Warm up: Show that if a^2 is even then a is even.

Suggestion: think carefully about proof technique.

Number Theory Proofs

CSE 311 Autumn 20
Lecture 14

Announcements

HW5 is coming out this evening.

It's due Monday November 9th

It's also a little longer than usual, so don't think this is an excuse to put it off.

"Part I" of the homework is on number theory – these slides have everything you need.

"Part II" is on induction, the topic for next week.

We want to give you feedback on induction proofs before the midterm, hence the different setup.

Announcements

Everyone gets an extra late day!

Why?

HW3 grades ~~aren't back out yet,~~ we want to make sure you don't repeat mistakes if you learn from them. They'll be out this afternoon.

And HWs 3 and 4 seem to be taking some folks longer than anticipated.

Use this as a learning opportunity; 311 homeworks are not like calculus homeworks where it's easy to predict exactly how long it will take. Get started early.

Announcements

Daylight Saving Time ends this Sunday.

If you're in a part of the U.S. that observes Daylight Saving Time, enjoy your extra hour of sleep.

If you're not…the time of everything relative to you probably shifts by an hour Sunday (Seattle time). :/

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

a b   b a%b

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)

m q n r

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

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{array}{ccccccc}
r & & q & & n & & m \\
35 & = & 1 & \cdot & 27 & + & 8 \\
27 & = & 3 & \cdot & 8 & + & 3 \\
8 & = & 2 & \cdot & 3 & + & 2 \\
3 & = & 1 & \cdot & 2 & + & 1
\end{array}
$$

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

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

$\gcd(35,27) = 1 = 3 - 1 \cdot 2$

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

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

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

Extended Euclidian Algorithm

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

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$\boxed{\begin{array}{l} 8 = 35 - 1 \cdot 27 \\ 3 = 27 - 3 \cdot 8 \\ 2 = 8 - 2 \cdot 3 \\ 1 = 3 - 1 \cdot 2 \end{array}}$$

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)

So…what's it good for?

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

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

$s7x \equiv s \cdot 1 (mod\ n)$

$x \equiv s (mod\ n)$

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!

Try it

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

$y \equiv \quad (mod\ 2)$

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.

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

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

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

$$
\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2(7 - 5 \cdot 1) \\
&= 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 \\
\gcd(26,7) = 1 &= 3 \cdot 26 - 11 \cdot 7
\end{aligned}
$$

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

Try it

$26|(3-7y)$

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

What do we need to find?

$3 \cdot 26 - 11 \cdot 7 = 1$

The multiplicative inverse of 7 $(mod, 26)$.

$3 \cdot 26 = 1 + 11 \cdot 7$

$26 \mid 1 - (-11 \cdot 7)$

$-11 \cdot 7 \equiv 1 \ (mod\ 26)$

gcd(

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

$1 \cdot y \equiv 45(mod\ 26)$

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 $\{\dots, -7, 19, 45, \dots 19 + 26k, \dots\}$

Multiplicative Inverse

The number b is a multiplicative inverse of a (mod n) if $ba \equiv 1 (mod\ n)$.

If $\text{gcd}(a, n) = 1$ then the multiplicative inverse exists.

If $\text{gcd}(a, n) \neq 1$ then the inverse does not exist.

Arithmetic $(mod\ p)$ for p prime is really nice for that reason.

Sometimes equivalences still have solutions when you don't have inverses (but sometimes they don't) – you'll experiment with these facts on HW5.

Proof By Contradiction

Proof By Contradiction

Suppose the negation of your claim. P Suppose $\neg P$

Show that you can derive `False` (i.e. (¬claim) → `F`)

If your proof is right, the implication is true. $\neg$claim $= F$

So ¬claim must be `False`. $\neg P = F$

So claim must be `True`! $P = T$

Proof By Contradiction

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Proof By Contradiction

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

We don't have a fixed target.
That can make this proof harder.

But [] is a contradiction!

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = s/t$

Let $p = \frac{s}{\gcd(s,t)}, q = \frac{t}{\gcd(s,t)}$ Note that $\gcd(p, q) = 1$.

$\sqrt{2} = \frac{p}{q}$

That's is a contradiction! We conclude $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = s/t$

Let $p = \frac{s}{\gcd(s,t)}, q = \frac{t}{\gcd(s,t)}$ Note that $\gcd(p, q) = 1$.

