

1 Extended Euclid

In this problem we will consider the extended Euclid's algorithm. The bolded numbers below keep track of which numbers appeared as inputs to the gcd call. Remember that we are interested in writing the GCD as a linear combination of the original inputs, so we don't want to accidentally simplify the expressions and eliminate the inputs.

- (a) Note that $x \bmod y$, by definition, is always x minus a multiple of y . So, in the execution of Euclid's algorithm, each newly introduced value can always be expressed as a "combination" of the previous two, like so:

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

(Fill in the blanks)

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

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

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:

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

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

$$= ___ \times \mathbf{128} + ___ \times \mathbf{56}$$

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

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

(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.

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

2 Mechanical Chinese Remainder Theorem

In this problem, we will solve for x such that

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

(a) Find a number $0 \leq b_2 < 30$ such that $b_2 \equiv 1 \pmod{2}$, $b_2 \equiv 0 \pmod{3}$, and $b_2 \equiv 0 \pmod{5}$.

(b) Find a number $0 \leq b_3 < 30$ such that $b_3 \equiv 0 \pmod{2}$, $b_3 \equiv 1 \pmod{3}$, and $b_3 \equiv 0 \pmod{5}$.

(c) Find a number $0 \leq b_5 < 30$ such that $b_5 \equiv 0 \pmod{2}$, $b_5 \equiv 0 \pmod{3}$, and $b_5 \equiv 1 \pmod{5}$.

(d) What is x in terms of b_2 , b_3 , and b_5 ? Evaluate this to get a numerical value for x .

3 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0, 1, \dots, n-1\}$ to $\{0, 1, \dots, n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

(b) $f(x) = 5x \pmod{n}$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} \pmod{n} & \text{if } x \neq 0. \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod{n}$.

4 Baby Fermat

Assume that a does have a multiplicative inverse mod m . Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \dots \pmod{m}$. Prove that this sequence has repetitions.

(Hint: Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j ?