Even More Number Theory

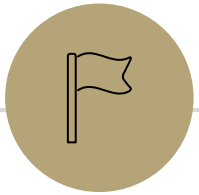
CSE 311 25 Au
Lecture 13

Outline for today

English Proof Practice!

One more proof technique (it's an easy one ☺)

Some More Number Theory



More Mod proofs

More proofs

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Step 1: What do the words mean?

Step 2: What does the statement as a whole say?

Step 3: Where do we start?

Step 4: What's our target?

Step 5: Now prove it.

Another Proof

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let a, b, c, d, n be arbitrary integers, with $n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$ac \equiv bd(mod\ n)$

Another Proof

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let a, b, c, d, n be arbitrary integers, with $n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd(mod\ n)$

Another Proof

Show that if $a \equiv b(mod\, n)$ and $c \equiv d\ (mod\, n)$ then $ac \equiv bd\ (mod\, n)$.

Let a, b, c, d, n be arbitrary integers, with $n \geq 0$
and suppose $a \equiv b(mod\, n)$ and $c \equiv d\ (mod\, n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$nknj = (d-c)(b-a)$ by multiplying the two equations

$nknj = (bd - bc - ad + ac)$

…

$n?? = bd - ac$

$n|(bd-ac)$

$ac \equiv bd(mod\, n)$

Another Proof

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let a, b, c, d, n be arbitrary integers, with $n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$nknj = (d-c)(b-a)$ by multiplying the two equations

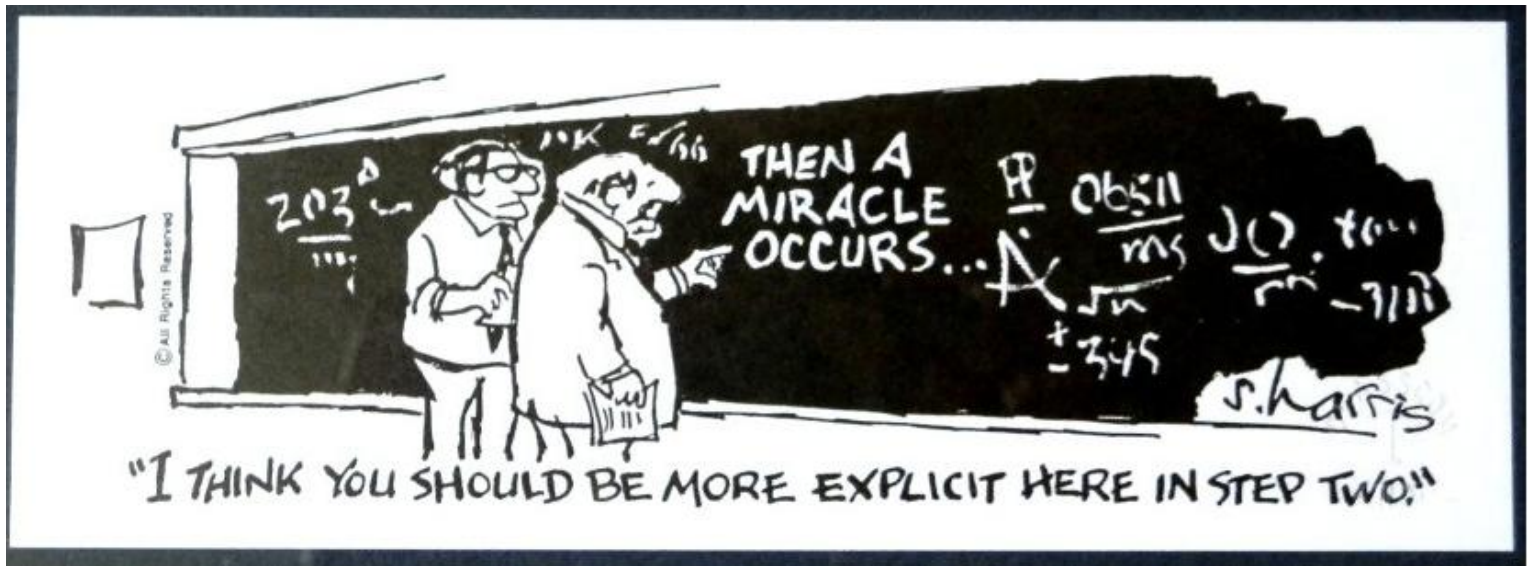
$nknj = (bd - bc - ad + ac)$

And then a miracle occurs

$n?? = bd - ac$

$n|(bd - ac)$

$ac \equiv bd(mod\ n)$



Uh-Oh

We hit (what looks like) a dead end.

