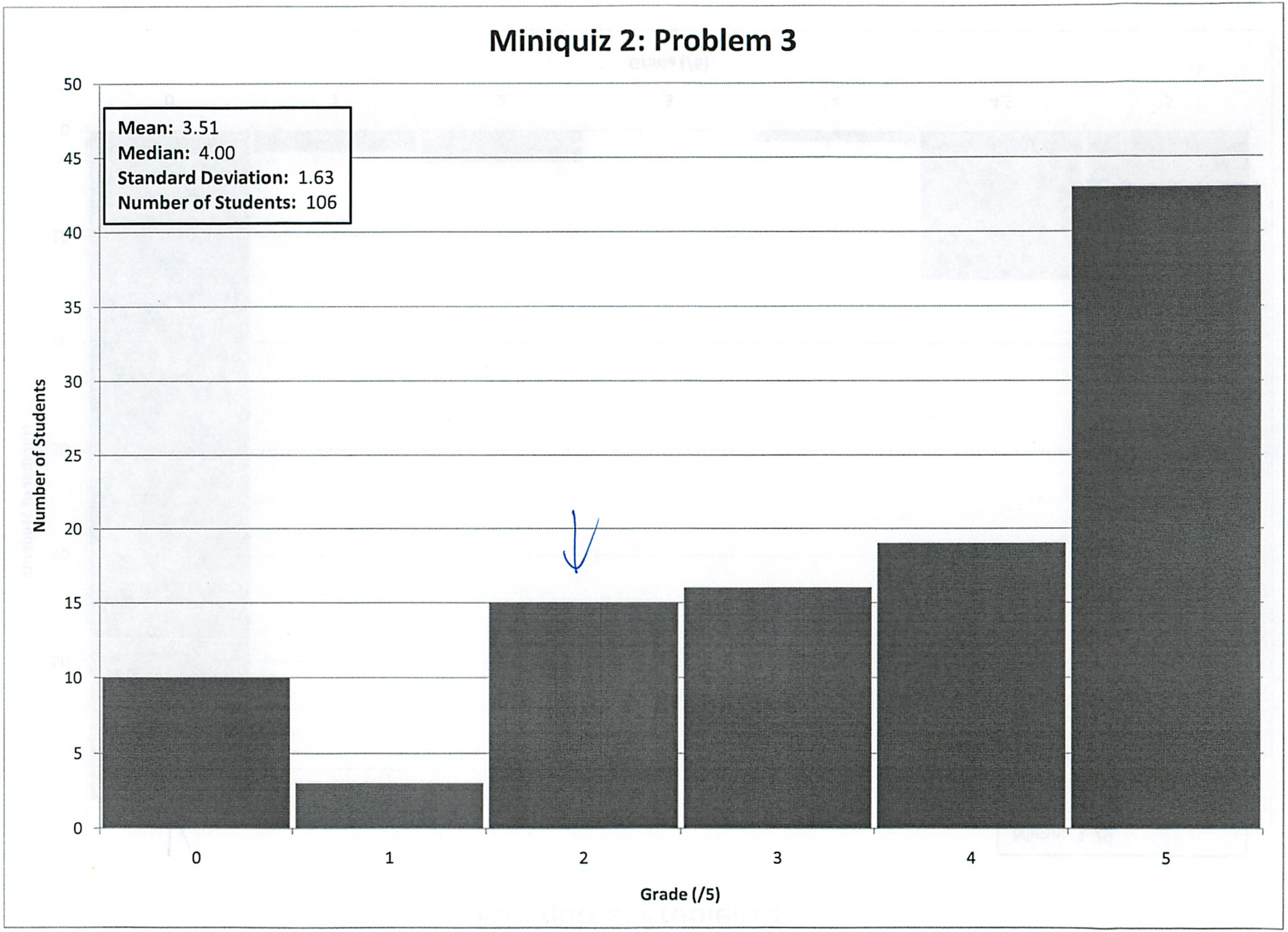
Solution. If a definition is ambiguous, functions defined recursively on it may not be well-defined.

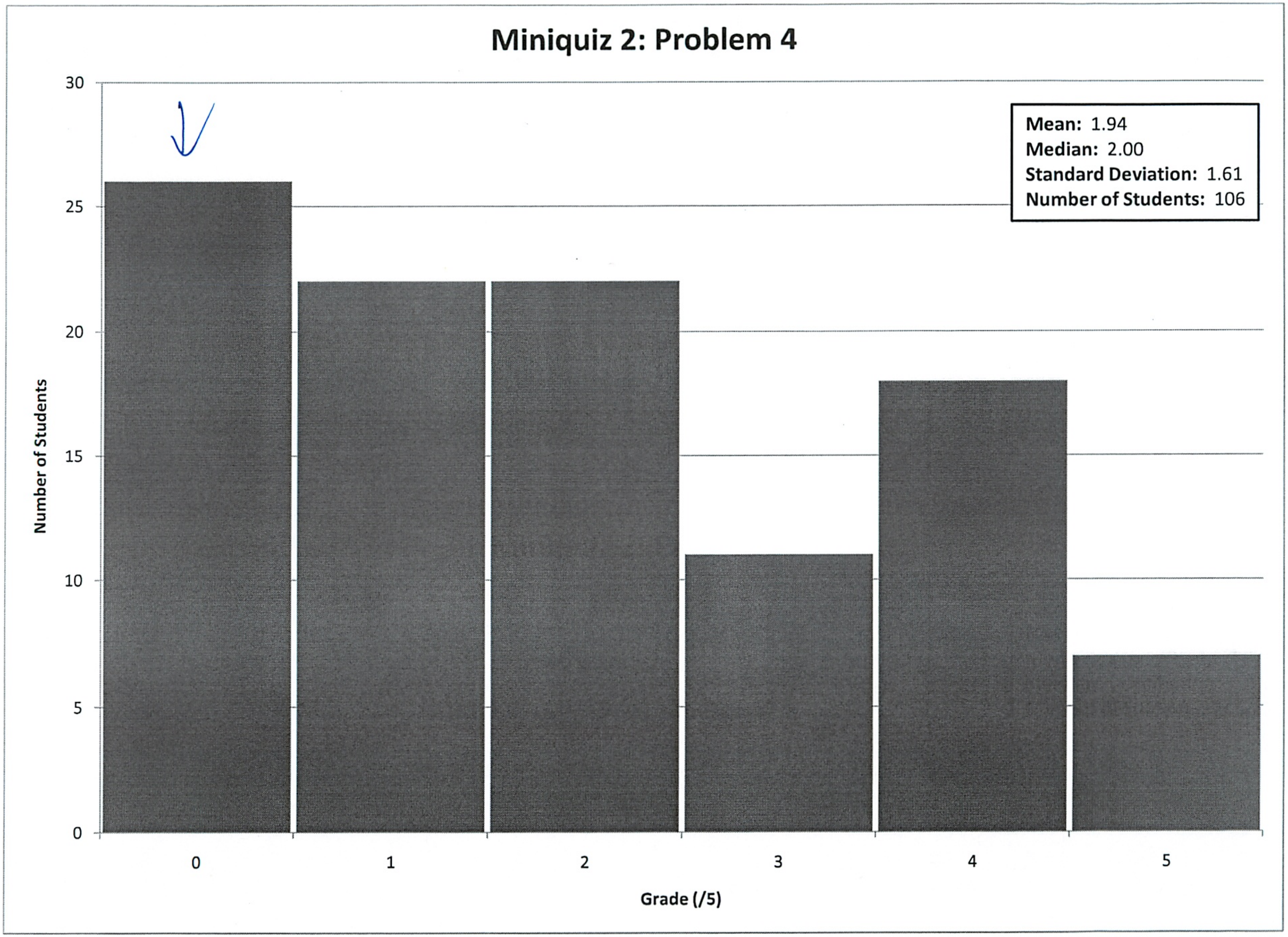
■


Miniquiz 2: Overall
Mean: 9.73
Median: 9.50
Standard Deviation: 5.71
Number of Students: 106
Number of Students
Grade (/20)
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20


Miniquiz 2: Problem 1
Mean: 2.42
Median: 3.00
Standard Deviation: 2.14
Number of Students: 106
Number of Students
45
40
35
30
25
20
15
10
5
0
0
1
2
3
4
5
Grade (/5)


Miniquiz 2: Problem 2
Mean: 1.79
Median: 0.00
Standard Deviation: 2.28
Number of Students: 106
Number of Students
70
60
50
40
30
20
10
0
0
1
2
3
4
4.5
5
Grade (/5)


Miniquiz 2: Problem 3
Mean: 3.51
Median: 4.00
Standard Deviation: 1.63
Number of Students: 106
Number of Students
0
5
10
15
20
25
30
35
40
45
50
Grade (/5)
0
1
2
3
4
5


Miniquiz 2: Problem 4
Mean: 1.94
Median: 2.00
Standard Deviation: 1.61
Number of Students: 106
Number of Students
30
25
20
15
10
5
0
0
1
2
3
4
5
Grade (/5)

B 2/28

Mathematics for Computer Science

MIT 6.042J/18.062J

Intro to Number Theory: Divisibility, GCD's

Arithmetic Assumptions

assume usual rules for +, ·, − :

$a(b+c) = ab + ac$, $ab = ba$,

$(ab)c = a(bc)$, $a - a = 0$,

$a + 0 = a$, $a+1 > a$, ...