$\sqrt{2} = \frac{p}{q}$

$2 = \frac{p^2}{q^2}$

$2q^2 = p^2$ so p^2 is even. p is even by fact in purple box. $\rightarrow 2 \mid p$

$p = 2k \quad k \in \mathbb{Z}$.

$p^2 = 4k^2$

$2q^2 = 4k^2 \rightarrow q^2 = 2k^2 \rightarrow 2 \mid q$

q^2 is even. $\rightarrow$ q is even.

$\gcd(p,q) \geq 2$

That's is a contradiction! We conclude $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $\mathrm{t} \neq 0$ and $\sqrt{2} = s/t$

Let $p = \frac{\mathrm{s}}{\mathrm{gcd(s,t)}}, \mathrm{q} = \frac{\mathrm{t}}{\mathrm{gcd(s,t)}}$ Note that $\mathrm{gcd}(p, q) = 1$.

$\sqrt{2} = \frac{p}{q}$

$2 = \frac{p^2}{q^2}$

$2q^2 = p^2$ so p^2 is even. By the fact above, p is even, i.e. $p = 2k$ for some integer k. Squaring both sides $p^2 = 4k^2$

Substituting into our original equation, we have: $2q^2 = 4k^2$, i.e. $q^2 = 2k^2$.

So q^2 is even. Applying the fact above again, q is even.

But if both p and q are even, $\mathrm{gcd}(p, q) \geq 2$. But we said $\mathrm{gcd}(p, q) = 1$

That's is a contradiction! We conclude $\sqrt{2}$ is irrational.

Proof By Contradiction

How in the world did we know how to do that?

In real life…lots of attempts that didn’t work.

Be very careful with proof by contradiction – without a clear target, you can easily end up in a loop of trying random things and getting nowhere.

What's the difference?

What's the difference between proof by contrapositive and proof by contradiction?

Show $p \to q$	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg(p \to q) \equiv (p \land \neg q)$	$\neg q$
Target	Something false	$\neg p$

Show p	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg p$	---
Target	Something false	---

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

But [] is a contradiction! So there must be infinitely many primes.

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$

$q \% p_i =$

$0 = 1$

Case 1: q is prime

$q = p_i$ for some i $\qquad$ $q > p_i$ for all i

Case 2: q is composite

$r | q, r \neq 1, r \neq q$ $\qquad$ some $p_i | q$ $\qquad$ $q \% p_i = 0$

$p_1 \cdot p_2 \cdots p_k + 1 \% p_i$

But [] is a contradiction! So there must be infinitely many primes.

$\rightarrow p_i \cdot j + 1 \% p_i = 1$

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$

Case 1: q is prime

$q > p_i$ for all i. But every prime was supposed to be on the list $p_1, \ldots, p_k$. A contradiction!

Case 2: q is composite

Some prime on the list (say p_i) divides q. So $q \% p_i = 0.$ and $(p_1 p_2 \cdots p_k + 1) \% p_i = 1$. But $q = (p_1 p_2 \cdots p_k + 1)$. That's a contradiction!

In either case we have a contradiction! So there must be infinitely many primes.

We're continuing on deck 14's slides
(with 4^{13} changed to 4^{11} in calculations)

Warmup: Show that if $n>0$ and 4^n-1 is prime then n is odd.

Use pf by contradiction

What is the negation of

$\forall n([n>0 \wedge \mathrm{Prime}(4^n-1)] \to \mathrm{odd}(n))$

Fast Exponentiation Algorithm

Proof by Contradiction

Suppose for the sake of contradiction
There is an integer k s.t. $k>0$, 4^k-1 is prime and
k is even.

Target some contradiction

RSA

An application of all of this modular arithmetic

Amazon chooses random 512-bit (or 1024-bit) prime numbers p, q and an exponent e (often about 60,000).

Amazon calculates $\mathrm{n} = pq$. They tell your computer (n, e) (not p, q)

You want to send Amazon your credit card number a.

You compute $C = a^e \% n$ and send Amazon C.

Amazon computes d, the multiplicative inverse of e $(mod\ [p-1][q-1])$

a

Amazon finds $C^d \% n$

Fact: $a = C^d \% n$ as long as $0 < a < n$ and $p \nmid a$ and $q \nmid a$

How big are those numbers?

1230186684530117755130494958384962720772853569595334792197322
4521517264005072636575187452021997864693899564749427740638459
2519255732630345373154826850791702612214291346167042921431160
2221240479274737794080665351419597459856902143413

=

3347807169895689878604416984821269081770479498371376856891243
1388982883793878002287614711652531743087737814467999489

~300 to 350 bits

×

3674604366679959042824463379962795263227915816434308764267603
2283815739666511279233373417143396810270092798736308917

How do we accomplish those steps?

