More Number Theory

CSE 311 Autumn 2025
Lecture 11

Proof Practice

Over the next few weeks:

Practice direct proofs in English (formatting details, doing more examples)

See a few other proof techniques

Proof by contrapositive, proving an exists statement, proof by contradiction

All while learning some number theory.

Claim: for all integers $a, b, c, n,$ with $n > 0$:

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

Before we start, we must know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Equivalence in modular arithmetic

Let a, b, n be integers with $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Claim: for all integers a, b, c, n, with $n > 0$:

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

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$,
and suppose $a \equiv b \pmod{n}$.

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

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Equivalence in modular arithmetic

Let a, b, n be integers with $n > 0$.
We say $a \equiv b \pmod{n}$ if and only if $n|(b - a)$

A proof

Claim: for all integers $a, b, c, n,$ with $n > 0$:

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

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$,
and suppose $a \equiv b \pmod{n}$.

By definition of mod, $\mathrm{n}|(b - a)$

By definition of divides, $nk = (b - a)$ for some integer k.

Adding and subtracting c, we have $nk = ([b + c] - [\mathrm{a} + \mathrm{c}])$.

Since k is an integer $n|([b + c] - [a + c])$

By definition of mod, $a + c \equiv b + c \pmod{n}$. Since a, b, c, n were arbitrary, the claim holds for all integers a, b, c and positive integers n.

Logical Ordering (1)

When doing a proof, we often work from both sides…

But we have to be careful!

When you read from top to bottom, every step has to follow only from what's **before** it, not after it.

Suppose our target is q and I know $q \to p$ and $r \to q$.

What can I put as a "new target?"

Logical Ordering (2)

So why have all our prior steps been ok backward?

They've all been either:

A definition (which is always an "if and only if")

An algebra step that is an "if and only if"

A logical equivalence (can work in both directions)

Even if your steps are "if and only if" you still have to put everything in order – start from your assumptions, and only assert something once it can be shown.

A bad proof

Claim: if x is positive then $x + 5 = -x - 5$.

$x + 5 = -x - 5$

$|x + 5| = |-x - 5|$

$|x + 5| = |-(x + 5)|$

$|x + 5| = |x + 5|$

$0 = 0$

This claim is **false** – if you're trying to do algebra, you need to start with an equation you know (say $x = x$ or $2 = 2$ or $0 = 0$) and expand to the equation you want.

You Try!

Claim: for all integers a, b, c, n with $n > 0$:
If $a \equiv b \ (mod\ n)$ then $ac \equiv bc \ (mod\ n)$

Before we start we must know:
1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

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 $n|(b - a)$

You try---skeleton

Claim: for all integers $a, b, c, n,$ with $n > 0$:

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

Proof:

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

$ac \equiv bc\ (mod\ n)$

You try---the full proof

Claim: for all integers $a, b, c, n,$ with $n > 0$:

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

Proof:

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

By definition of mod $n|(b - a)$

By definition of divides, $nk = b - a$ for some integer k

Multiplying both sides by c, we have $n(ck) = bc - ac$.

Since c and k are integers, $n|(bc - ac)$ by definition of divides.

So, $ac \equiv bc\ (mod\ n)$, by the definition of mod. Since a, b, c, n were arbitrary, the claim holds for all integers a, b, c and positive integers n.

Don’t lose your intuition!

Let’s check that we understand “intuitively” what mod means:

$x \equiv 0 \pmod 2$

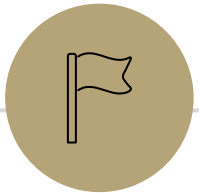
“x is even” Note that negative (even) x values also make this true.

$-1 \equiv 19 \pmod 5$

This is true! They both have remainder 4 when divided by 5.

$y \equiv 2 \pmod 7$

This is true as long as $y = 2 + 7k$ for some integer k



Small Techniques

Proof By [Counter]Example

To prove an existential statement (or *dis*prove a universal statement), provide an example, and demonstrate that it is the needed example.

You don't have to explain where it came from! (In fact, you **shouldn't)**

Computer scientists and mathematicians like to keep an air of mystery around our proofs.

(or more charitably, we want to focus on just enough to believe the claim)

Skeleton of an Exists Proof

To show $\exists x(P(x))$

Consider x =[the value that will work]

[Show that x does cause $P(x)$ to be true.]

So [value] is the desired x.

You'll probably need some "scratch work" to determine what to set x to. That might not end up in the final proof!

Exists proofs

Suppose I claim that for all integers, if x is even then $8|x^2$.

That…doesn't look right.

How do you prove me wrong?

Want to show: $\exists x\big(Even(x) \wedge \neg[8|x^2]\big)$

Consider $x = 6$. Then x is even (since $6 = 3 \cdot 2$), but 8 does not divide 36 (as $36\%8 = 4$).

Proof By Cases - motivation

If x is prime then x^2 is odd or $2|x$.

We need two different arguments – one for 2 and one for all the other primes…

Proof By Cases - example

Let x be an arbitrary prime number

We divide into two cases.

Case 1: x is even

If x is even then $x = 2k$ for some integer k, this is the definitions of $2|x$.

Case 2: x is odd

If x is odd, then $x = 2j + 1$ for some integer j. Squaring, we get
$x^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1.$
Since j is an integer $2j^2 + 2j$ is as well, so x^2 is odd by definition.

In either case, x met the condition of $2|x$ or x^2 is odd, so the claim is true.

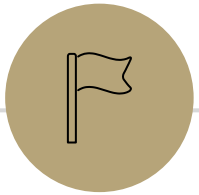
Proof By Cases

Make it clear how you decide which case you're addressing.

It should be obvious your cases are “exhaustive”

Reach the same conclusion in each of the cases, and you can say you’ve got that conclusion no matter what (outside the cases).

Advanced version: sometimes you end up arguing a certain case “can’t happen”



Proof by Contrapositive

Another Proof (statement)

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

Another Proof (initial skeleton)

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 $az = bc$

…

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 arbitrar c).

Then there is not an

…

so $a \nmid b$ or $a \nmid c$

There has to be a better way!

Another Proof (contrapositive)

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 $a|b$ and $a|c$ then $a|(bc)$.

By contrapositive (setup)

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 $a|c$.

Therefore $a|bc$

By contrapositive (complete)

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 $a|bc$.

Signs you might want to use proof by contrapositive

1. The hypothesis of the implication you're proving has a "not" in it (that you think is making things difficult)

2. The target of the implication you're proving has an "or" or "not" in it.

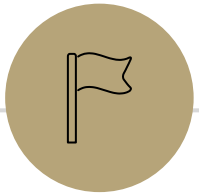
3. There's a step that is difficult forward, but easy backwards

   e.g., taking a square-root forward, squaring backwards.

4. You get halfway through the proof and you can't "get ahold of" what you're trying to show.

   e.g., you're working with a "not equal" instead of an "equals" or "every thing doesn't have this property" instead of "some thing does have that property"

All of these are reasons you **might** want contrapositive. Sometimes you just have to try and see what happens!



GCD and LCM

GCD and LCM definitions

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)

gcd(17,49)

gcd(17,34)

gcd(13,0)

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;
}
```