Quick Review

- GCD / Bezout's Theorem
  - Use Euclidean Alg. to find gcd(a,b)
  - Do it backwards to find s, t such that $as + bt = \gcd(a,b)$.
- Modular Arithmetic
  - $a \equiv b \bmod m$ is equivalent to
    - → $m \mid a - b$
    - → $a \% m = b \% m$.
  - You can add / multiply by integers, but you can't divide.
    - → next best thing is inverses, but those don't always exist...

General Notes

- Mods make everything simpler, so don't be afraid to use them.
- Work with primes whenever you can
- When dealing w/ squares or higher powers, taking mod 4 or mod 3 might help.
- You can show $a = b$ by showing that $a \mid b$ and $b \mid a$.
- If $x \mid a$ and $x \mid b$, then $x \mid \gcd(a,b)$; this can be useful.

Modular Inverses

2D #1

(a) Is 3 an inverse of 5 mod 10? N

(b) Is 3 an inverse of 5 mod 14? Y

(c) Is $3+14n$ an inverse of 5 mod 14 for all $n \in \mathbb{N}$? Y

(d) Does 4 have an inverse mod 8? N

(e) Suppose $x, x' \in \mathbb{Z}$ are inverses of a mod m. Is it possible for $x \not\equiv x' \bmod m$?

(f) Prove that if $\gcd(a,m)=1$, then a has an inverse mod m.

(g) Prove that if a^{-1} exists mod m, then $\gcd(a,m)=1$.

(e) No. We have $x \equiv xax' \equiv x' \bmod m$.

(f) By Bezout, $\exists s,t$ such that $as+mt=1$. Taking both sides mod m, we get $as \equiv 1$, so $s = a^{-1}$ exists.

(g) Let $s \equiv a^{-1} \bmod m$. Then $as = km+1$ for some k, hence $as-km=1$. Since $\gcd(a,m)$ divides the LHS, it must divide the RHS, so $\gcd(a,m) \mid 1$ thus $\gcd(a,m)=1$.

Euclid Verification

2D #2

Let $a = bq + r$ where $a, b, q, r \in \mathbb{Z}$ and $0 \leq r < b$. Prove that $\gcd(a,b) = \gcd(b,r)$

Observe that since $\gcd(a,b) \mid a$ and since $\gcd(a,b) \mid b$, it follows that

$$\gcd(a,b) \mid a - bq = r,$$

so $\gcd(a,b) \mid r$ and thus $\gcd(a,b) \mid \gcd(b,r)$

Now, observe that $\gcd(b,r) \mid bq + r = a$, so $\gcd(b,r) \mid a$ and $\gcd(b,r) \mid b$, so $\gcd(b,r) \mid \gcd(a,b)$. Thus they must be equal.

(a) Fill in the blanks below for executing the Euclidean Algorithm

$$\begin{aligned} \gcd(2328,440) &= \gcd(440,128) & [\mathbf{128} = 1 \times \mathbf{2328} + (-5) \times \mathbf{440}] \\ &= \gcd(128,56) & [\mathbf{56} = 1 \times \mathbf{440} + \underline{-3} \times \mathbf{128}] \\ &= \gcd(56,16) & [\mathbf{16} = 1 \times \mathbf{128} + \underline{-2} \times \mathbf{56}] \\ &= \gcd(16,8) & [\mathbf{8} = 1 \times \mathbf{56} + \underline{-3} \times \mathbf{16}] \\ &= \gcd(8,0) & [\mathbf{0} = 1 \times \mathbf{16} + (-2) \times \mathbf{8}] \\ &= \mathbf{8}. \end{aligned}$$

(Fill in the blanks)

(b) Recall that our goal is to fill out the blanks in

$$8 = \underline{\quad\quad} \times \mathbf{2328} + \underline{\quad\quad} \times \mathbf{440}.$$

To do so, we work back up from the bottom, and express the gcd above as a combination of the two arguments on each of the previous lines:

$$\begin{aligned} 8 &= 1 \times \mathbf{8} + 0 \times \mathbf{0} = 1 \times \mathbf{8} + (1 \times \mathbf{16} + (-2) \times \mathbf{8}) \\ &= 1 \times \mathbf{16} - 1 \times \mathbf{8} \\ &= \underline{-1} \times \mathbf{56} + \underline{4} \times \mathbf{16} \end{aligned}$$

[*Hint*: Remember, $\mathbf{8} = 1 \times \mathbf{56} + (-3) \times \mathbf{16}$. Substitute this into the above line.]

$$= \underline{4} \times \mathbf{128} + \underline{-9} \times \mathbf{56}$$

[*Hint*: Remember, $\mathbf{16} = 1 \times \mathbf{128} + (-2) \times \mathbf{56}$.]

$$\begin{aligned} &= \underline{-9} \times \mathbf{440} + \underline{31} \times \mathbf{128} \\ &= \underline{31} \times \mathbf{2328} + \underline{-164} \times \mathbf{440} \end{aligned}$$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

$\gcd(17, 38) = 1 = 13 \cdot 38 - 29 \cdot 17$

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

$17 \cdot (-29) \equiv 1 \mod 38$

$\Rightarrow \; -29 \equiv 9 \equiv 17^{-1}.$