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:

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

(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 Fibonacci GCD

Note 6

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

3 Chinese Remainder Theorem Practice

Note 6

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

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 4 \pmod{11} \end{aligned} \tag{1}$$

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

$$a \equiv 1 \pmod 3 \; ; \; a \equiv 0 \pmod 7 \; ; \; a \equiv 0 \pmod{11}, \tag{2}$$
$$b \equiv 0 \pmod 3 \; ; \; b \equiv 1 \pmod 7 \; ; \; b \equiv 0 \pmod{11}, \tag{3}$$
$$c \equiv 0 \pmod 3 \; ; \; c \equiv 0 \pmod 7 \; ; \; c \equiv 1 \pmod{11}. \tag{4}$$

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 satisfies (1).

(b) Find a natural number a that satisfies (2). That is, $a \equiv 1 \pmod 3$ and is a multiple of 7 and 11.

It may help to start with a number that is a multiple of both 7 and 11; what number should we multiply this by in order to make it equivalent to $1 \pmod 3$?

(c) Find a natural number b that satisfies (3). That is, $b \equiv 1 \pmod 7$ and is a multiple of 3 and 11.

(d) Find a natural number c that satisfies (4). That is, $c \equiv 1 \pmod{11}$ and is a multiple of 3 and 7.

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

4 When/Why can we use CRT?

Let $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbb{Z}$ where $m_i > 1$ and pairwise relatively prime. In lecture, you've constructed a solution to

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

Let $m = m_1 \cdot m_2 \cdots m_n$.

1. Show the solution is unique modulo m. (Recall that a solution is unique modulo m means given two solutions $x, x' \in \mathbb{Z}$, we must have $x \equiv x' \pmod{m}$.)

2. Suppose m_i's are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.

3. Suppose m_i's are not pairwise relatively prime and a solution exists. Is it guaranteed that the solution is unique modulo m? Prove or give a counterexample.