The Division Theorem

For $b > 0$ and any a, have

q = quotient(a,b)

r = remainder(a,b)

∃ unique numbers q, r such that

$a = qb + r$ and $0 \leq r < b$.

Take this for granted too!

Divisibility

c divides a $(c|a)$ iff

$a = k \cdot c$ for some k

$5|15$ because $15 = 3 \cdot 5$

$n|0$ because $0 = 0 \cdot n$

Simple Divisibility Facts

- $c|a$ implies $c|(sa)$

[$a=k'c$ implies

$(sa)=\underbrace{(sk')}_{k}c$]

Simple Divisibility Facts

- $c|a$ implies $c|(sa)$
- if $c|a$ and $c|b$ then $c|(a+b)$

[if $a=k_1c$, $b=k_2c$ then $a+b= (k_1+k_2)c$]

Simple Divisibility Facts

c a common divisor of a,b

- if c|a and c|b then

  c| (sa+tb)

  integer linear combination of a and b

Albert R Meyer February 28, 2011 lec 5M.7

Common Divisors

Common divisors of a & b divide integer linear combinations of a & b.

Albert R Meyer February 28, 2011 lec 5M.9

GCD

gcd(a,b) ::= the *greatest* common divisor of a and b

gcd(10,12) = 2

gcd(13,12) = 1

gcd(17,17) = 17

gcd(0, n) = n for $n>0$

Albert R Meyer February 28, 2011 lec 5M.10

GCD Remainder Lemma

Lemma: for $b \neq 0$

gcd(a,b) = gcd(b, rem(a,b))

Proof: a = qb + r

any divisor 2 of these 3 terms, divides all 3.

Albert R Meyer February 28, 2011 lec 5W.12

Euclidean Algorithm

as a State Machine:

States ::= $\mathbb{N} \times \mathbb{N}$

start ::= (a,b)

state transitions defined by

$(x,y) \rightarrow (y, \text{rem}(x,y))$

for $y \neq 0$

Albert R Meyer February 28, 2011 lec 5W.13

GCD correctness

Example: GCD(662,414)

= GCD(414, 248) since rem(662,414) = 248

= GCD(248, 166) since rem(414,248) = 166

= GCD(166, 82) since rem(248,166) = 82

= GCD(82, 2) since rem(166,82) = 2

= GCD(2, 0) since rem(82,2) = 0

return value: 2

Albert R Meyer February 28, 2011 lec 5W.15

GCD correctness

By Lemma, gcd(x,y) is constant.
so preserved invariant is
P((x,y)) ::= [gcd(a,b) = gcd(x,y)]

P(start) is trivially true:
(gcd(a,b) = gcd(a,b))

Albert R Meyer February 28, 2011 lec 5W.16

GCD partial correctness

at termination

x = gcd(a,b)

Proof: at termination, y = 0, so
x = gcd(x,0) = gcd(x,y) = gcd(a,b)

(gcd(x,y) = gcd(a,b): preserved invariant)

Albert R Meyer February 28, 2011 lec 5W.18

GCD Termination

y halves or smaller at each step
reaches minimum in ≤ log2 b transitions

Albert R Meyer February 28, 2011 lec 5W.19

GCD is a linear combination

Theorem:
gcd(a,b) is an integer linear combination of a and b.

Albert R Meyer February 28, 2011 lec 5M.22

gcd(a,b) = sa+tb

Proof: Show how to find coefficients s,t.

Method: apply Euclidean algorithm, finding coefficients as you go.

Albert R Meyer February 28, 2011 lec 5M.28

Finding s and t

Example: a = 899, b=493

899 = 1·493 + 406 so 406 = 1·899 + -1·493
493 = 1·406 + 87 so 87 = 493 - 1·406
= -1·899 + 2·493
406 = 4·87 + 58 so 58 = 406 - 4·87
= 5·899 + -9·493
87 = 1·58 + 29 so 29 = 87 - 1·58
= -6·899 + 11·493
58 = 2·29 + 0 done, gcd = 29

Albert R Meyer February 28, 2011 lec 5M.30

Finding s and t

Example: a = 899, b=493

899 = 1·493 + 406 so 406 = 1·899 + -1·493

493 = 1·406 + 87 so 87 = 493 - 1·406
= -1·899 + 2·493

406 = 4·87 + 58 so 58 = 406 - 4·87
= 5·899 + -9·493

87 = 1·58 + 29 so 29 = 87 - 1·58
= -6·899 + 11·493

58 = 2·29 + 0 done, gcd = 29

the Pulverizer s = -6, t = 11

Finding s > 0 and t

gcd(899,493) = -6·899 + 11·493

get positive coeff. for 899?:

(-6+493k)·899 + (11-899k)·493
= -6·899 + 11·493

so use k=1: 487·899 + -888·493
= gcd(899,493)

Prime Divisibility

Lemma: p prime and p|(a·b) implies p|a or p|b

pf: in Class Problem 3.

Prime Divisibility

Cor : If p is prime, and $p|a_1 \cdot a_2 \cdot \cdots \cdot a_m$ then $p|a_i$ for some i.

pf: By induction on m.

Fundamental Thm. of Arithmetic

Every integer > 1 factors uniquely into a weakly increasing sequence of primes

Unique Prime Factorization

Every integer n > 1 has a unique factorization into primes: $p_0 \cdot p_1 \cdot \cdots \cdot p_k = n$ with $p_0 \le p_1 \le \cdots \le p_k$

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Example:

61394323221 =

$3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$

Unique Prime Factorization

pf: suppose not. choose smallest $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \le p_2 \le \cdots \le p_k$$

$$q_1 \le q_2 \le \cdots \le q_m$$

can assume $q_1 < p_1$

so $q_1 \neq$ any p_i

Unique Prime Factorization

Pf: but $q_1 | n$ & $n = p_1 \cdot p_2 \cdots p_k$ so $q_1 | p_i$ for some i by Cor, contradicting that p_i is prime QED

Team Problems

Problems

1—3

6.042 # Theory

2/28

(10 min late)

GCD

Factoring is hard

Lemma to find GCD

$gcd(a, b) = gcd(b, rem(a, b))$

Proof: $a = q b + r$

Have same divisor

So same GCD

So can change # into smaller #s

__Euclidean Algorthm__ as SM

States $= N \times N$

Start $= (a, b)$

Transitions $(x, y) \to (y, rem(x, y))$

repeat, repeat, etc

$GCD(n, 0) = n$

Invarient - new # has the __same__ GCD

$P((x, y)) ::= [gcd(a, b) = gcd(x, y)]$

(2)

P(start) trivally true

then true for anything you can get to

at termination $y=0$

$x = gcd(x,0) = gcd(x,y) = gcd(a,b)$

Reaches min in $\leq 2\log_2 b$ transitions

Theorm $gcd(a,b)$ is an integer linear combo of a, b

$gcd(a,b) = sa + tb$

↑ show how to find the coefficents s, t

Pulverizer

Start $a = 899$ $b = 493$

$899 = 1 \cdot 493 + 406$

↑ quotient ↑ divisor ↑ remainder

so $406 = 1 \cdot 899 - 1 \cdot 493$

$493 = 1 \cdot 406 + 87$

$87 = 493 - 1 \cdot 406$

$= -1 \cdot 899 + 2 \cdot 493$ back substitute

$406 = 4 \cdot 87 + 58$

$58 = 406 - 4 \cdot 87$

$= 5 \cdot 899 - 9 \cdot 493$ keep info from 2 stages back

$87 = 1 \cdot 58 + 29$

$29 = 87 - 1 \cdot 58$

$= -6 \cdot 899 + 11 \cdot 493$

$58 = 2 \cdot 29 + 0$

gcd $= 29$

$s = -6$ $t = 11$

(3)

One is always ⊕ and one is always ⊖

Get + coeff for 899:

$(-6 + 493k) \cdot 899 + (11 - -899k) \ldots$

... (missed info, see slide 34)

Prime Divisibility

Lemma: p prime and $p \mid (a \cdot b) \Rightarrow p \mid a$ or $p \mid b$

↳ in class problem 3

P-Set - had to ~~prove~~ divide by a prime

Corrolary: If p is prime and $p \mid a_1 \cdot a_2 \cdot a_m$

... (missed)

Get Unique Factorization Theorm / Fnd. Theorm of Alegbra

- Can do weakly increasing ~~or~~ or decreasing

Unique factorization of primes

...

If there is any, there is a smallest one

...

$a_1 < p_1$

(9)

q is a divisor of n

So $q_1 | n$ and $n = p_1 p_2 \cdots p_k$

So $q_1 | p_i$ for some i by corellary

In-Class Problems Week 5, Mon.