But how did I know we hit a dead end? Because I knew exactly where we needed to go. If you didn't, you'd have been staring at that for ages trying to figure out the magic step.

(or worse, assumed you lost a minus sign somewhere, and just "fixed" it….)

Let's try again. This time, let's **separate** b from a and d from c before combining.

Another Approach

Show that if $a \equiv b(mod\, n)$ and $c \equiv d\ (mod\, n)$ then $ac \equiv bd\ (mod\, n)$.

Let a, b, c, d, n be arbitrary integers, with $n \geq 0$
and suppose $a \equiv b(mod\, n)$ and $c \equiv d\ (mod\, n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

$b = nk + a, d = nj + c$

$bd = (nk+a)(nj+c)$

$n??= bd - ac$

$n|(bd - ac)$

$ac \equiv bd(mod\, n)$

Another Approach

Show that if $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$ then $ac \equiv bd\ (mod\ n)$.

Let a, b, c, d, n be arbitrary integers, with $n \geq 0$
and suppose $a \equiv b(mod\ n)$ and $c \equiv d\ (mod\ n)$.

$n|(b-a)$ and $n|(d-c)$ by definition of mod.

$nk = (b-a)$ and $nj = (d-c)$ for integers j, k by definition of divides.

Rearranging the equations, we have: $b = nk + a, d = nj + c$,

Multiplying the equatiosn together, we get: $bd = (nk+a)(nj+c) = n^2kj + anj + cnk + ac$

Rearranging, $bd - ac = n^2kj + anj + cnk = n(nkj + aj + ck)$

That is, $n(nkj + aj + ck) = bd - ac$. Note that n, k, j, a, c, k are all integers so multiplying and adding them gives another integer. Thus $bd - ac$ is n times an integer.

$n|(bd - ac)$ by definition of divides

$ac \equiv bd(mod\ n)$. (by definition of equivalence mod n) Since a, b, c, d, n were arbitrary, the claim always holds.

Some Style Notes

When applying a definition, be sure to explicitly check all pieces of the definition.

$a|b$ means there is an integer z such that $az = b$.

Since z needs to be an integer in the definition, make sure it's an integer when you apply that definition.

Every step should have a justification. Sometimes it's very short ("rearranging this equation" or "doing some algebra"); sometimes it's much more detailed.

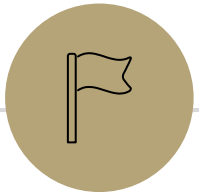
Arbitrary variables are always explicitly called arbitrary.

Use fresh variable names from an exists. (k, j)

Some Style Notes

You'll often see something that looks a lot like our equivalence proofs if you have a sequence of algebra steps

$$bd = (nk + a)(nj + c) \quad \text{(multiplying equations together)}$$
$$= n^2kj + anj + cnk + ac \text{ (FOILing)}$$
$$= n(nkj + aj + ck) + ac \text{ (factoring out } n\text{)}$$



Proving a biconditional

Warm up

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Show that $a \equiv b \ (mod\ n)$ if and only if $b \equiv a (mod\ n)$

How do you prove an if and only if?

Proving a biconditional

How do we prove $p \leftrightarrow q$

Two options:

1. (preferred style for this class): show $p \rightarrow q$, then show $q \rightarrow p$.
2. Show a "chain of if-and-only-if"s (possible, but stylistically difficult)

Two proofs

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b-a)$

Show that $a \equiv b \ (mod\ n)$ if and only if $b \equiv a (mod\ n)$

Forward direction (if $a \equiv b (mod\ n)$ then $b \equiv a \ (mod\ n)$)