That fact? You can prove it in the extra credit problem on HW5. It's a nice combination of lots of things we've done with modular arithmetic.

Let's talk about finding $C = a^e \% n$.

e is a BIG number (about 2^{16} is a common choice)

```
int total = 1;
for(int i = 0; i < e; i++){
    total = (a * total) % n;
}
```

Let’s build a faster algorithm.

Fast exponentiation – simple case. What if e is exactly 2^{16}?

$a^{(2^{16})} \% n$

```
int total = 1;
for(int i = 0; i < e; i++){
     total = a * total % n;
}
Instead:
int total = a;
for(int i = 0; i < log(e); i++){
     total = total^2 % n;
}
```

$a \rightarrow a^2 \% n$

$(a^2)^2 \rightarrow a^4 \% n$

$(a^4)^2 \rightarrow a^8 \% n$

$(a^8)^2 = a^{16} \% n$

$\vdots$

$a^{(2^{16})}$

Fast exponentiation algorithm

What if e isn't exactly a power of 2?

Step 1: Write e in binary.

Step 2: Find $a^c \% n$ for c every power of 2 up to e.

Step 3: calculate a^e by multiplying a^c for all c where binary expansion of e had a 1.

Fast exponentiation algorithm

$e = 11$

Find $4^{11}\%10$ ... $\cancel{16}$

1	0	1	1
8	4	2	1

$11 - 8 = 3$ left

$3 - 2 = 1$

Step 1: Write e in binary.

Step 2: Find $a^c\%n$ for c every power of 2 up to e.

Step 3: calculate a^e by multiplying a^c for all c where binary expansion of e had a 1.

Start with largest power of 2 less than e (8). 8's place gets a 1. Subtract power

Go to next lower power of 2, if remainder of e is larger, place gets a 1, subtract power; else place gets a 0 (leave remainder alone).

11 = 1011_2

Fast exponentiation algorithm

Find $4^{11}\%10$

$4^1, 4^2, 4^4, 4^8, \ldots$

Step 1: Write e in binary.

Step 2: Find $a^c\%n$ for c every power of 2 up to e.

Step 3: calculate a^e by multiplying a^c for all c where binary expansion of e had a 1.

$4^4\%10 = (4^2)^2\%10$

$4^8 = (4^4)^2$

$4^1\%10 = 4$

$4^2\%10 = 6$

$4^4\%10 = 6^2\%10 = 6$

$4^8\%10 = 6^2\%10 = 6$

$4^8 \cdot$

Fast exponentiation algorithm

Find $4^{11}\%10$

Step 1: Write e in binary.

Step 2: Find $a^c\%n$ for c every power of 2 up to e.

Step 3: calculate a^e by multiplying a^c for all c where binary expansion of e had a 1.

$4^1\%10 = 4$

$4^2\%10 = 6$

$4^4\%10 = 6^2\%10 = 6$

$4^8\%10 = 6^2\%10 = 6$

$4^{11}\%10 = 4^{8+2+1}\%10 =$
$[(4^8\%10)\cdot(4^2\%10)\cdot(4\%10)]\%10 = (6\cdot 6\cdot 4)\%10$
$= (36\%10\cdot 4)\%10 = (6\cdot 4)\%10 = 24\%10 = 4.$