Problem 1.
A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.[1]

Problem 2. **(a)** Use the Pulverizer to find integers x, y such that

$$x \cdot 50 + y \cdot 21 = \gcd(50, 21).$$

(b) Now find integers x', y' with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \gcd(50, 21)$$

Problem 3.
For nonzero integers, a, b, prove the following properties of divisibility and GCD'S. (You may use the fact that $\gcd(a, b)$ is an integer linear combination of a and b. You may *not* appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

(a) Every common divisor of a and b divides $\gcd(a, b)$.

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

(c) If $p \mid ab$ for some prime, p, then $p \mid a$ or $p \mid b$.

(d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

Prof - read sols for #3
Very important

[1] Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: *every* even perfect number is of this form (for a simple proof see `http://primes.utm.edu/notes/proofs/EvenPerfect.html`). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.

Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned}
\gcd(259, 70) &= \gcd(70, 49) && \text{since rem}(259, 70) = 49 \\
&= \gcd(49, 21) && \text{since rem}(70, 49) = 21 \\
&= \gcd(21, 7) && \text{since rem}(49, 21) = 7 \\
&= \gcd(7, 0) && \text{since rem}(21, 7) = 0 \\
&= 7.
\end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

In Class Problems

2/28

1. So this was in the book

   10 does not work

   1, 2, 5, 10

   $1+2+5=8$ ⊗

   When ___ is prime? – only then

   What is k? – just a #

   $k=0$

   ~~$2^{-1}(2^0-1)$~~

   · First test $2^0-1=0$ ⊗

   $k=1$

   $2^1-1=1$ ~~⊗~~ ⊗ Not prime by convention

   $k=2$

   ~~2~~ $2^2-1=3$ ✓ prime

   $2^1(3)=6$ ⊗ Not prime

   but that is not what we are looking for

   looking for perfectness

   1, 2, 3, 6

   $1+2+3$ ✓

(2)

But how does this work generally?
What patterns are there in prime, in perfect

(our board)

$2^{k-1}(2^k-1)$ has following factors besides itself

a) Those that are divided by the prime 2^k-1
b) Those that are not, but are instead powers of 2

These correspond to

a) $(2^k-1)(1)+(2^k-1)(2)+(2^k-1)(4)+ \dots +(2^k-1)(2^{k-2})$
b) $1, 2, 4, \dots, 2^{k-2}$

Summing (a) we get

$$(2^k-1)\sum_{n=0}^{k-2} 2^n = (2^k-1)(2^{k-1}-1)$$

never show 2^{k-1} is prime
- show that those are the only divisors

Summing (b) we get

$$\sum_{k=0}^{k-1} 2^n = 2^k - 1$$

So sum of the factors of $2^{k-1}(2^k-1)$ besides itself is

$= (2^k-1)(2^{k-1}-1+1)$

$= (2^k-1)(2^{k-1})$

③

2 (or board)

Pulverizer $x(0) = 50 \quad y(0) = 21$

x	y	r = x − qy	
50	21	8	50 − (2·21)
21	8	5	21 − (2·8)
8	5	3	8 − 5
5	3	2	5 − 3
3	2	1	3 − 2
2	1	0	gcd = 1

$= 5 \cdot 21 - 2 \cdot 50$

$= 3 \cdot 50 - 7 \cdot 21$

$= 12 \cdot 21 - 5 \cdot 50$

$= 8 \cdot 50 - 19 \cdot 21$

$\gcd(50, 21) = 1 = 8 \cdot 50 - 19 \cdot 21$

↑ s ↑ t

not the shortest way to do

b) $8 \cdot 50 - 19 \cdot 21 = 1$, so $-8 \cdot 50 + 19 \cdot 21 = -1$

$5 \cdot 50 = 250$

$12 \cdot 21 = 252$

$12 \cdot 21 - 5 \cdot 50 = 2$

$-8 \cdot 50 + 19 \cdot 21 + 5 \cdot 50 + 12 \cdot 21 = -1 + 2 = 1$

$-13 \cdot 50 + 31 \cdot 21 = 1 = \gcd(50, 21)$

$x' = -13$

$y' = 31$

(4)

2b easier

~~Subtract~~

$8 \cdot 50 - 19 \cdot 21 = 1$

$-21 \cdot 50$ $+21 \cdot 50$

$-13 \cdot 50 + 31 \cdot 21 = 1$

So this is switching which is -

Can keep doing to find ∞ combos

- One side gets more ⊖
- Other side gets more ⊕

3.

Solutions to In-Class Problems Week 5, Mon.

Problem 1.
A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.[1]

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, \quad 2, \quad 4, \quad \ldots, \quad 2^{k-1}, \tag{1}$$

and

$$1 \cdot (2^k - 1), \quad 2 \cdot (2^k - 1), \quad 4 \cdot (2^k - 1), \quad \ldots, \quad 2^{k-2} \cdot (2^k - 1). \tag{2}$$

The sequence (1) sums to $2^k - 1$ (using the formula for a geometric series,[2] and likewise the sequence (2) sums to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect. ■

Problem 2. (a) Let $m = 2^9 5^{24} 11^7 17^{12}$ and $n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2$. What is the $\gcd(m, n)$? What is the *least common multiple*, $\text{lcm}(m, n)$, of m and n? Verify that

$$\gcd(m, n) \cdot \text{lcm}(m, n) = mn. \tag{3}$$

Solution.

GCD
$$g = 2^3 11^7 17^9,$$
LCM
$$l = 2^9 5^{24} 7^{22} 11^{211} 13^1 17^{12} 19^2$$
$$gl = 2^{12} 5^{24} 7^{22} 11^{218} 13^1 17^{21} 19^2 = mn$$

does not say how got...

■

(b) Describe in general how to find the $\gcd(m, n)$ and $\text{lcm}(m, n)$ from the prime factorizations of m and n. Conclude that equation (3) holds for all positive integers m, n.

Solution. The divisors of m correspond to subsequences of the weakly increasing sequence of primes in the factorization of m, and likewise for n. So the factorization $\gcd(m, n)$ is the largest common subsequence of the two factorizations. This can be calculated by taking all the primes that appear in both factorizations raised to the *minimum* of the powers of that prime in each factorization.

[1]Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: *every* even perfect number is of this form (for a simple proof see `http://primes.utm.edu/notes/proofs/EvenPerfect.html`). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.

[2]It's fun to notice the "computer science" proof that (1) sums to $2^k - 1$. The binary binary representation of 2^j is a 10^j, so the sum is represented by 1^k. This what you get by subtracting 1 from by 10^k which is the binary representation of 2^k.

Likewise, the factorization of $\text{lcm}(m,n)$ is the shortest sequence that has the factorizations of m and n as subsequences. So the factorization of $\text{lcm}(m,n)$ can be calculated by taking all the primes that appear in either factorization raised to the *maximum* of the powers of that prime in each factorization.

So in the factorization of $\gcd(m,n) \cdot \text{lcm}(m,n)$ each prime appears raised to a power equal to the sum of its powers in the factorizations of m and n, which is precisely its power in the factorization of mn. ■

Problem 3. **(a)** Use the Pulverizer to find integers x, y such that

$$x \cdot 50 + y \cdot 21 = \gcd(50, 21).$$

Solution. Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x,y)$		$x - q \cdot y$
50	21	8	=	$50 - 2 \cdot 21$
21	8	5	=	$21 - 2 \cdot 8$
			=	$21 - 2 \cdot (50 - 2 \cdot 21)$
			=	$-2 \cdot 50 + 5 \cdot 21$
8	5	3	=	$8 - 1 \cdot 5$
			=	$(50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$
			=	$3 \cdot 50 - 7 \cdot 21$
5	3	2	=	$5 - 1 \cdot 3$
			=	$(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$
			=	$-5 \cdot 50 + 12 \cdot 21$
3	2	1	=	$3 - 1 \cdot 2$
			=	$(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$
			=	$\boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0		

■

(b) Now find integers x', y' with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \gcd(50, 21)$$

Solution. since $(x, y) = (8, -19)$ works, so does $(8 - 21n, -19 + 50n)$ for any $n \in \mathbb{Z}$, so letting $n = 1$, we have

$$-13 \cdot 50 + 31 \cdot 21 = 1$$

■

Problem 4.

For nonzero integers, a, b, prove the following properties of divisibility and GCD'S. (You may use the fact that $\gcd(a,b)$ is an integer linear combination of a and b. You may *not* appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

(a) Every common divisor of a and b divides $\gcd(a,b)$.

Solution. For some s and t, $\gcd(a,b) = sa + tb$. Let c be a common divisor of a and b. Since $c \mid a$ and $c \mid b$, we have $a = kc, b = k'c$ so

$$sa + tb = skc + tk'c = c(sk + tk')$$

so $c \mid sa + tb$. ■

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Solution. Since $\gcd(a, b) = 1$, we have $sa + tb = 1$ for some s, t. Multiplying by c, we have

$$sac + tbc = c$$

but a divides the second term of the sum since $a \mid bc$, and it obviously divides the first term, and therefore it divides the sum, which equals c.

■

(c) If $p \mid ab$ for some prime, p, then $p \mid a$ or $p \mid b$.

