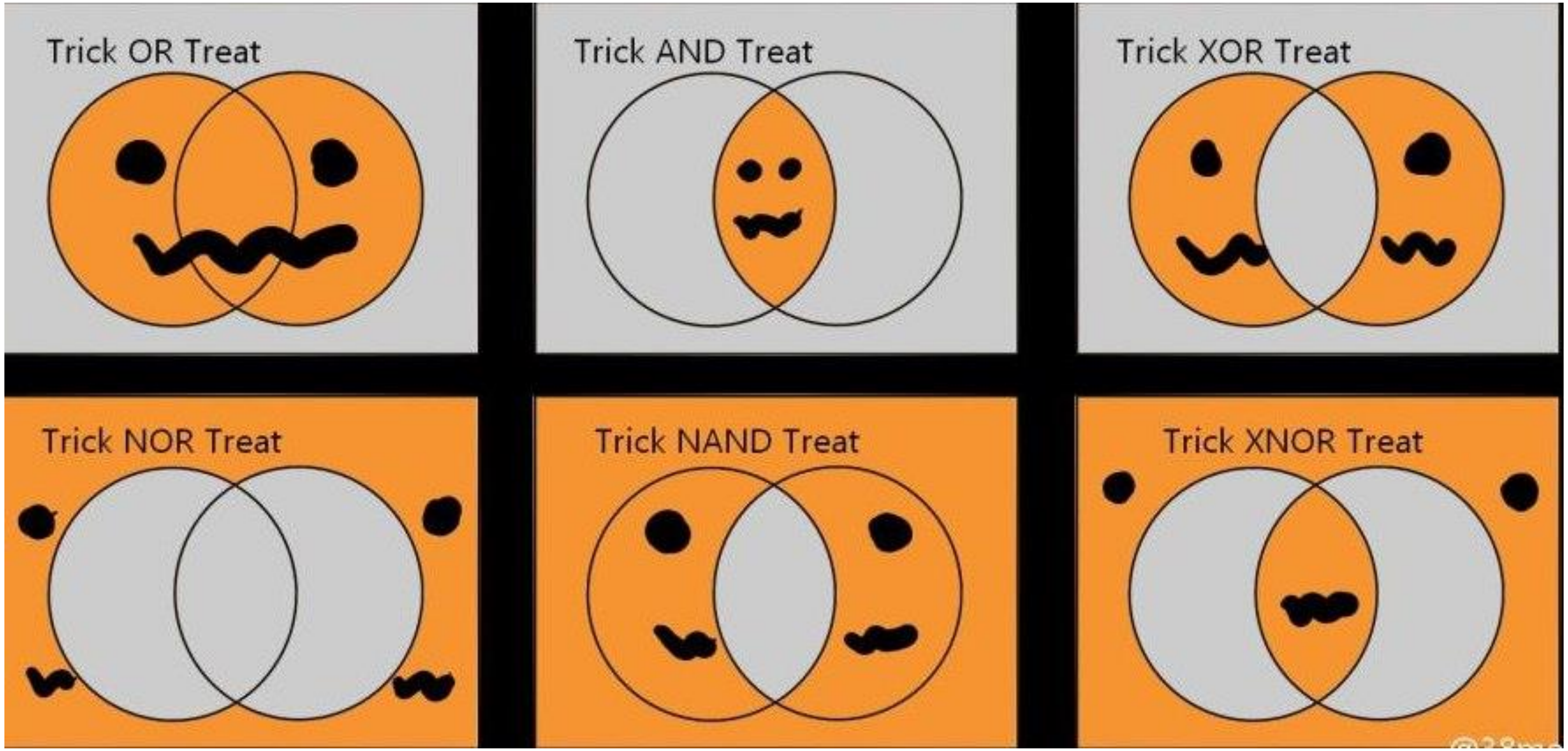


More Number Theory

CSE 311 Autumn 20
Lecture 12

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 $b \equiv a (mod\ n)$

$$a \equiv b (mod\, n) \underset{\text{(by def)}}{\Longleftrightarrow} n \mid (b-a) \underset{\text{(by def)}}{\Longleftrightarrow} nk = b - a \ (k \in \mathbb{Z})$$

$$\Longleftrightarrow n(-k) = a - b \ (-k \in \mathbb{Z}) \underset{\text{by def}}{\Longleftrightarrow} n \mid (a-b) \underset{\text{by def}}{\Longleftrightarrow} b \equiv a (mod\, n)$$

$0 \le r < c$

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

$$a = nq + (a\%n) \qquad q \in \mathbb{Z},\ a\%n \text{ int.}$$

$$a - n = (q-1)n + (a\%n)$$

$$a - n = (?)n + [(a-n)\%n]$$

a n

The Division Theorem

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

Warm up

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

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

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

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

Modular arithmetic so far

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

If $a \equiv b (mod\ n)$ then $a + c \equiv a + \overset{c}{\cancel{d}}(mod\ n)$.

If $a \equiv b (mod\ n)$ then $ac \equiv bc\ (mod\ n)$.

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

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

% 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 $0 \le r < b$ and $a = bq + r$ for some integer q.

This is the "mod function"

I claim $\overbrace{a\%n = b\%n}^{p}$ if and only if $\overbrace{a \equiv b (mod\ n)}^{q}$.

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

$p \to q$ "the forward direction"

$q \to p$ the backward direction

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

Backward direction:

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

$\Rightarrow n \mid b-a$

$\rightarrow nk = b-a \quad (k \in \mathbb{Z})$

$\rightarrow a = b-nk$

$a\%n = \underbrace{(b-nk)\%n}$

$b\%n$

$a\%n \cancel{= (b-nk)\%n} = b\%n$ ← target

$a\%n = b\%n$ 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: $n | (b-a)$

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!!

