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 mod 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:

$$\begin{aligned} \gcd(54,17) &= \gcd(17,3) & \mathbf{3} &= 1\times\mathbf{54} - 5\times\mathbf{17} \\ &= \gcd(3,2) & \mathbf{2} &= 1\times\mathbf{17} - \_\_\_\_\times\mathbf{3} \\ &= \gcd(2,1) & \mathbf{1} &= 1\times\mathbf{3} - \_\_\_\_\times\mathbf{2} \\ &= \gcd(1,0) & [\mathbf{0} &= 1\times\mathbf{2} - \_\_\_\_\times\mathbf{1}] \\ &= 1. \end{aligned}$$

(Fill in the blanks)

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

$$1 = \_\_\_\_\times\mathbf{54} + \_\_\_\_\times\mathbf{17}.$$

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:

$$\begin{aligned} 1 &= \_\_\_\_\times\mathbf{3} + \_\_\_\_\times\mathbf{2} \\ &= \\ &= \_\_\_\_\times\mathbf{17} + \_\_\_\_\times\mathbf{3} \\ &= \\ &= \_\_\_\_\times\mathbf{54} + \_\_\_\_\times\mathbf{17} \end{aligned}$$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 39, and determine how to express this as a "combination" of 17 and 39.

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 39?

2 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number x such that,

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned} \tag{1}$$

(a) Suppose you find 3 natural numbers a, b, c that satisfy the following properties:

$$a \equiv 2 \pmod 3 \; ; \; a \equiv 0 \pmod 5 \; ; \; a \equiv 0 \pmod 7, \tag{2}$$

$$b \equiv 0 \pmod 3 \; ; \; b \equiv 3 \pmod 5 \; ; \; b \equiv 0 \pmod 7, \tag{3}$$

$$c \equiv 0 \pmod 3 \; ; \; c \equiv 0 \pmod 5 \; ; \; c \equiv 4 \pmod 7. \tag{4}$$

Show how you can use the knowledge of a, b and c to compute an x that satisfies (1).

In the following parts, you will compute natural numbers a, b and c that satisfy the above 3 conditions and use them to find an x that indeed satisfies (1).

(b) Find a natural number a that satisfies (2). In particular, an a such that $a \equiv 2 \pmod 3$ and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find a^*, the multiplicative inverse of 5×7 modulo 3. What do you see when you compute $(5 \times 7) \times a^*$ modulo 3, 5 and 7? What can you then say about $(5 \times 7) \times (2 \times a^*)$?

(c) Find a natural number b that satisfies (3). In other words: $b \equiv 3 \pmod 5$ and is a multiple of 3 and 7.

(d) Find a natural number c that satisfies (4). That is, c is a multiple of 3 and 5 and $\equiv 4 \pmod 7$.

(e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1).

3 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 infinite sequence $a, a^2, a^3, \ldots \pmod{m}$. 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 is the value of $a^{i-j} \pmod{m}$?

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