CS 70 Discrete Mathematics and Probability Theory
Summer 2023 Huang, Suzani, and Tausik

# DIS 2D

## 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?

**Solution:**

(a) Filling in the blanks,

$$\begin{aligned}\mathbf{3} &= 1 \times \mathbf{54} - 3 \times \mathbf{17} \\ \mathbf{2} &= 1 \times \mathbf{17} - 5 \times \mathbf{3} \\ \mathbf{1} &= 1 \times \mathbf{3} - 1 \times \mathbf{2} \\ [\mathbf{0} &= 1 \times \mathbf{2} - 2 \times \mathbf{1}]\end{aligned}$$

It may be easier to think about this in a rearranged form: $\mathbf{54} = 3 \times \mathbf{17} + \mathbf{3}$, etc.; this directly corresponds to the 54 mod 17 = 3 operation in the forward pass, and the desired blank comes from $\lfloor 54/17 \rfloor$.

(b) Working our way backward up the equalities and substituting them in, we have

$$\begin{aligned}1 &= 1 \times \mathbf{3} - 1 \times \mathbf{2} \\ &= 1 \times \mathbf{3} - 1 \times (1 \times \mathbf{17} - 5 \times \mathbf{3}) \\ &= -1 \times \mathbf{17} + 6 \times \mathbf{3} \\ &= -1 \times \mathbf{17} + 6 \times (1 \times \mathbf{54} - 3 \times \mathbf{17}) \\ &= 6 \times \mathbf{54} - 19 \times \mathbf{17}\end{aligned}$$

(c) Doing the forward pass,

$$\begin{aligned}\gcd(39,17) &= \gcd(17,5) \\ &= \gcd(5,2) \\ &= \gcd(2,1) \\ &= \gcd(1,0)\end{aligned} \qquad \begin{aligned}\mathbf{5} &= 1 \times \mathbf{39} - 2 \times \mathbf{17} \\ \mathbf{2} &= 1 \times \mathbf{17} - 3 \times \mathbf{5} \\ \mathbf{1} &= 1 \times \mathbf{5} - 2 \times \mathbf{2} \\ [\mathbf{0} &= 1 \times \mathbf{2} - 2 \times \mathbf{1}]\end{aligned}$$

Going back up, we have

$$\begin{aligned}\mathbf{1} &= 1 \times \mathbf{5} - 2 \times \mathbf{2} \\ &= 1 \times \mathbf{5} - 2 \times (1 \times \mathbf{17} - 3 \times \mathbf{5}) \\ &= -2 \times \mathbf{17} + 7 \times \mathbf{5} \\ &= -2 \times \mathbf{17} + 7 \times (1 \times \mathbf{39} - 2 \times \mathbf{17}) \\ &= 7 \times \mathbf{39} - 16 \times \mathbf{17}\end{aligned}$$

This leaves us with a final answer of $1 = 7 \times \mathbf{39} - 16 \times \mathbf{17}$.

(d) It is equal to $-16$ mod 39, which is equal to 23 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 $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

**Solution:**

Proceed by induction.

**Base Case:** We have $\gcd(F_1, F_0) = \gcd(1, 0) = 1$, which is true.

**Inductive Hypothesis:** Assume we have $\gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$.

**Inductive Step:** Now we need to show that $\gcd(F_{k+1}, F_k) = 1$ as well.

We can show that:

$$\gcd(F_{k+1}, F_k) = \gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1}) = 1.$$

Note that the second expression comes from the definition of Fibonacci numbers. The last expression comes from Euclid's GCD algorithm, in which $\gcd(x, y) = \gcd(y, x \bmod y)$, since

$$F_k + F_{k-1} \equiv F_{k-1} \pmod{F_k}.$$

Therefore the statement is also true for $n = k + 1$.

By the rule of induction, we can conclude that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

## 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).

**Solution:**

(a) Observe that $a+3b+4c \equiv 1+0+0 \pmod 3$, $a+3b+4c \equiv 0+3+0 \pmod 7$ and $a+3b+4c \equiv 0+0+4 \pmod{11}$. Therefore $x = a+3b+4c$ indeed satisfies the conditions in (1).

(b) This question asks to find a number $0 \leq a < 3 \times 7 \times 11$ that is divisible by 7 and 11 and has a remainder of 1 when divided by 3.

Starting with a number divisible by 7 and 11, we can start with $7 \cdot 11 = 77$. Notice that we can multiply by the multiplicative inverse mod 3 to make it equivalent to $1 \pmod 3$. In particular, since $77 \cdot 77^{-1} \equiv 1 \pmod 3$, we just need to compute

$$77^{-1} \equiv 2^{-1} \equiv 2 \pmod 3.$$

This gives us $a = 77 \cdot 2 = 154$.

