GCD and the Euclidian Algorithm

Warm-up

Try to prove $(a/b)c \equiv (a/c)b$ if $a \neq kbc$ then $a/c \equiv a/b$ or $a/c$

activity pdf will be up in a minute

I got stuck.

We'll introduce a new technique to get around this.

is up now
Extra Set Practice

Show $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof:
First, we'll show: $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Let $x$ be an arbitrary element of $A \cup (B \cap C)$.

Then by definition of $\cup, \cap$ we have:
$x \in A \lor (x \in B \land x \in C)$

Applying the distributive law, we get
$(x \in A \lor x \in B) \land (x \in A \lor x \in C)$

Applying the definition of union, we have:
$x \in (A \cup B)$ and $x \in (A \cup C)$

By definition of intersection we have $x \in (A \cup B) \cap (A \cup C)$.

So $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Now we show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

Let $x$ be an arbitrary element of $(A \cup B) \cap (A \cup C)$.

By definition of intersection and union, $(x \in A \lor x \in B) \land (x \in A \lor x \in C)$

Applying the distributive law, we have $x \in A \lor (x \in B \land x \in C)$

Applying the definitions of union and intersection, we have $x \in A \cup (B \cap C)$

So $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Combining the two directions, since both sets are subsets of each other, we have $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. 
Suppose $A \subseteq B$. Show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Let $A, B$ be arbitrary sets such that $A \subseteq B$.

Let $X$ be an arbitrary element of $\mathcal{P}(A)$.

By definition of powerset, $X \subseteq A$.

Since $X \subseteq A$, every element of $X$ is also in $A$. And since $A \subseteq B$, we also have that every element of $X$ is also in $B$.

Thus $X \in \mathcal{P}(B)$ by definition of powerset.

Since an arbitrary element of $\mathcal{P}(A)$ is also in $\mathcal{P}(B)$, we have $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
Extra Set Practice

Disprove: If $A \subseteq (B \cup C)$ then $A \subseteq B$ or $A \subseteq C$

Consider $A = \{1,2,3\}$, $B = \{1,2\}$, $C = \{3,4\}$.

$B \cup C = \{1,2,3,4\}$ so we do have $A \subseteq B$, but $A \not\subseteq B$ and $A \not\subseteq C$.

When you disprove a $\forall$, you’re just providing a counterexample (you’re showing $\exists$) – your proof won’t have “let $x$ be an arbitrary element of $A$."

$P(A \cap B) = P(\{2,3\}) = \{\emptyset, \{2\}, \{3\}, \{2,3\}\}$

$P(A \cup B) = P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$
Facts about modular arithmetic

For all integers $a, b, c, d, n$ where $n > 0$:

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

$a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.

$a \% n = (a - n) \% n$.

We didn’t prove the first, it’s a good exercise! You can use it as a fact as though we had proven it in class.
Another Proof

For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let $a, b, c$ be arbitrary integers, and suppose $a \nmid (bc)$.

Then there is not an integer $z$ such that $az = bc$.

There is not an integer $x$ such that $ax = b$, or there is not an integer $y$ such that $ay = c$.

So $a \nmid b$ or $a \nmid c$.
Another Proof

For all integers, \(a, b, c\): Show that if \(a \nmid (bc)\) then \(a \nmid b\) or \(a \nmid c\).

Proof:
Let \(a, b, c\) be arbitrary integers, and suppose \(a \nmid (bc)\).
Then there is not an integer \(z\) such that \(a \cdot z = bc\).

So \(a \nmid b\) or \(a \nmid c\).

There has to be a better way!
Another Proof

For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

There has to be a better way!
If only there were some equivalent implication...
One where we could negate everything...

Take the contrapositive of the statement:
For all integers, $a, b, c$: Show if $a \mid b$ and $a \mid c$ then $a \mid (bc)$. 
Claim: For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let $a, b, c$ be arbitrary integers, and suppose $a \mid b$ and $a \mid c$.

Therefore $a \mid bc$
By contrapositive

Claim: For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let $a, b, c$ be arbitrary integers, and suppose $a|b$ and $a|c$.

By definition of divides, $ax = b$ and $ay = c$ for integers $x$ and $y$.

Multiplying the two equations, we get $axay = bc$

Since $a, x, y$ are all integers, $xay$ is an integer. Applying the definition of divides, we have $a|bc$.