Solution. If p does not divide a, then since p is prime, $\gcd(p, a) = 1$. By part (b), we conclude that $p \mid b$. ■

(d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

Solution. Since $\gcd(a, b)$ is positive and an integer linear common of a and b, we have

$$m \leq \gcd(a, b).$$

On the other hand, since m is a linear combination of a and b, every common factor of a and b divides m. So in particular, $\gcd(a, b) \mid m$, which implies

$$\gcd(a, b) \leq m.$$

■

Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned}
\gcd(259, 70) &= \gcd(70, 49) && \text{since rem}(259, 70) = 49 \\
&= \gcd(49, 21) && \text{since rem}(70, 49) = 21 \\
&= \gcd(21, 7) && \text{since rem}(49, 21) = 7 \\
&= \gcd(7, 0) && \text{since rem}(21, 7) = 0 \\
&= 7.
\end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

Mathematics for Computer Science
MIT 6.042J/18.062J

Congruences: arithmetic (mod n)

Congruence mod n

Def: $a \equiv b \pmod{n}$
iff $n \mid (a - b)$

example: $30 \equiv 12 \pmod{9}$
since
9 divides 30 - 12

Congruence mod n

example:
$66666663 \equiv 788253 \pmod{10}$

WHY?

$$\begin{array}{r} 66666663 \\ -\ \ \ 788253 \\ \hline \text{xxxxxxx}0 \end{array}$$

Remainder Lemma

$a \equiv b \pmod{n}$
iff
$\text{rem}(a,n) = \text{rem}(b,n)$

example: $30 \equiv 12 \pmod{9}$
since
$\text{rem}(30,9) = 3 = \text{rem}(12,9)$

Remainder Lemma

$a \equiv b \pmod{n}$
iff
$\text{rem}(a,n) = \text{rem}(b,n)$

abbreviate: $r_{b,n}$

proof: (if)

$a = q_a n + r_{a,n}$

$b = q_b n + r_{b,n}$

if rem's are =, then

$a-b=(q_a-q_b)n$ so $n \mid (a-b)$

(only if) proof similar

Remainder Lemma

$a \equiv b \pmod{n}$

iff

$\text{rem}(a,n) = \text{rem}(b,n)$

QED

More Corollaries

- *symmetric*

  $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

- *transitive*

  $a \equiv b$ & $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

Congruence mod n

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

$a+c \equiv b+c \pmod{n}$

pf: $n \mid (a - b)$ implies

$n \mid ((a+c) - (b+c))$

Congruence mod n

Corollary:

If $a \equiv b \pmod{n}$ &

$c \equiv d \pmod{n}$,

then $a \cdot c \equiv b \cdot d \pmod{n}$

Congruence mod n

Cor: if $a \equiv a' \pmod{n}$, then replacing a by a′ in any arithmetic formula gives an $\equiv \pmod{n}$ formula

Remainder arithmetic

important: congruence &

$a \equiv \text{rem}(a,n) \pmod{n}$

keeps (mod n) arithmetic in the remainder range

0 to n-1

Remainder arithmetic

example: $287^9 \equiv ?$ (mod 4)

$287^9 \equiv 3^9$ since $r_{287,4} = 3$

$= ((3^2)^2)^2 \cdot 3$

$\equiv (1^2)^2 \cdot 3$ since $r_{9,4} = 1$

$= 3$ (mod 4)

Congruence mod n

So arithmetic (mod n) a lot like ordinary arithmetic

the main difference:

$8 \cdot \not{2} \equiv 3 \cdot \not{2}$ (mod 10)

$8 \not\equiv 3$ (mod 10)

no arbitrary cancellation

cancellation (mod n)

When can you cancel k?

--when k has no common factors with n

inverses (mod n)

If gcd(k,n)=1, then have k'

$k \cdot k' \equiv 1$ (mod n).

k' is an *inverse* mod n of k

pf: $sk + tn = 1$, so just let $k' ::= s$

cancellation (mod n)

If $a \cdot k \equiv b \cdot k$ (mod n) and gcd(k,n) = 1, then multiply by k':

$(a \cdot k) \cdot k' \equiv (b \cdot k) \cdot k'$ (mod n)

$a \cdot 1 \equiv b \cdot 1$

so $a \equiv b$ (mod n)

cancellation (mod n)

summary:

k is *cancellable* (mod n) iff

k has an *inverse* (mod n) iff

k is *relatively prime* to n

Team Problems

Problems

1—3

Albert R Meyer, March 2, 2011 lec 5W.42

6.042 Congruences

Think went pretty well
Should have studied last part more
But starting to see patterns
- read old solutions is best
Should have spent hr more

happy to have this over

Prof want to see median 17/20

More number theory
- RSA, hashing, ECC

Congruences / remainder / residue artimitic

Def $a \equiv b \pmod{n}$ iff $n \mid (a-b)$
Congruence mod n $n \mid (b-a)$

- on negitive # wacky in programs

equivilance and mod are attached to each other

Goes back to Gauss 18th century

$30 \equiv 12 \pmod{4}$

... (missed)

②

Remainder Lemma

$a \equiv b \pmod{n}$

iff

$rem(a,n) = rem(b,n)$

$30 \equiv 12 \pmod{9}$

since $rem(30,9) = 3 = rem(12,9)$

alt way to verify 30 congruent mod 9

$rem(b,n) = r_{b,n}$ <u>notation</u>

<u>Proof</u>

$a = q_a n + r_{a,n}$ q = quotient

$b = q_b n + r_{b,n}$

if rem = then

$a - b = (q_a - q_b)n$

So $n \mid (a-b)$

<u>More Corollaries</u>

- <u>Symmetric</u> $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
- <u>transitive</u> $a \equiv b$ AND $b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$

(3)

It acts like an equality that preseves operations

If $a \equiv b \pmod{n} \rightarrow a+c \equiv b+c \pmod{n}$

Proof (missed)

Corollary

If $a \equiv b \pmod{n}$ AND $c \equiv d \pmod{n}$

Then $a+c \equiv b+d \pmod{n}$

Also $a \cdot c \equiv b \cdot d \pmod{n}$

~~[illegible]~~ Can do familar algebric expressions

replace a by a' gives $\equiv \pmod{n}$

↳ in any arithmetic formula

It means # never have to get big, can bang down to b/w 0, n-1

$a = rem(a, n) \pmod{n}$

keeps (mod n) arithmetic in rem range 0, n-1

$[0, n)$

↑ includes ↑ does not include

Example $287^9 \equiv ? \pmod{4}$

$287^9 \equiv 3^9$ since $r_{287,4} = 3$

$= ((3^2)^2)^2 \cdot 3$

succesive square gimmic

(4)

(did not read for b/c quiz?)

But $3^2 = 1 \mod 4$

$= (1^2)^2 \cdot 3$ since $r_{9,4} = 1$

$= 3 \pmod 4$

Watch simplification - not in exponent!

A lot like ordinary arithmitic

But can't cancle

$8 \cdot 2 = 3 \cdot 2 \pmod{10}$

$8 \neq 3 \pmod{10}$

Sometimes it will work

- when k has no common factors w/ n

If $\gcd(k,n) = 1$ then have k'

$k \cdot k' = 1 \pmod n$

k' is an inverse mod n of k

Proof $sk + tn = 1$ so

Its that s is coefficent
- linear combo
- pulverizer

(missed some stuff here)

Just let $k' := s$

Lot of milage out of linear combo

(5)

Multiply by k'
To show a,b =

(See slides)

Summary

k is cancellable (mod n) iff
k has an inverse (mod n) iff
k is relatively prime to n

Did not read b/c quiz
Need to catch up

In-Class Problems Week 5, Wed.

Problem 1. **(a)** Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9? *Hint:* $10 \equiv 1 \pmod 9$.

(b) Take a big number, such as 37273761261. Sum the digits, where every other one is negated:

$$3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 = -11$$

Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11.

Problem 2. **(a)** Use the Pulverizer to find integers s, t such that

$$40s + 7t = \gcd(40, 7).$$

(b) Adjust your answer to part (a) to find an inverse modulo 40 of 7 in $[1, 40)$.

Problem 3.
Suppose a, b are relatively prime and greater than 1. In this problem you will prove the *Chinese Remainder Theorem*, which says that for all m, n, there is a *unique* $x \in [0, ab)$ such that

$$x \equiv m \pmod a, \tag{1}$$
$$x \equiv n \pmod b. \tag{2}$$

(a) Prove that for any m, n, there is some x satisfying (1) and (2).
Hint: Let b^{-1} be an inverse of b modulo a and define $e_a ::= b^{-1}b$. Define e_b similarly. Let $x = me_a + ne_b$.

(b) Prove that if

$$x \equiv 0 \pmod a, \text{ and}$$
$$x \equiv 0 \pmod b,$$

then

$$x \equiv 0 \pmod{ab}.$$

(c) Conclude that if x_0 and x_1 both satisfy (1) and (2) (for the same m, n), then

$$x_0 \equiv x_1 \pmod{ab}.$$

(d) Prove that if $x \equiv m \pmod{ab}$, then $x \equiv m \pmod a$ for all m.

(e) Conclude that there is an $x \in [0, ab)$ satisfying (1) and (2).

(f) Conclude that there is a *unique* $x \in [0, ab)$ satisfying (1) and (2).

Solutions to In-Class Problems Week 5, Wed.