$a\%n = b\%n$

$a = qn + a\%n \quad q \in \mathbb{Z}$

$b = sn + b\%n \quad s \in \mathbb{Z}$.

$\to n | \underbrace{(b-a)}_{= b-a} \to a \equiv b (mod\ n)$

Fill out the poll everywhere for Activity Credit!
Go to pollev.com/cse311 and login with your UW identity
Or text cse311 to 22333

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 $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$
There exist *unique* integers q, r with $0 \le r < d$ 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 $a \equiv b (mod\ n)$.

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 $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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 $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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 $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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 $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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

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

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

And then a miracle occurs

$nknj = (bd - ac)$

$n?? = bd - ac$

$- bc - ad$

$n|(bd - ac)$

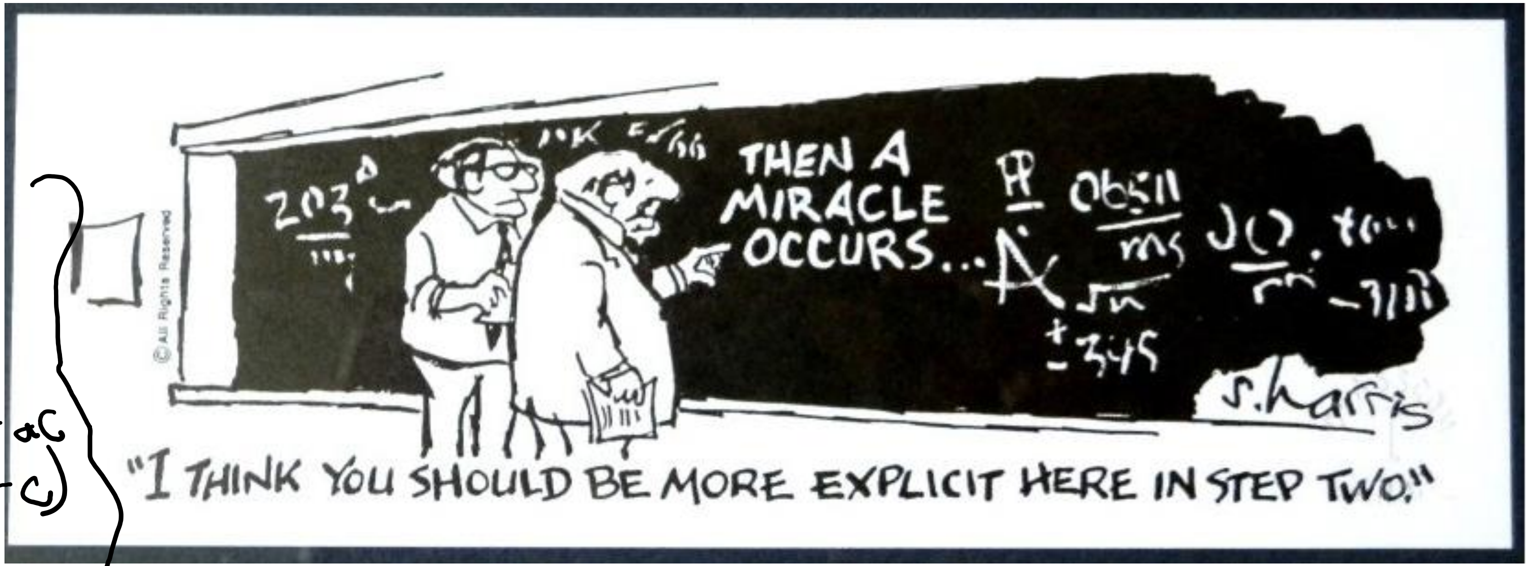
$+ ac + ac$

$ac \equiv bd (mod\ n)$

$c(a-b) - ad + ac$

$c(a-b) - a(d-c)$

$= nu - nv$



Uh-Oh

We hit 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 $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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.

$\underline{b} = nk + a, d = nj + c$

$n?? = bd - ac$

$n|(bd - ac)$

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

Another Approach

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

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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.

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

$bd = (nk+a)(nj+c) = n^2kj + anj + cnk + ac$

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

$n?? = bd - ac$

$n|(bd-ac)$

$ac \equiv bd(mod\ n)$

Another Approach

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

Let $a, b, c, d, n \in \mathbb{Z}, n \geq 0$
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.

Isolating,b and d, we have: $b = nk + a, d = nj + c$

Muliplying the equations, and factoring, $bd = (nk+a)(nj+c) = n^2kj + anj + cnk + ac$

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

Since all of $n, j, k, a,$ and c are integers, we have that $bd - ac$ is n times an integer, so

$n|(bd - ac)$, and by definition of mod

$ac \equiv bd (mod\ n)$

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?"

$r \quad \wedge \quad \vee \to q$

q

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 $x + 5 = -x - 5$.

Pred.

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

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

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

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

$$0 = 0$$

$0 = 0$

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.

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 $az = bc$

…

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

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

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

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 $a|bc$.

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.

Divisors and Primes

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 $\boldsymbol{b}$ (gcd(a,b)) is the largest integer $\boldsymbol{c}$ such that $\boldsymbol{c}|\boldsymbol{a}$ and $\boldsymbol{c}|\boldsymbol{b}$

Least Common Multiple

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

```
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;
}
```

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$(2^3 \cdot 3, 2^2 \cdot 5) = 2\text{^}\{\min(2,3)\} = 2\text{^}2 = 4$.

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

But that's….really expensive. Mystery from a few slides ago find gcd.

GCD fact

If a and b are positive integers, then gcd(a,b) = 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 $\mathrm{x} = \mathrm{gcd}(a, b)$ and $y = \mathrm{gcd}(b, a\%b)$.

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