So for all integers $a, b, c$ if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$. 
Try it yourselves!

Show for any sets $A, B, C$: if $A \not\subseteq (B \cup C)$ then $A \not\subseteq C$.

1. What do the terms in the statement mean?
2. What does the statement as a whole say?
3. Where do you start?
4. What’s your target?
5. Finish the proof 😊

Fill out the poll everywhere for Activity Credit!

Go to pollev.com/cse311 and login with your UW identity
Or text cse311 to 22333
Try it yourselves!

Show for any sets $A, B, C$: if $A \not\subseteq (B \cup C)$ then $A \not\subseteq C$.

\[
\forall A \forall B \forall C \left( A \not\subseteq (B \cup C) \rightarrow A \not\subseteq C \right)
\]

Proof:

We argue by contrapositive,

Let $A, B, C$ be arbitrary sets, and suppose $A \subseteq C$.

Let $x$ be an arbitrary element of $A$. By definition of subset, $x \in C$. By definition of union, we also have $x \in B \cup C$. Since $x$ was an arbitrary element of $A$, we have $A \subseteq (B \cup C)$.

Since $A, B, C$ were arbitrary, we have: if $A \not\subseteq (B \cup C)$ then $A \not\subseteq C$. 
Primes and FTA

Prime
An integer \( p > 1 \) is prime iff its only positive divisors are 1 and \( p \). Otherwise it is “composite”

Fundamental Theorem of Arithmetic
Every positive integer greater than 1 has a unique prime factorization.

\[ 35 = 5 \cdot 7 \]
\[ 50 = 2 \cdot 5^2 \]
GCD and LCM

Greatest Common Divisor

The Greatest Common Divisor of $a$ and $b$ (gcd($a,b$)) is the largest integer $c$ such that $c|a$ and $c|b$.

\[
gcd(6,12) = 6 = \frac{1}{2}
\]

Least Common Multiple

The Least Common Multiple of $a$ and $b$ (lcm($a,b$)) is the smallest positive integer $c$ such that $a|c$ and $b|c$.

\[
\frac{1}{2} + \frac{2}{3} = \frac{3}{6} + \frac{4}{6} = \frac{7}{6}
\]
Try a few values...

\[
\begin{align*}
gcd(100,125) &= 25 \\
gcd(17,49) &= 1 \\
gcd(17,34) &= 17 \\
gcd(13,0) &= 13
\end{align*}
\]

\[
\begin{align*}
lcm(7,11) &= 77 \\
lcm(6,10) &= 30
\end{align*}
\]
public int Mystery(int m, int n){
    if(m<n){
        int temp = m;
        m=n;
        n=temp;
    }
    while(n != 0) {
        int rem = m % n;
        m=n;
        n=rem;
    }
    return m;
}
How do you calculate a gcd?

You could:

Find the prime factorization of each

Take all the common ones. E.g.

\[
gcd(24,20) = gcd(2^3 \cdot 3, 2^2 \cdot 5) = 2^{\min(2,3)} = 2^2 = 4.\]

(lcm has a similar algorithm – take the maximum number of copies of everything)

But that’s....really expensive. Mystery from a few slides ago finds gcd.
Two useful facts

**gcd Fact 1**

If $a, b$ are positive integers, then $\gcd(a, b) = \gcd(b, a \% b)$

Tomorrow’s lecture we’ll prove this fact. For now: just trust it.

**gcd Fact 2**

Let $a$ be a positive integer: $\gcd(a, 0) = a$

Does $a|a$ and $a|0$? Yes $a \cdot 1 = a$; $a \cdot 0 = 0$.
Does anything greater than $a$ divide $a$?
public int Mystery(int m, int n) {
    if (m < n) {
        int temp = m;
        m = n;
        n = temp;
    }
    while (n != 0) {
        int rem = m % n;
        m = n;
        n = rem;
    }
    return m;
}
Euclid’s Algorithm

\[ \text{gcd}(a, b) = \text{gcd}(b, \text{rem}) \checkmark \]

\[
\begin{align*}
gcd(660, 126) &= \text{gcd}(126, 660 \mod 126) = \text{gcd}(26, 30) \\
&= \text{gcd}(30, 26 \mod 30) = \text{gcd}(20, 6) \\
&= \text{gcd}(6, 20 \mod 6) = \text{gcd}(6, 0) \\
&= 6.
\end{align*}
\]