1011

$a \equiv b \pmod n$

$c \equiv d \pmod n$

$ac \equiv bd \pmod n$

$\log_2(e)$

$e^{2^{\log_2(e)}} = a^8$

$(4^8\cdot 4^2\cdot 4^1)\%10$

$4^{11}\%10 = 4$

$4^4\%10$

$= (4^2)^2\%10$

$= (4^2\%10)^2\%10$

$= (6)^2\%10$

$= 6$

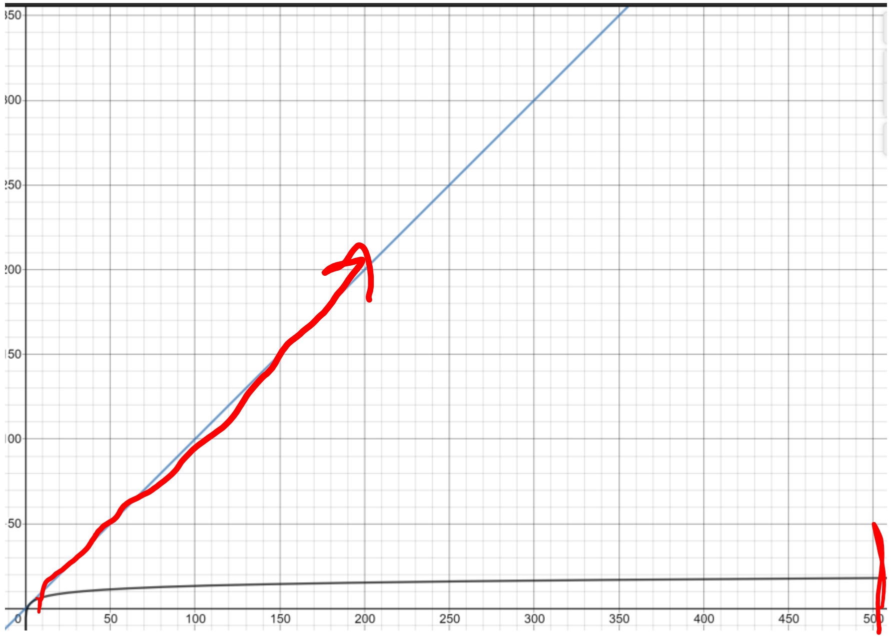
Fast Exponentiation Algorithm

Is it…actually fast?

The number of multiplications is between $\log_2 e$ and $2 \log_2 e$.

That's A LOT smaller than e

2^{16}



$e = 500$

One More Example for Reference

Find $3^{25}\%7$ using the fast exponentiation algorithm.

Find 25 in binary:

16 is the largest power of 2 smaller than 25. $(25 - 16) = 9$ remaining

8 is smaller than 9. $(9 - 8) = 1$ remaining.

4s place gets a 0.

2s place gets a 0

$1s$ place gets a 1

11001_2

One More Example for Reference

Find $3^{25}\%7$ using the fast exponentiation algorithm.

Find $3^{2^i}\%7$:

$3^1\%7 = 3$

$3^2\%7 = 9\%7 = 2$

$3^4\%7 = (3^2 \cdot 3^2)\%7 = (2 \cdot 2)\%7 = 4$

$3^8\%7 = \left(3^4 \cdot 3^4\right)\%7 = (4 \cdot 4)\%7 = 2$

$3^{16}\%7 = \left(3^8 \cdot 3^8\right)\%7 = (2 \cdot 2)\%7 = 4$

One More Example for Reference

Find $3^{25}\%7$ using the fast exponentiation algorithm.

$3^1\%7 = 3$

$3^2\%7 = 2$

$3^4\%7 = 4$

$3^8\%7 = 2$

$3^{16}\%7 = 4$

$$3^{25}\%7 = 3^{16+8+1}\%7$$
$$= [(3^{16}\%7) \cdot \left(3^8\%7\right) \cdot (3^1\%7)]\%7$$
$$= [4 \cdot 2 \cdot 3]\%7$$
$$= (1 \cdot 3)\%7 = 3$$

A Brief Concluding Remark

Why does RSA work? i.e. why is my credit card number "secret"?

Raising numbers to large exponents (in mod arithmetic) and finding multiplicative inverses in modular arithmetic are things computers can do quickly.

But factoring numbers (to find p, q to get d) or finding an "exponential inverse" (not a real term) directly are not things computers can do quickly. At least as far as we know.

An application of all of this modular arithmetic

Amazon chooses random 512-bit (or 1024-bit) prime numbers p, q and an exponent e (often about 60,000).

Amazon calculates $\mathrm{n} = pq$. They tell your computer (n, e) (not p, q)

You want to send Amazon your credit card number a.

You compute $C = a^e \% n$ and send Amazon C.

Amazon computes d, the multiplicative inverse of e $(mod\ [p-1][q-1])$

Amazon finds $C^d \% n$

Fact: $a = C^d \% n$ as long as $0 < a < n$ and $p \nmid a$ and $q \nmid a$

And now, for even more proofs!

If a^2 is even then a is even

Proof:

We argue by contrapositive.

Suppose a is odd.

a^2 is odd.

If a^2 is even then a is even

Proof:

We argue by contrapositive.

Suppose a is odd.

By definition of odd, $a = 2k + 1$ for some integer k.

$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$.

Factoring, $a^2 = 2(2k^2 + 2k) + 1$.

So a^2 is odd by definition.

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 $a = \gcd(w, x), b = \gcd(y, z)$

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

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