CS70 Discussion 2D: tinyurl.com/frank-discussion 7/2/2020

2 min alone
6 min room
10 min go over

1

(a) 3 an inverse of 5 modulo 10?

$3(5) = 15 \pmod{10}$
$\equiv 5 \pmod{10}$

$\boxed{\text{Not an inverse}}$

(b) 3 an inverse of 5 modulo 14?

$3(5) = 15 \pmod{14}$
$= 1$

$\boxed{\text{yes, is inverse}}$

(c) $(3+14n), n \in \mathbb{Z}$ inverse of 5 modulo 14?

$5(3+14n) \pmod{14}$
$\equiv 15 + 5(\underbrace{14n}) \pmod{14}$
$= 1 + 0 = \underline{1}$ $\boxed{\text{yes, is an inverse}}$

(d) Does 4 have inverse mod 8? $(a, m \in \mathbb{Z})$

A mult. inverse for a mod $\underline{m}$ exists iff a and m are coprime.

$\gcd(4,8) = 4 \neq 1$

$\boxed{\text{no inverse exists}}$

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a mod m. $x \not\equiv x' \pmod{m}$?

$\begin{cases} ax \equiv 1 \pmod{m} \\ ax' \equiv 1 \pmod{m} \end{cases}$

$a(x-x') \equiv 0 \pmod{m}$

$\cancel{xa}(x-x') \equiv \cancel{0 \cdot x} \pmod{m}$

$\boxed{x \equiv x' \pmod{m}}$

When a multiplicative inverse exists, that inverse is going to be unique

(f) Prove if $\gcd(a,m) = 1$ and $m > 1$, then unique inverse of a modulo m exists.

Since a and m are relatively prime, then $\exists\, s, t \in \mathbb{Z}$

$1 = as + mt$ (division algorithm)

Take modulo m of both sides of the equation.

$1 \equiv as + mt \pmod{m}$

$1 \equiv as \pmod{m}$

$\boxed{\text{s is the mult. inverse of a mod m}}$

(g) Prove that if inverse of a modulo m exists, then a and m are relatively prime.

Contradiction: Suppose that a has a mult. inverse mod m called a^{-1}, and that $\gcd(a,m) = n > 1$

$aa^{-1} \equiv 1 \pmod{m}$
$aa^{-1} - 1 \equiv 0 \pmod{m}$

$m \mid aa^{-1} - 1$

$\exists\, b \in \mathbb{Z}$ $mb = aa^{-1} - 1$

$mb \equiv aa^{-1} - 1 \pmod{n}$
$0 \equiv 0 - 1 \pmod{n}$

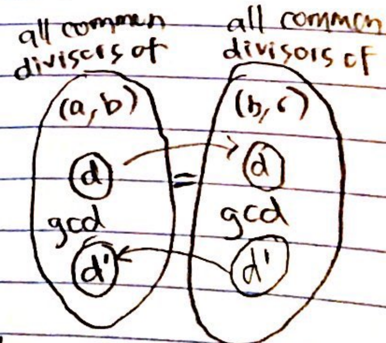
$\boxed{0 \equiv -1 \pmod{n}}$

$\boxed{\text{Contradiction!}}$

2 Let $a = bq + r$ for $a, b, q, r \in \mathbb{Z}$. Prove $\gcd(a,b) = \gcd(b,r)$

1 min alone
5 min break
10 min go over

Show that (a,b) and (b,r) share all of their common divisors.



Consider any generic $d \in \mathbb{Z}$ $d \mid a$ and $d \mid b$. Then, $r = a - bq$
d = common divisor of (a,b) $d \mid r$ b/c $d \mid a$ and $d \mid b$

Consider any generic $d' \in \mathbb{Z}$ $d' \mid b$ and $d' \mid r$. Then $a = bq + r$,
d' = common divisor of (b,r) $d' \mid a$ - $d' \mid b$ and $d' \mid r$

So since (a,b) and (b,r) share all the same common divisors, their greatest common divisors must be the same as well.