

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
 - $a \equiv b \pmod{m}$ 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?
- (b) Is 3 an inverse of 5 mod 14?
- (c) Is $3 + 14n$ an inverse of 5 mod 14 for all $n \in \mathbb{N}$?
- (d) Does 4 have an inverse mod 8?
- (e) Suppose $x, x' \in \mathbb{Z}$ are inverses of a mod m . Is it possible for $x \not\equiv x' \pmod{m}$?
- (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 $\gcd(a, m) = 1$.

Euclid Verification

2D # 2

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

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

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

(Fill in the blanks)

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

$$8 = ___ \times 2328 + ___ \times 440.$$

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:

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

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

$$= ___ \times 128 + ___ \times 56$$

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

$$\begin{aligned}&= ___ \times 440 + ___ \times 128 \\ &= ___ \times 2328 + ___ \times 440\end{aligned}$$

(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.

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