Let a, b, n be arbitrary integers with $n > 0$; suppose $a \equiv b (mod\ n)$. By definition of equivalence: $n|(b-a)$. By definition of mod, $nk = b - a$ for some integer k. Multiplying by -1 we have $n(-k) = a - b$. But $-k$ is also an integer (since k was) so $n|(a-b)$, and (applying the definition of equivalence $b \equiv a \ (mod\ n)$

Backward direction (if $b \equiv a (mod\ n)$ then $a \equiv b \ (mod\ n)$)

Let a, b, n be arbitrary integers with $n > 0$; suppose $b \equiv a (mod\ n)$. By definition of equivalence: $n|(a-b)$. By definition of mod, $nj = a - b$ for some integer j. Multiplying by -1 we have $n(-j) = b - a$. But $-j$ is also an integer (since j was) so $n|(b-a)$, and (applying the definition of equivalence $a \equiv b \ (mod\ n)$

Or one proof

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Show that $a \equiv b \ (mod\ n)$ if and only if $b \equiv a (mod\ n)$

Let a, b, n be arbitrary integers with $n > 0$.

Observe that

$a \equiv b (mod\ n)$ if and only if $n|(b - a)$ (by definition of modular equiv)

If and only if $nk = b - a$ (where k is an integer)

If and only if $n(-k) = a - b$

If and only if $n|(a - b)$ (by definition of divides)

If and only if $b \equiv a (mod\ n)$ (by def of modular equiv).

Since a, b, n were arbitrary, the claim always holds.

To prove a biconditional

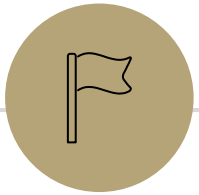
Option 1 is just to prove two implications (you know how to prove implications already---direct proof rule and/or contrapositive)

Option 2 is to connect the left and right sides with a sequence of "if and only if"s. **Every** step must be an if-and-only-if

Every step must explicitly be stated as an if-and-only-if.

(By default, proofs are like inference proofs: we're listing true facts that follow from prior facts; if you want to know a biconditional, you have to assert the biconditional explicitly).

Option 1 is usually the default; option 2 is sometimes used, especially for algebraic expressions.



Computing GCDs

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 $c|b$

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 $b|c$.

Try a few values…

gcd(100,125) =25

gcd(17,49)

gcd(17,34)

gcd(13,0) =13

lcm(7,11)

lcm(6,10)

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 finds gcd.

```
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;
}
```

Running Mystery

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.

GCD facts

1. gcd(a,0)=a

Pf: a is a common divisor ($a = 1 \cdot a$; $0 = 0 \cdot a$); larger numbers don't divide a (for positive numbers, if $x|y$ then $x \leq y$)

2. If a and b are positive integers, then gcd(a,b) = gcd(b, a % b)

Why is 2 true? The proof isn't easy; it's at the end of this deck.

Why should you care?

So…what's it good for?

Remember everything we're learning contributes to us eventually understanding RSA. This is a key step in generating keys.

Suppose I want to solve $7x \equiv 3 (mod\ n)$

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

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

What number can we pick?

The next two slides are going to get more abstract…we're listing out the facts we need to solve that equation.

Bézout's Theorem

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 it turns out `Mystery` can be extended to find them.

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.

$$26 = 3 \cdot 7 + 5 \; ; \; 5 = 26 - 3 \cdot 7$$

$$7 = 5 \cdot 1 + 2 \; ; \; 2 = 7 - 5 \cdot 1$$

$$5 = 2 \cdot 2 + 1 \; ; \; 1 = 5 - 2 \cdot 2$$

$$\begin{gathered} 1 = 5 - 2 \cdot 2 \\ = 5 - 2(7 - 5 \cdot 1) \\ = 3 \cdot 5 - 2 \cdot 7 \\ = 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 \\ 3 \cdot 26 - 11 \cdot 7 \end{gathered}$$

-11 is a multiplicative inverse of 7 for (mod 26) arithmetic!
We'll write that as 15, since we're working mod 26.

So…what's it good for?

Suppose I want to solve $7x \equiv 3 (mod\ n)$

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 $7s \equiv 1 (mod\ n)$.

So the s from Bézout's Theorem is what we should multiply by!

Ok…how am I supposed to find s, t?