Tableau form

\[
\begin{pmatrix}
m & n \\
660 & 126 \\
126 & 30 \\
30 & 6 \\
30 & 0
\end{pmatrix}
\]

while(n != 0) {
    int rem = m % n;
    m=n;
    n=temp;
}
Euclid’s Algorithm

while(n != 0) {
    int rem = m % n;
    m = n;
    n = temp;
}

$\gcd(660, 126) = \gcd(126, 660 \mod 126) = \gcd(126, 30)$
$\quad = \gcd(30, 126 \mod 30) = \gcd(30, 6)$
$\quad = \gcd(6, 30 \mod 6) = \gcd(6, 0)$
$\quad = 6$

Tableau form

<table>
<thead>
<tr>
<th>Starting Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>660 = 5 \cdot 126 + 30</td>
</tr>
<tr>
<td>126 = 4 \cdot 30 + 6</td>
</tr>
<tr>
<td>30 = 5 \cdot 6 + 0</td>
</tr>
</tbody>
</table>
Bézout’s Theorem

If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that
$$\gcd(a,b) = sa + tb$$

We’re not going to prove this theorem...
But we’ll show you how to find $s,t$ for any positive integers $a, b$. 
Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.
Step 2 solve all equations for the remainder.
Step 3 substitute backward

gcd(35,27)
Extended Euclidian Algorithm

Step 1 compute \( \text{gcd}(a,b) \); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

\[
\begin{align*}
gcd(35,27) &= gcd(27, 35 \% 27) = gcd(27,8) \\
&= gcd(8, 27 \% 8) = gcd(8, 3) \\
&= gcd(3, 8 \% 3) = gcd(3, 2) \\
&= gcd(2, 3 \% 2) = gcd(2, 1) \\
&= gcd(1, 2 \% 1) = gcd(1, 0)
\end{align*}
\]

\[
\begin{align*}
35 &= 1 \cdot 27 + 8 \\
27 &= 3 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{align*}
\]
Extended Euclidian Algorithm

Step 1 compute $\gcd(a,b)$; keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

\[
\begin{align*}
35 &= 1 \cdot 27 + 8 \\
27 &= 3 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{align*}
\]
Extended Euclidian Algorithm

Step 1 compute $\text{gcd}(a,b)$; keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

\[
\begin{align*}
35 & = 1 \cdot 27 + 8 \\
27 & = 3 \cdot 8 + 3 \\
8 & = 2 \cdot 3 + 2 \\
3 & = 1 \cdot 2 + 1 \\
\end{align*}
\]

\[
\begin{align*}
8 & = 35 - 1 \cdot 27 \\
3 & = 27 - 3 \cdot 8 \\
2 & = 8 - 2 \cdot 3 \\
1 & = 3 - 1 \cdot 2 \\
\end{align*}
\]
Extended Euclidian Algorithm

Step 1 compute $\gcd(a,b)$; keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

\[ \gcd(a,b) = sa + tb \]

\[
\begin{align*}
\text{Step 1:} & \quad 8 = 35 - 1 \cdot 27 \\
& \quad 3 = 27 - 3 \cdot 8 \\
& \quad 2 = 8 - 2 \cdot 3 \\
& \quad 1 = 3 - 1 \cdot 2 \\
\text{Step 2:} & \quad 1 = -10 \cdot 35 + 13 \cdot 27 \\
\end{align*}
\]
Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.
Step 2 solve all equations for the remainder.
Step 3 substitute backward

\[
\begin{align*}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= -1 \cdot 8 + 2 \cdot 3
\end{align*}
\]
Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

\[
\begin{align*}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{align*}
\]

\[
\begin{align*}
\text{gcd}(27,35) &= 13 \cdot 27 + (-10) \cdot 35
\end{align*}
\]

When substituting back, you keep the larger of \( m, n \) and the number you just substituted. Don’t simplify further! (or you lose the form you need)
So...what’s it good for?

Suppose I want to solve $7x \equiv 1 \pmod{n}$

Just multiply both sides by $\frac{1}{7}$...

Oh wait. We want a number to multiply by 7 to get 1.

If the $\gcd(7,n) = 1$

Then $s \cdot 7 + tn = 1$, so $7s - 1 = -tn$ i.e. $n|(7s - 1)$ so $7s \equiv 1 \pmod{n}$.