Problem 1. **(a)** Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9? *Hint:* $10 \equiv 1 \pmod{9}$.

Solution. Since $10 \equiv 1 \pmod{9}$, so is

$$10^k \equiv 1^k \equiv 1 \pmod{9}. \tag{1}$$

Now a number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0.$$

From (1), we have

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod{9}$$

This shows something stronger than what we were asked to show, namely, it shows that the remainder when the original number is divided by 9 is equal to the remainder when the sum of the digits is divided by 9. In particular, if one is zero, then so is the other. ■

(b) Take a big number, such as 37273761261. Sum the digits, where every other one is negated:

$$3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 = -11$$

Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11.

Solution. A number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

Observing that $10 \equiv -1 \pmod{11}$, we know:

$$\begin{aligned}
&d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_1 \cdot 10 + d_0 \\
&\equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \cdots + d_1 \cdot (-1)^1 + d_0 \cdot (-1)^0 \pmod{11} \\
&\equiv d_k - d_{k-1} + \cdots - d_1 + d_0 \pmod{11}
\end{aligned}$$

assuming k is even. The case where k is odd is the same with signs reversed.

The procedure given in the problem computes $\pm$ this alternating sum of digits, and hence yields a number divisible by 11 ($\equiv 0 \pmod{11}$) iff the original number was divisible by 11. ■

Problem 2. **(a)** Use the Pulverizer to find integers s, t such that

$$40s + 7t = \gcd(40, 7).$$

Solution. $s = 3$ and $t = -17$

Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
40	7	5	$=$	$40 - 5 \cdot 7$
7	5	2	$=$	$7 - 5$
			$=$	$7 - (40 - 5 \cdot 7)$
			$=$	$-1 \cdot 40 + 6 \cdot 7$
5	2	1	$=$	$5 - 2 \cdot 2$
			$=$	$(40 - 5 \cdot 7) - 2 \cdot (-1 \cdot 40 + 6 \cdot 7)$
			$=$	$3 \cdot 40 - 17 \cdot 7$
2	1	0		

■

(b) Adjust your answer to part (a) to find an inverse modulo 40 of 7 in $[1, 40)$.

Solution.

$$\begin{aligned}1 &= 3 \cdot 40 - 17 \cdot 7\\ &= 3 \cdot 40 - 7 \cdot 40 + 40 \cdot 7 - 17 \cdot 7\\ &= (3 - 7) \cdot 40 + (40 - 17) \cdot 7\\ &= -4 \cdot 40 + 23 \cdot 7\end{aligned}$$

Therefore, $23 \cdot 7 \equiv 1 \pmod{40}$ and 23 is the inverse of 7 modulo 40.

Alternatively, since -17 is an inverse, so is $\text{rem}(-17, 40) = 23$.

■

Problem 3.

Suppose a, b are relatively prime and greater than 1. In this problem you will prove the *Chinese Remainder Theorem*, which says that for all m, n, there is an x such that such that

$$x \equiv m \bmod a, \tag{2}$$

$$x \equiv n \bmod b. \tag{3}$$

Moreover, x is unique up to congruence modulo ab, namely, if x' also satisfies (2) and (3), then

$$x' \equiv x \bmod ab.$$

(a) Prove that for any m, n, there is some x satisfying (2) and (3).

Hint: Let b^{-1} be an inverse of b modulo a and define $e_a ::= b^{-1}b$. Define e_b similarly. Let $x = me_a + ne_b$.

(b) Prove that

$$[x \equiv 0 \bmod a \text{ AND } x \equiv 0 \bmod b] \quad \text{implies} \quad x \equiv 0 \bmod ab.$$

(c) Conclude that

$$\left[x \equiv x' \bmod a \text{ AND } x \equiv x' \bmod b\right] \quad \text{implies} \quad x \equiv x' \bmod ab.$$

(d) Conclude that the Chinese Remainder Theorem is true.

(e) What about the converse of the implication in part (c)?

Solutions TBA

February 26
revised Sunday 27th February, 2011, 01:33

Problem Set 4

Due: March 4

Reading: Chapter 8–8.3. GCD's and Unique factorization, by Monday, Feb 28
Chapter 8.4–8.6. Arithmetic mod a prime, by Wed. Mar. 2
Chapter 8.7. Euler's Theorem, by Fri. Mar. 4
Chapter 8.8–8.9. The RSA crypto-system, by Mon. Mar. 7
This pset covers Ch. 7 and Ch. 8–8.6.

Problem 1.

Definition 1.1. The set, RecMatch, of strings of matching brackets, is defined recursively as follows:

- **Base case:** $\lambda \in$ RecMatch.
- **Constructor case:** If $s, t \in$ RecMatch, then

$$[\, s \,]\, t \in \text{RecMatch}.$$

One precise way to determine if a string is matched is to start with 0 and read the string from left to right, adding 1 to the count for each left bracket and subtracting 1 from the count for each right bracket. For example, here are the counts for two sample strings:

	[	]	]	[	[	[	[	[	]	]	]	]
0	1	0	−1	0	1	2	3	4	3	2	1	0

	[	[	[	]	]	[	]	]	[	]
0	1	2	3	2	1	2	1	0	1	0

A string has a *good count* if its running count never goes negative and ends with 0. So the second string above has a good count, but the first one does not because its count went negative at the third step.

Definition 1.2. Let

$$\text{GoodCount} ::= \{s \in \{\,]\,,\,[\,\}^* \mid s \text{ has a good count}\}.$$

The matched strings can now be characterized precisely as this set of strings with good counts.

(a) Prove that GoodCount contains RecMatch by structural induction on the definition of RecMatch.

(b) Conversely, prove that RecMatch contains GoodCount. w ind on def of Good Cont

Problem 2. **(a)** Use the Pulverizer to find the inverse of 13 modulo 23 in $[1, 22]$.

(b) Use Fermat's theorem to find the inverse of 13 modulo 23 in $[1, 22]$.

Problem 3.
Define the Pulverizer State machine to have:

$$\begin{aligned}
\text{states} &::= \mathbb{N}^7 \\
\text{start state} &::= (a, b, 0, 1, 1, 0) && \text{(where } a \geq b > 0) \\
\text{transitions} &::= (x, y, s, t, u, v) \longrightarrow \\
&\quad (y,\ \text{rem}(x, y),\ u - sq,\ v - tq,\ s,\ t) && \text{(for } q = \text{qcnt}(x, y), y > 0).
\end{aligned}$$

(a) Show that the following properties are preserved invariants of the Pulverizer machine:

$$\gcd(x, y) = \gcd(a, b), \tag{1}$$

$$sa + tb = y, \text{ and} \tag{2}$$

$$ua + vb = x. \tag{3}$$

(b) Conclude that the Pulverizer machine is partially correct.

(c) Explain why the machine terminates after at most the same number of transitions as the Euclidean algorithm.

Doing P-set 4

3/3

1. What is structural induction again?
   Messed up on quiz
   recursive data types
   Base case - some known math els
   Constructor - build up
   to prove all elements of data type have property

Matt

b) Base Case = 0
   Put brackets +1 -1
   if s, t both are 0
   So must come out to 0 ~~come out~~

Is it in book?

I am confusing the two

Why does a ask ~~????~~ w/ def RecMatch!?!

2. What section

Ok I see

That was a fun, achievable problem

Where I leaned stuff while doing

#3

Matt says straightforward

I am not really finding it like that

For the two invariants we proved you could simply show it

C - Can I write more

Or is that pretty much it?

Student's Solutions to Problem Set 4

Your name: Michael Plasmeier

Due date: March 4

Table 12

Submission date: 3/4

Circle your TA/LA: Ali Nick Oscar Oshani

Collaboration statement: Circle one of the two choices and provide all pertinent info.

1. I worked alone and only with course materials.
2. I collaborated on this assignment with: ← forgot to include him last week
   got help from:[1] Matt Falk
   and referred to:[2] Wikipedia: Modular Multiplicative Inverse
   TAMU notes Euclid

DO NOT WRITE BELOW THIS LINE

Problem	Score
1	5+3
2	8
3	8
Total	[illegible]

24/30

cool!

[1]People other than course staff.

[2]Give citations to texts and material other than the Spring '11 course materials.

#1 RecMatch

Count the # of [and] in a string
+1 -1

Should always ≥ 0 and = 0 at end

GoodCount ::= {s ∈ {], [}* | s has good count}

a. Prove that GoodCount contains RecMatch w/ structural induction on RecMatch

Hyp: P(s) has GoodCount

<u>Base Case</u> GoodCount(λ) = 0 ✓

The empty string has 0 brackets so it is = 0 and always ≥ 0 ✓

<u>Constructor Case</u> If s, t ∈ RecMatch then [s] t ∈ RecMatch ✓

Assume P(s), P(t) ✓

This is same as +1 s −1 t ✓

+1 +0 −1 +0

0

5

~~Prove that RecMatch contains Good Count~~ This is actually another a

Proof by Structual Induction $P(s) ::= \#_{[}(s) + \#_{]}(s) = 0$

Base Case $\lambda \in$ RecMatch $= \#[(s) = \#](s) =$

The string λ contains 0 brackets thus 0

$= 0$ and is always ≥ 0

Constructor Case

Assume s, t are both 0

aka assume $P(s), P(t)$

Now show $P([s]t)$

$$\#_{[}([s]t) = \#_{[}([) + \#_{[}(s) + \#_{]}(s) + \#_{]}(]) + \#_{[}(t) + \#_{]}(t)$$

$$= 1 + 0 + -1 + 0$$

$$= 0$$

This shows that $\#[(s) + \#](s) = 0$

Did not show must be ≥ 0 at all times

When you read L→R.

may not be able to write

But as you can see above the 1 comes first.

