Even More Number Theory

CSE 311 Spring 2022
Lecture 13

Logical Ordering

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

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"

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.

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.

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)

gcd(17,49)

gcd(17,34)

gcd(13,0)

lcm(7,11)

lcm(6,10)

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 $b|c$.

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=temp;
      }
      return m;
}
```

GCD fact

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

Why is this true? The proof isn't easy, we'll do it next week.

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 $7x \equiv 1 (mod\ n)$

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 we'll show you in section how to find s,t for any positive integers a, b.

So…what's it good for?

Suppose I want to solve $7x \equiv 1 (mod\ n)$

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"

You'll walk through it in section on Thursday.

Facts about modular arithmetic

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

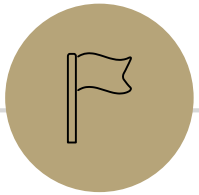
If $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$ then $a + c \equiv b + d (mod\ n)$.

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

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

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

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.



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 $x \leq y$.

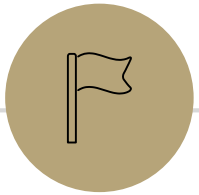
gcd(a,b) = gcd(b, a % b)

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 $\gcd(a, b) = \gcd(b, a\%b)$.



Extra Practice!

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 $b \equiv a (mod\ n)$

Show that $a\%n=(a-n)\%n$ Where $b\%c$ is the unique r such that $b = kc + r$ for some integer k.

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist *unique* integers q, r with $0 \leq r < d$ Such that $a = dq + r$

Warm up

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

$a \equiv b(mod\ n) \leftrightarrow n|(b-a) \leftrightarrow nk = b - a(\text{for } k \in \mathbb{Z}) \leftrightarrow$

$n(-k) = a - b(\text{for } -\text{k} \in \mathbb{Z}) \leftrightarrow n|(a-b) \leftrightarrow b \equiv a(mod\ n)$

Show that $a\%n=(a-n)\%n$ Where $b\%c$ is the unique r such that $b = kc + r$ for some integer k.

By definition of %, $a = qn + (a\%n)$ for some integer q. Subtracting n,

$a - n = (q-1)n + (a\%n)$. Observe that $q-1$ is an integer, and that this is the form of the division theorem for $(a-n)\%n$. Since the division theorem guarantees a unique integer, $(a-n)\%n = (a\%n)$

% and Mod

Other resources use mod to mean an operation (takes in an integer, outputs an integer). We will not in this course. mod only describes $\equiv$. It's not "just on the right hand side"

Define $a\%b$ to be "the r you get from the division theorem"
i.e. the integer r such that $0 \leq r < d$ and $a = bq + r$ for some integer q.

This is the "mod function"

I claim $a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$.

How do we show and if-and-only-if?

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Backward direction:

Suppose $a \equiv b(mod\ n)$

$a\%n = (b - nk)\%n = b\%n$

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Backward direction:

Suppose $a \equiv b(mod\ n)$

$n|b - a$ so $nk = b - a$ for some integer k. (by definitions of mod and divides).

So $a = b - nk$

Taking each side $\%n$ we get:

$a\%n = (b - nk)\%n = b\%n$

Where the last equality follows from k being an integer and doing k applications of the identity we proved in the warm-up.

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Show the forward direction:

If $a\%n = b\%n$ then $a \equiv b(mod\ n)$.

This proof is a bit different than the other direction.

Remember to work from top and bottom!!

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 $n|(b - a)$

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist ***unique*** integers q, r with $0 \leq r < d$ Such that $a = dq + r$

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Forward direction:

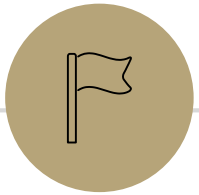
Suppose $a\%n = b\%n$.

By definition of $\%, a = kn + (a\%n)$ and $b = jn + (b\%n)$ for integers k, j

Isolating $a\%n$ we have $a\%n = a - kn$. Since $a\%n = b\%n$, we can plug into the second equation to get: $b = jn + (a - kn)$

Rearranging, we have $b - a = (j - k)n$. Since k, j are integers we have $n|(b - a)$.

By definition of mod we have $a \equiv b(mod\ n)$.



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)

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.

We'll write it 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 $7\ (mod\ 26)$.

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

$y \equiv 45(mod\ 26)$
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 $k \in \mathbb{Z}$
So $\{\dots, -7, 19, 45, \dots 19 + 26k, \dots\}$