So the $s$ from Bézout’s Theorem is what we should multiply by!
Try it

Solve the equation $7y \equiv 3 \pmod{26}$

What do we need to find?
The multiplicative inverse of $7 \pmod{26}$

$\gcd(26, 7)$
Finding the inverse...

gcd(26,7) = gcd(7, 26%7) = gcd(7,5)
   = gcd(5, 7%5) = gcd(5,2)
   = gcd(2, 5%2) = gcd(2, 1)
   = gcd(1, 2%1) = gcd(1,0) = 1.

26 = 3 \cdot 7 + 5 ; 5 = 26 - 3 \cdot 7
7 = 5 \cdot 1 + 2 ; 2 = 7 - 5 \cdot 1
5 = 2 \cdot 2 + 1 ; 1 = 5 - 2 \cdot 2

1 = 5 - 2 \cdot 2
   = 5 - 2(7 - 5 \cdot 1)
   = 3 \cdot 5 - 2 \cdot 7
   = 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7
   = 3 \cdot 26 - 11 \cdot 7

\(-11\) is a multiplicative inverse.
We'll write it as 15, since we're working mod 26.
Try it

Solve the equation $7y \equiv 3 \pmod{26}$

What do we need to find?
The multiplicative inverse of $7 \pmod{26}$.

$15 \cdot 7 \cdot y \equiv 15 \cdot 3 \pmod{26}$

$y \equiv 45 \pmod{26}$

Or $y \equiv 19 \pmod{26}$

So $26 \mid 19 - y$, i.e. $26k = 19 - y$ (for $k \in \mathbb{Z}$) i.e. $y = 19 - 26 \cdot k$ for any $k \in \mathbb{Z}$

So $\{..., -7, 19, 45, ... 19 + 26k, ... \}$
And now, for some proofs!
GCD fact

If $a$ and $b$ are positive integers, then $\text{gcd}(a,b) = \text{gcd}(b, a \% b)$

How do you show two gcds are equal?

Call $a = \text{gcd}(w, x), b = \text{gcd}(y, z)$

If $b|w$ and $b|x$ then $b$ is a common divisor of $w, x$ so $b \leq a$

If $a|y$ and $a|z$ then $a$ is a common divisor of $y, z$, so $a \leq b$

If $a \leq b$ and $b \leq a$ then $a = b$
gcd(a,b) = gcd(b, a % b)

Let \( x = \gcd(a, b) \) and \( y = \gcd(b, a \% b) \).

We show that \( y \) is a common divisor of \( a \) and \( b \).

By definition of gcd, \( y \mid b \) and \( y \mid (a \% b) \). So it is enough to show that \( y \mid a \).

Applying the definition of divides we get \( b = yk \) for an integer \( k \), and \( (a \% b) = yj \) for an integer \( j \).

By definition of mod, \( a \% b \) is \( a = qb + (a \% b) \) for an integer \( q \).

Plugging in both of our other equations:
\[
a = qyk + yj = y(qk + j).
\]
Since \( q, k, \) and \( j \) are integers, \( y \mid a \). Thus \( y \) is a common divisor of \( a, b \) and thus \( y \leq x \).
gcd(a,b) = gcd(b, a % b)

Let x = gcd(a, b) and y = gcd(b, a%b).

We show that x is a common divisor of b and a%b.

By definition of gcd, x|b and x|a. So it is enough to show that x|(a%b).

Applying the definition of divides we get b = xk' for an integer k', and a = xj' for an integer j'.

By definition of mod, a%b is a = qb + (a%b) for an integer q

Plugging in both of our other equations:

xj' = qxk' + a%b. Solving for a%b, we have a%b = xj' - qxk' = x(j' - qk'). So x|(a%b). Thus x is a common divisor of b, a%b and thus x ≤ y.
\[ \text{gcd}(a,b) = \text{gcd}(b, a \% b) \]

Let \( x = \text{gcd}(a, b) \) and \( y = \text{gcd}(b, a \% b) \).

We show that \( x \) is a common divisor of \( b \) and \( a \% b \).

We have shown \( x \leq y \) and \( y \leq x \).

Thus \( x = y \), and \( \text{gcd}(a, b) = \text{gcd}(b, a \% b) \).