Also you can see that it always $= 0$ so it never goes negitive

b) Prove that RecMatch catains Good Count

Proof by strong induction on the lenght of members of good count = n

$P(s) = \#[- \#] = 0$

Base Case λ = empty string

The string is empty, so has no lenght so adds to 0 ✓

Constructor

Assume $P(n)$

Show that $P(n+2)$ holds

Holds if [s] t

One character is [which is +1, other is] so −1

Still sums to 0

Recursivly evalutate s, t to be same thing

See Solution for inductive step

3

Michael Plasmeier
Oshani
Table 12

8

#2 Find inverse of 13 mod 23 in [1,22] using Pulverizer

[1,22] ::= (1,22) ∪ {1,22}

8.6.1 Multiplicitate Inverses

All numbers that satisfy

$$13 \cdot k = 1 \pmod{23}$$

Wikipedia: Modular Multliplicate Invase of a mod m is x such that

$$a^{-1} \equiv x \pmod{m}$$

So multiplicative inverse is in the ring of Ints mod m

$$ax \equiv aa^{-1} \equiv 1 \pmod{m}$$

So how to find: guess and check:

k=1

$13 \cdot 1 = 13 - 23 = x$

k=2

$13 \cdot 2 = 26 - 23 = 3$

k=3

$13 \cdot 3 = 39 - 23 = 16$

k=4

$13 \cdot 4 = 52 - 23 = 29 - 23 = 6$

k=5

$13 \cdot 5 = 65 - 23 = 42 - 23 = 19$

k=6

$13 \cdot 6 = 78 - 23 \ldots 9$

(2) ...

$k=7$

$13 \cdot 7 = 91$ ... -1

$k=8$

$13 \cdot 8$ ... 11

$k=9$

$13 \cdot 9 = 117$ ... 2

$k=10$

$13 \cdot 10 = 130$ ... 15

Am I missing a trick?

$k=11$

$13 \cdot 11 =$ ... 5

$k=12$ ... 18

$k=13$ ... 8

$k=14$ ... 21

$k=15$ 11

$k=16$ ... 1 ← Tada

So now all numbers congruent to

16 mod 23 are also multiplicative inverses

Like $16 + 23 = 39$

$16 + 23 + 23 = 62$

$16 + 23n$

But the range says just in that interval

(3) . .

b) Do the same w/ Fermat's Little Theorm 13 mod 23
8.6.3 in reading - alt approach

$k^{p-2} \cdot k \equiv 1 \pmod{p}$

Compute rem(13^{21}, 23)

But first need to exponitate
- Do it with fast exponetiation (13, 21)

x = a = 13
y = 1
z = b = 21

Loop
  If z = 0 return y, terminate
  r = rem(z, 2)
  z = quot(z, 2)
  if r = 1 then y = xy
  x = x^2
End Loop

So run

~~r = rem(21, 2) = 2·n = 21 tr r = 1~~
~~z = quo (21, 2) = 10~~
y = x·y = 13·1 = 13
x = x^2 = 13^2 = 169

(4)

$r = rem(10,2) = 0$

$z = quot(10,2) = 5$

$x = x^2 = 169^2 = 28561$

$r = rem(5,2) = 1$

$z = quot(5,2) = 2$

$y = xy = 28561 \cdot 13 = 371293$

$x = x^2 = 815730721$

$r = rem(2,2) = 0$

$z = quot(2,2) = 1$

$x = x^2 = 665416609183179841$

$r = rem(1,2) = 1$

$z = quot(1,2) = 0$

$y = xy = 665416609183179841 \cdot 371293$

$= 247064529073450392704413$

$x = x^2$ ... (does not matter)

---

return $y = 247064529073450392704413$

Now check w/ calc ✓ worked

But should have done all the math mod 23!

Start over...

calc says → 16

⑤ ..

$r = rem(21,2) \bmod 23 = 1$

$z = quot(21,2) \bmod 23 = 10$

$y = x \cdot y = 13 \cdot 1 \bmod 23 = 13$

$x = x^2 = 13^2 \bmod 23 = 8$

$r = rem(10,2) \bmod 23 = 0$

$z = quot(10,2) \bmod 23 = 5$

~~$y = xy = 16 \cdot 13 \bmod 17 = 4$~~

$x = x^2 = 8^2 \bmod 23 = 18$

How do you do mod arithmetic
mod first?
Just do and then mod adjust

$r = rem(5,2) \bmod 23 = 1$

$z = quot(5,2) \bmod 23 = 2$

$y = xy = 18 \cdot 13 \bmod 23 = 4$

$x = x^2 = 18^2 \bmod 23 = 2$

$r = rem(2,2) \bmod 23 = 0$

$z = quot(2,2) \bmod 23 = 1$

$x = x^2 = 2^2 \bmod 23 = 4$

$r = rem(1,2) = 1$

$z = quot(1,2) = 0$

$y = xy \bmod 23 = 4 \cdot 4 = 16$

$x = x^2 \bmod 23 = 4^2 = 16$

---

return 16 ← could tell not changing in last part ✓ matches calculator

(6) - .

And now back to regularly scheduled math

So $13^{21} \equiv 16 \pmod{23}$] how do you know this?

So is 16 a multiplicitative inverse?

$13 \cdot 16 = 208 - 23 \cdots = 1$ ✓

matches previvous. result

Michael Plasmeier
Oshani
Table 12
#3 Define Pulverizer State

States ::= $\mathbb{N}^7$
Start state ::= (a, b, 0, 1, 1, 0) where (a ≥ b > 0)
transitions ::= (x, y, s, t, u, v) → (y, rem(x, y), u − sq, v − tq, s, t)
for (q = qcnt(x, y), y > 0)

✓
a) Show that following properties are preserved invariants of the Pulverizer machine
1. gcd(x, y) = gcd(a, b)
This is assume P(gcd(x, y)) and gcd(x, y) → gcd(x', y')
Prove P(gcd(x', y'))

gcd(y, rem(x, y)) still a GCD
This is prove Euclid's Algorthm, right? yes
Proof by Division Theorm 8.1.5
$a = qb + r$
define r = rem(a, b). a is a linear combo of b and r which implies that any divisor of b and r is a divisor of a by Lemma 8.1.3.2

(2)

Likewise r is a linear combo $a=qb$ of a and b
So any divisor of a and b is a divisor of r
This means that a, b have the same common divisors as b and r, so they have the same greatest GCD,
So they are invarient.

If $b \neq 0$ then $\langle a,b\rangle = \langle b, \underbrace{a \bmod b}_{rem(a,b)}\rangle$

Since $\langle b, a \bmod b\rangle$ is a subset of $\langle a,b\rangle$
Since $a = qb + r$

③

2. $sa + tb = y$

$\mathrm{rem}(x,b) = x \bmod b$

$(u - sq)a + (v - tq)b = \mathrm{rem}(x,y)$

$q = \mathrm{qcnt}(x,y) = \left\lfloor \frac{x}{y} \right\rfloor = \frac{x - x \bmod y}{y}$? floor $y > 0$

$(u - s(\mathrm{qcnt}(x,y)))a + (v - t(\mathrm{qcnt}(x,y)))b = \mathrm{rem}(x,y)$ $y > 0$

$(u - s\left\lfloor \frac{x}{y} \right\rfloor)a + (v - t\left\lfloor \frac{x}{y} \right\rfloor)b = x \bmod y$ $y > 0$

$\left(u - s\left(\frac{x - x \bmod y}{y}\right)\right)a + \left(v - t\left(\frac{x - x \bmod y}{y}\right)\right)b = x \bmod y$

$ua - \frac{asx}{y} - \frac{asx \bmod y}{y} + vb - \frac{btx}{y} - \frac{btx \bmod y}{y} = x \bmod y$

alt

$(s - (u - sq)q)a + (t - (v - tq)q)b = y \bmod y$

$(s - uq + sq^2)a + t - vq - tq^2 b = 0$

$((u - sq) - uq + (u - sq)q^2)a + \ldots$

$(u - sq - uq + uq^2 - sq^3)a$

does not seem invarient
seems to recurse only

see solutions
-1

(4)

3. $ua + vb = x$

$sa + tb = y$

$(u - sq)a + (v - tq)b = rem(x, y)$

which is the same as (2)

See that page

(5)

b) Conclude that Pulverizer machine is partially correct

Partially correct → means if one gets a result its correct

It means that there is a final state - where no transition is possible

Well you get to a point where

$gcd(x, 0)$

And top p189, when $y = 0$ the value of x is the gcd because the Invarient Principal

$$x = gcd(x, 0) = gcd(a, b)$$

↑ You can not go any lower than

rem (x, 0)

because ↑ divide by 0 error

Why do we get desired s, t? -1

$\langle a, b\rangle = \langle g, 0\rangle$

Since $g = ax + by$

So $g = gcd(a, b)$

(6)

c) Explain why machine terminates after at most the same # of transitions as the Euclidean algorithm

Because it is the same thing except with extra paperwork. yes!