It turns out that while you're calculating the gcd (using the Mystery algorithm), you can keep some extra information recorded, and end up with the s, t

This is called the "extended Euclidian algorithm"

Examples in these slides.

Try it

Solve the equation $7y \equiv 3(mod\ 26)$

What do we need to find?

The multiplicative inverse of $7(\mathbf{mod}\ 26)$

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.

$$26 = 3 \cdot 7 + 5 \; ; \; 5 = 26 - 3 \cdot 7$$

$$7 = 5 \cdot 1 + 2 \; ; \; 2 = 7 - 5 \cdot 1$$

$$5 = 2 \cdot 2 + 1 \; ; \; 1 = 5 - 2 \cdot 2$$

$$\begin{gathered} 1 = 5 - 2 \cdot 2 \\ = 5 - 2(7 - 5 \cdot 1) \\ = 3 \cdot 5 - 2 \cdot 7 \\ = 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 \\ 3 \cdot 26 - 11 \cdot 7 \end{gathered}$$

-11 is a multiplicative inverse of 7 for (mod 26) arithmetic!
We'll write that as 15, since we're working mod 26.

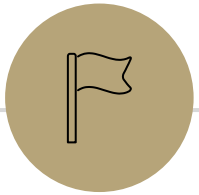
Try it

Solve the equation $7y \equiv 3(mod\ 26)$

What do we need to find?
The multiplicative inverse of $7\ (mod\ 26)$. We found it's 15.

$15 \cdot 7 \cdot y \equiv 15 \cdot 3(mod\ 26)$

$y \equiv 45(mod\ 26)$
Or $y \equiv 19(mod\ 26)$
So $26|19 - y$, i.e. $26k = 19 - y$ (for $k \in \mathbb{Z}$) i.e. $y = 19 - 26 \cdot k$ for any $k \in \mathbb{Z}$
Solutions: $\{\dots, -7, 19, 45, \dots 19 + 26k, \dots\}$ i.e. $\{x: x = 19 + 26k$ for some $k \in \mathbb{Z}\}$



Proving the key fact about gcds

gcd(a,b) = gcd(b, a % b)

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

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

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

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, $y|a$. Thus y is a common divisor of a, b and thus $y \leq x$.

gcd(a,b) = gcd(b, a % b)

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

We show that x is a common divisor of b and $\mathrm{a}\%b$.

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

Applying the definition of divides we get $b = xk'$ for an integer k', and $\mathrm{a} = xj'$ 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 $x \leq y$.

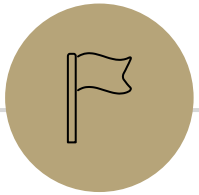
gcd(a,b) = gcd(b, a % b)

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

We show that x is a common divisor of b and $\mathrm{a}\%b$.

We have shown $x \leq y$ and $y \leq x$.

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



Euclidian Algorithm

Euclid's Algorithm

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

gcd(660,126)

Euclid's Algorithm

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

gcd(660,126) = gcd(126, 660 mod 126) = gcd(126, 30)
= gcd(30, 126 mod 30) = gcd(30, 6)
= gcd(6, 30 mod 6) = gcd(6, 0)
= 6

Tableau form

$$660 = 5 \cdot 126 + 30$$
$$126 = 4 \cdot 30 + 6$$
$$30 = 5 \cdot 6 + 0$$

Starting Numbers

Final answer

Bézout's Theorem

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 gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

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)

$$35 = 1 \cdot 27 + 8$$
$$27 = 3 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
35 &= 1 \cdot 27 + 8 \\
27 &= 3 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}
$$

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
35 &= 1 \cdot 27 + 8 \\
27 &= 3 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}
$$

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= -1 \cdot 8 + 2 \cdot 3
\end{aligned}
$$

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

gcd(27,35) = $13 \cdot 27 + (-10) \cdot 35$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= -1 \cdot 8 + 3 \cdot 3 \\
&= -1 \cdot 8 + 3(27 - 3 \cdot 8) \\
&= 3 \cdot 27 - 10 \cdot 8 \\
&= 3 \cdot 27 - 10(35 - 1 \cdot 27) \\
&= 13 \cdot 27 - 10 \cdot 35
\end{aligned}
$$

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)