We can check to make sure that what we've computed actually satisfies (2):

$$\begin{aligned} 154 &= 3 \cdot 51 + 1 \equiv 1 \pmod 3 \\ 154 &= 22 \cdot 7 \equiv 0 \pmod 7 \\ 154 &= 14 \cdot 11 \equiv 0 \pmod{11} \end{aligned}$$

Taking a step back, notice that what we've computed is

$$a = (7 \cdot 11) \cdot \left((7 \cdot 11)^{-1} \bmod 3\right).$$

Here, the first term ensures that we have a multiple of 7 and 11, and the last term ensures that we have a quantity equivalent to $1 \pmod 3$.

(c) Using a similar approach here, we can start with a multiple of 3 and 11; namely, $3 \cdot 11 = 33$.

Here, we can multiply by its multiplicative inverse mod 7 to make it equivalent to $1 \pmod 7$. In particular, we just need to compute

$$33^{-1} \equiv 5^{-1} \equiv 3 \pmod 7.$$

This gives us $b = 33 \cdot 3 = 99$.

Again, notice that we've essentially just computed

$$b = (3 \cdot 11) \cdot \left((3 \cdot 11)^{-1} \bmod 7\right).$$

(d) Similarly, we can start with a multiple of 3 and 7; namely, $3 \cdot 7 = 21$.

Here, we can multiply by its multiplicative inverse mod 11 to make it equivalent to $1 \pmod{11}$. In particular, we just need to compute

$$21^{-1} \equiv 10^{-1} \equiv 10 \pmod{11}.$$

This gives us $c = 21 \cdot 10 = 210$.

Again, notice that we've essentially just computed

$$c = (3 \cdot 7) \cdot \left((3 \cdot 7)^{-1} \bmod 11\right).$$

(e) From Parts (b), (c) and (d) we've found $a = 154$, $b = 99$, and $c = 210$ which satisfies (2), (3) and (4) respectively. Together with Part (a) of the question, this implies that

$$x = a + 3b + 4c = 154 + 3 \cdot 99 + 4 \cdot 210 = 154 + 297 + 840 = 1291$$

satisfies the required criterion in (1).

To verify this, observe that

$$\begin{aligned} 1291 &= 430 \times 3 + 1 \equiv 1 \pmod{3} \\ 1291 &= 184 \times 7 + 3 \equiv 3 \pmod{7} \\ 1291 &= 117 \times 11 + 4 \equiv 4 \pmod{11} \end{aligned}$$

Further, this solution will be unique mod $3 \cdot 7 \cdot 11 = 231$, so we have $x \equiv 1291 \equiv 136 \pmod{231}$.

As a side note, what we're essentially doing here is computing values that satisfy exactly one of the equivalences, while not affecting any of the other equivalences. In particular, suppose we have a system of $k$ modular equations $x \equiv a_i \pmod{m_i}$ for $i = 1$ through $k$. For each equation, we want a value $b_i \equiv 1 \pmod{m_i}$ and $b_i \equiv 0 \pmod{m_j}$ for $j \neq i$, such that $a_i b_i$ satisfies exactly the mod $m_i$ equivalence but is equivalent to zero for everything else. This way, adding up all of the $a_i b_i$'s will give us a quantity that satisfies all of the equivalences.

Computing each $b_i$ can be written as the following formula:

$$b_i = \frac{M}{m_i} \cdot \left( \left( \frac{M}{m_i} \right)^{-1} \bmod m_i \right),$$

where $M = m_1 \cdot m_2 \cdots m_k$. The first term ensures that $b_i \equiv 0 \pmod{m_j}$ for $j \neq i$, and the second term ensures that $b_i \equiv 1 \pmod{m_i}$. The solution can then be computed by

$$x \equiv \sum_{i=1}^{k} a_i b_i \pmod{M}.$$

# 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.

**Solution:**

1. Suppose $x, x' \in \mathbb{Z}$ are two solutions to the system of linear congruences. For $1 \leq i \leq n$, we have $x \equiv x' \pmod{m_i}$. Then $m_i \mid x' - x$. Since $m_i$'s are pairwise relatively prime, we have $m \mid x' - x$. Hence $x \equiv x' \pmod{m}$.
2. No. For example, the system
$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{4} \end{aligned}$$
doesn't have a solution, since the first congruence says $x$ is odd but the second says $x$ is even.
3. No. For example, consider
$$\begin{aligned} x &\equiv 0 \pmod{4} \\ x &\equiv 0 \pmod{8} \end{aligned}$$
Then $x = 0$ is a solution. But $x = 8$ is also a solution, and $0 \not\equiv 8 \pmod{32}$.