The Pulverizer is more commonly known as "the extended Euclidean GCD algorithm."

All we do is write the remainders as linear combinations as a linear combination of a and b

The last non-zero remainder is the linear combination we are looking for

The Pulverizer machine is just a formalization of the Pulverizer algorithm

Solutions to Problem Set 4

Reading: Chapter 8–8.3. GCD's and Unique factorization, by Monday, Feb 28
Chapter 8.4–8.6. Arithmetic mod a prime, by Wed. Mar. 2
Chapter 8.7. Euler's Theorem, by Fri. Mar. 4
Chapter 8.8–8.9. The RSA crypto-system, by Mon. Mar. 7
This pset covers Ch. 7 and Ch. 8–8.6.

Problem 1.
One way to determine if a string has matching brackets, that is, if it is on the set, RecMatch, [1] is to start with 0 and read the string from left to right, adding 1 to the count for each left bracket and subtracting 1 from the count for each right bracket. For example, here are the counts for two sample strings:

	[	]	]	[	[	[	[	[	]	]	]	]
0	1	0	−1	0	1	2	3	4	3	2	1	0

	[	[	[	]	]	[	]	]	[	]
0	1	2	3	2	1	2	1	0	1	0

A string has a *good count* if its running count never goes negative and ends with 0. So the second string above has a good count, but the first one does not because its count went negative at the third step. Let

$$\text{GoodCount} ::= \{s \in \{],[\}^* \mid s \text{ has a good count}\}.$$

The empty string has a length 0 running count we'll take as a good count by convention, that is, $\lambda \in$ GoodCount. The matched strings can now be characterized precisely as this set of strings with good counts.

(a) Prove that GoodCount contains RecMatch by structural induction on the definition of RecMatch.

Solution. We prove by induction on the definition of RecMatch (that is, structural induction) that every element of RecMatch counts well, so RecMatch is contained in GoodCount. The induction hypothesis is

$$P(s) ::= s \in \text{GoodCount}.$$

Proof. **Base Case:** $P(\lambda)$ holds since the count of the empty string ends when it starts at zero.

Inductive Step: Assume $P(s)$ and $P(t)$ are true. We need to show that $P([\,s\,]\,t)$ is true.

The count values for $[\,s\,]\,t$ start with 0. Reading the initial left bracket yields 1 as the next count value. This 1 serves as the start of a series of count values exactly equal to the count values of s, with each value incremented by one. Since $s \in$ GoodCount by hypothesis, these incremented count values begin with 1, always stay positive, and end with 1. The right bracket immediately after s reduces the ending count to 0. This 0 serves as the start of the remaining count values which are exactly the count values of t. Since

[1] The set, RecMatch, of strings of brackets is defined recursively as follows:

- **Base case:** $\lambda \in$ RecMatch.
- **Constructor case:** If $s, t \in$ RecMatch, then $[\,s\,]\,t \in$ RecMatch.

$t \in$ GoodCount, these remaining values never go negative and end at 0. Hence the entire sequence of count values for $[\, s \,]\, t$ starts with 0, never goes negative, and ends with 0, which proves that $[\, s \,]\, t \in$ GoodCount.

■

(b) Conversely, prove that RecMatch contains GoodCount.

Hint: By induction on the length of strings in GoodCount. Consider when the running count equals 0 for the second time.

Solution. *Proof.* We show that every string $r \in$ GoodCount is in RecMatch by strong induction on the length of r. The induction hypothesis is

$$Q(n) ::= \forall r \in \text{GoodCount}.\, |r| = n \text{ IMPLIES } r \in \text{RecMatch}.$$

Base Case $n = 0$: In this case there is only one string of length n, namely the empty string, which is in RecMatch by definition, proving $Q(0)$.

Inductive Step: Assume that $Q(k)$ is true for all $k \leq n$, we need to prove that $Q(n+1)$ is also true.

So suppose r is a length $n+1$ string that counts well. We must prove that $r \in$ RecMatch.

Now since r has a good count, it must start with a left bracket (or else the count would immediately go negative). Likewise, since the count for r returns to the value 0 by the end, r must end with right bracket. So there must be a *first* right bracket in r after which the count returns to 0. Let s be the substring of r between the initial left bracket and this right bracket. So

$$r = [\, s \,]\, t$$

for some string t.

Since counts only change by one as each bracket character is read, and the count for r *first* returns to 0 after the right bracket following s, the count during s must start and end with 1 and must stay *positive* in between. But this implies that a count for s alone, which would start with 0, would also end with 0 and stay *nonnegative* in between. That is, s by itself has a good count. Since the length of $s \in$ GoodCount is less than the length of r, we have by strong induction that $s \in$ RecMatch.

Further, we know the count for r returns to 0 after the right bracket following s, and since $r \in$ GoodCount, the count ends with 0 again and stays nonnegative in between. But this implies that t has a good count, and since the length of t is less than the length of r, we have by strong induction that $t \in$ RecMatch. Now by the second case in the definition of RecMatch, we conclude $r = [\, s \,]\, t \in$ RecMatch.

■

Problem 2. (a) Use the Pulverizer to find the inverse of 13 modulo 23 in the interval $[1, 23)$.

Solution. We first use the Pulverizer to find s, t such that $\gcd(23, 13) = s \cdot 23 + t \cdot 13$, namely,

$$1 = 4 \cdot 23 - 7 \cdot 13.$$

This implies that -7 is an inverse of 13 modulo 23.

Here is the Pulverizer calculation:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
23	13	10	$=$	$23 - 13$
13	10	3	$=$	$13 - 10$
			$=$	$13 - (23 - 13)$
			$=$	$(-1) \cdot 23 + 2 \cdot 13$
10	3	1	$=$	$10 - 3 \cdot 3$
			$=$	$(23 - 13) - 3 \cdot ((-1) \cdot 23 + 2 \cdot 13))$
			$=$	$\boxed{4 \cdot 23 - 7 \cdot 13}$
3	1	0	$=$	

To get an inverse in the specified range, simply find $\text{rem}(-7, 23)$, namely **16**.

■

(b) Use Fermat's theorem to find the inverse of 13 modulo 23 in $[1, 23)$.

Solution. Since 23 is prime, Fermat's theorem implies $13^{23-2} \cdot 13 \equiv 1 \pmod{23}$ and so $\text{rem}(13^{23-2}, 23)$ is the inverse of 13 in the range $\{1, \ldots, 22\}$. Now using the method of repeated squaring, we have the following congruences modulo 23:

$$\begin{aligned}
13^2 &= 169 \\
&\equiv \text{rem}(169, 23) = 8 \\[1em]
13^4 &\equiv 8^2 \\
&= 64 \\
&\equiv \text{rem}(64, 23) = 18 \\[1em]
13^8 &\equiv 18^2 \\
&= 324 \\
&\equiv \text{rem}(324, 23) = 2 \\[1em]
13^{16} &\equiv 2^2 \\
&= 4 \\[1em]
13^{21} &= 13^{16} \cdot 13^4 \cdot 13 \\
&\equiv 4 \cdot 18 \cdot 13 \\
&= (4 \cdot 6) \cdot (3 \cdot 13) \\
&= 24 \cdot 39 \\
&\equiv 1 \cdot 39 \\
&\equiv \text{rem}(39, 23) = \boxed{16}.
\end{aligned}$$

← How did they find this

■

Problem 3.
Define the Pulverizer State machine to have:

$$\begin{aligned}
\text{states} &::= \mathbb{N}^6 \\
\text{start state} &::= (a, b, 0, 1, 1, 0) \qquad \text{(where } a \geq b > 0\text{)} \\
\text{transitions} &::= (x, y, s, t, u, v) \longrightarrow \\
&\quad (y,\ \text{rem}(x, y),\ u - sq,\ v - tq,\ s,\ t) \qquad \text{(for } q = \text{qcnt}(x, y), y > 0\text{)}.
\end{aligned}$$

(a) Show that the following properties are preserved invariants of the Pulverizer machine:

$$\gcd(x, y) = \gcd(a, b), \tag{1}$$

$$sa + tb = y, \text{ and} \tag{2}$$

$$ua + vb = x. \tag{3}$$

Solution. To verify that these are preserved invariants, suppose

$$(x, y, s, t, u, v) \longrightarrow (x', y', s', t', u', v').$$

Note that (1) is the same one we observed for the Euclidean algorithm. This leaves proving that (2) and (3) hold for the new state x', y', s', t', u', v'.

Now according to the procedure, $u' = s, v' = t, x' = y$, so (3) holds for u', v', x' because of (2) for s, t, y. Also,

$$s' = u - qs, \quad t' = v - qt, \quad y' = x - qy$$

where $q = \text{qcnt}((, x), y)$, so

$$s'a + t'b = (u - qs)a + (v - qt)b = ua + vb - q(sa + tb) = x - qy = y',$$

and therefore (2) holds for s', t', y'. ■

(b) Conclude that the Pulverizer machine is partially correct.

Solution. We claim that on termination, the values of s and t at termination are the desired coefficients, that is,

$$\gcd(a, b) = sa + tb.$$

To prove this, we first check that all three preserved invariants are true just before the first time around the loop. Namely, at the start:

$$x = a, y = b, s = 0, t = 1 \qquad \text{so}$$

$$sa + tb = 0a + 1b = b = y \qquad \text{confirming (2).}$$

Also,

$$u = 1, v = 0, \qquad \text{so}$$

$$ua + vb = 1a + 0b = a = x \qquad \text{confirming (3).}$$

Now by the Invariant Principle, they are true at termination. But at termination, $y \mid x$ so preserved invariants (1) and (2) imply

$$\gcd(a, b) = \gcd(x, y) = y = sa + tb.$$

so we have the desired coefficients s and t. ■

(c) Explain why the machine terminates after at most the same number of transitions as the Euclidean algorithm.

Solution. Note that x, y follows the transition rules of the Euclidean algorithm state machine given in equation (8.3), except that this extended machine stops one step sooner. ■

3/4

Mathematics for Computer Science
MIT 6.042J/18.062J

Euler's Theorem

Albert R Meyer March 4, 2011 lec 5F.1

Euler ϕ function

$\phi(n)$ ::=

k $\in$ [0,n) s.t.

k has a (mod n) inverse

Albert R Meyer March 4, 2011 lec 5F.2

Euler ϕ function

$\phi(n)$ ::= # k $\in$ [0,n) s.t.
k rel. prime to n

$\phi(7) = 6$ 1,2,3,4,5,6

$\phi(12) = 4$

0,1,2,3,4,5,6,7,8,9,10,11

Albert R Meyer March 4, 2011 lec 5F.3

Calculating ϕ

If p prime, everything in [1,p) is rel. prime to p, so

$\phi(p) = p - 1$

Albert R Meyer March 4, 2011 lec 5F.4

Euler ϕ function

$\phi(9)$? 0,1,2,3,4,5,6,7,8

k rel. prime to 9 iff
k rel. prime to 3
3 divides every 3rd number

so, $\phi(9) = 9-(9/3) = 6$

Albert R Meyer March 4, 2011 lec 5F.5

Calculating $\phi(p^k)$

$0,1,\dots,p,\dots,2p,\dots\dots,p^k-p,\dots,p^k-1$

p divides every pth number

p^k/p of these numbers are not rel. prime to p^k

Albert R Meyer March 4, 2011 lec 5F.6

Calculating $\phi(p^k)$

so

$$\phi(p^k) = p^k - p^{k-1}$$

Calculating $\phi(a \cdot b)$

Lemma :

For a, b *relatively prime*,

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

pf: Class prob. Another way later by "counting."

Calculating $\phi(a \cdot b)$

$$\phi(12) = \phi(3 \cdot 4)$$
$$= \phi(3) \cdot \phi(4)$$
$$= (3 - 1) \cdot (2^2 - 2^{2-1})$$
$$= 2 \cdot (4 - 2) = 4$$

Euler's Theorem

For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Fermat's "Little" Theorem

special case:

$$k^{p-1} \equiv 1 \pmod{p}$$

for prime p

Proof of Euler's Theorem

n^* ::= $\{m \in [1,n) \mid m \text{ rel prime to } n\}$

Note: $m,k \in n^*$ implies

$$\text{rem}(mk,n) \in n^*$$

Proof of Euler's Theorem

n^* ::=

$\{m \in [1,n) \mid m$ rel prime to $n\}$

lemma:

mult by $k \in n^*$, permutes n^*

permuting (mod 9)

$\phi(9) = 3^2 - 3 = 6$

9*=	1	2	4	5	7	8

permuting (mod 9)

$\phi(9) = 3^2 - 3 = 6$

9*=	1	2	4	5	7	8
2·	2	4	8	1	5	7

permuting (mod 9)

$\phi(9) = 3^2 - 3 = 6$

9*=	1	2	4	5	7	8
2·	2	4	8	1	5	7
7·	7	5	1	8	4	2

Proof of Euler's Thm

say $n^* = \{m_1, m_2, \ldots, m_s\}$, $k \in n^*$

none of $m_1k, m_2k, \ldots, m_sk$

$\equiv$ (mod n) because k cancels

so each $m_ik \equiv m_j \pmod{n}$

for a unique m_j.

Proof of Euler's Thm

in particular,

$m_1 \cdot m_2 \cdots \cdot m_s$

$\equiv (m_1k) \cdot (m_2k) \cdots (m_sk) \pmod{n}$

now cancel the m_i's

Proof of Euler's Thm

in particular,

$$1 \equiv (\ k)\cdot(\ k)\cdots(\ k) \quad (\text{mod } n)$$

Proof of Euler's Thm

in particular,

$$1 \equiv k^s \quad (\text{mod } n)$$

Proof of Euler's Thm

in particular,

$$1 \equiv k^{\phi(n)} \quad (\text{mod } n)$$

QED

Team Problems

Problems

1–4

6042 Euler's Theorem

Last time: modular arithmetic
- lots of stuff works
- cancelation only works if cancle modula relativly prime

What happens when you raise # to a power w/ mod

ϕ = # elements reltivly prime to n

k {0, 1, 2, ..., n-1} (never included) [0, 1)
Cancleable

k has a (mod n) inverse

$\phi(7)$ = 1, 2, 3, 4, 5, 6 so 6
Since 7 is a prime, only divisors 1, 7 so all # not 0 reltativly prim

relatively prime: gcd(7,) = 1 (all the #) (wrong I think)

$\phi(12)$ = 1, 5, 7, 11 = 4
Should have no common factor other than 1

Calculating ϕ: If p prime, everything in [1, p) is rel. prime to p
$\phi(p) = p - 1$

②

$\phi(9) = 0, 1, 2, 3, 4, 5, 6, 7, 8$

k rel to prime to 9 iff k rel prime to 3

3 divides every 3 rd #

0, 3, 6 bad

All the others are good

$\phi(9) = 9 - \frac{9}{3} = 6$

↑ since 3 is ___

$\phi(p^k) = 0, 1, \ldots p, 2 \cdot p, \ldots, p^k - p, \ldots, p^k - 1$

p divides every pth #

$\frac{p^k}{p}$ of the # are not rel prime to p^k

so $\phi(p^k) = p^k - \frac{p^k}{p}$

$p^k - p^{k-1}$

(3)

Calculating $\phi(a \cdot b)$

For a, b relatively prime ← only if

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

Chinese Remainder Theorm

Think of working w/ pairs of # mod a, mod b

Questions turn into questions about pairs

↑ multiplicitivity

~~Appli~~ Proof > class problem

$\phi(12) = \phi(3) \cdot \phi(4)$ 3, 4 have no primes in common

$= \phi(3 \cdot 4) =$

$= (3-1) \cdot (2^2 - 2^{2-1})$ apply formula

$= 2 \cdot (4-2) = 4$

Finding ϕ is hard if you don't know how to factor n

Can find factors easily if know ϕ

Normally factoring is easy

(4)

For k relatively prime to n,

$k^{\phi(n)} \equiv 1 \pmod{n}$

Special case

$k^{p-1} \equiv 1 \pmod{p}$

Called Fermat's "Little" Theorem

Gives easy way to detect that # is not prime

Raise the # to the power (mod)

If does not come at 1, then not prime

Half of not-prime # will fail the test ~~once~~

Then odds is ~~[illegible]~~ $\frac{1}{2^{100}}$

which is very good odds

~~Very~~

(need to look over more)

Proof $n^* := \{m \in [1, n) \mid m$ rel prime to $n\}$

Note $m, k \in n^*$ implies $m \cdot k$ rel prime to n

- otherwise where would the #s come from

implies $rem(mk, n) \in n^*$

⑤

lemma: mult by $k \in n^*$ permutates n^*
(reorder

$\phi(9) = 3^2 - 3 = 6$

$9^* = 1, 2, 4, 5, 7, 8$

pick a # from list - say 2
multiply by that (mod 9)

$2 \cdot | \; 2 \; 4 \; 8 \; 1 \; 5 \; 7$ — same #, but in diff order!

$7 | \; 7 \; 5 \; 1 \; 8 \; 4 \; 2$

Say $n^* = \{m_1, m_2, m_3, \ldots, m_s\}$ $k \in n^*$

Multiply all by k

$m_1 k, m_2 k, \ldots, m_s k$

$\equiv$ (mod n) because k cancels

So each $m_i k \equiv m_j$ (mod n)
for a unique m_j

(6)

in particular

$$m_1 \cdot m_2 \cdot \cdots m_s$$

$$\equiv (m_1 k) \cdot (m_2 k) \cdots (m_s k) \pmod{n}$$

Now cancel the m_i's

$$1 \equiv k \cdot k \cdot \ldots \cdot k \mod n$$

$$\equiv k^s$$

$s = \#$ of elements rel prime to n

$$= k^{\phi(n)}$$

$\square$