CS 70 Discrete Mathematics and Probability Theory
Spring 2025 Rao

# DIS 3B

## Modular Arithmetic Intro II

Note 6

**Euclidean Algorithm**: An algorithm to find $\gcd(x,y)$ efficiently, using the following two identities:

- $\gcd(x,y) = \gcd(y,x)$
- $\gcd(x,y) = \gcd(y, x \bmod y)$

**Extended Euclidean Algorithm**: An extension to the Euclidean algorithm allowing us to find coefficients $a$ and $b$ such that $ax+by = \gcd(x,y)$, given inputs $x$ and $y$ (this is known as *Bezout's identity*). In particular, the *forward pass* of the algorithm is the standard Euclidean algorithm, and the *backward pass* of the algorithm allows us to find the coefficients. Note that if $\gcd(x,y) = 1$, then the equation $ax+by = \gcd(x,y) = 1$ tells us that $(a,x)$ are inverses in $\pmod{y}$ and $(b,y)$ are inverses in $\pmod{x}$.

**Chinese Remainder Theorem**: Given a system of $k$ modular equations $x \equiv a_i \pmod{n_i}$, for various constants $a_i$ and coprime moduli $n_i$, there exists a *unique* solution $x$ defined as follows:

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

$$b_i = \left(\frac{N}{n_i}\right)\left(\left(\frac{N}{n_i}\right)^{-1} \bmod n_i\right)$$

$$N = \prod_{i=1}^{k} n_i$$

## 1 Extended Euclid: Two Ways

Note 6

In this problem, we will explore the Extended Euclid's Algorithm: first, the traditional implementation, and second, a faster, iterative version. Both ways yield the same result.

Parts (b) and (c) explore the traditional 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) As motivation, suppose we've found values of $a$ and $b$ such that $54a + 17b = 1$. With this knowledge, what is $17^{-1} \pmod{54}$?

(b) 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)

(c) 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:

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

What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 54?

(d) In the previous parts, we used a recursive method to write $\gcd(54,17)$ as a linear combination of 54 and 17. We can also compute the same result iteratively—this is an alternative to the above method that is oftentimes faster. We begin by writing equations for our initial arguments, 54 and 17, as a linear combination of themselves:

$$\begin{aligned}
54 &= 1\times\mathbf{54} + 0\times\mathbf{17} && (E_1)\\
17 &= 0\times\mathbf{54} + 1\times\mathbf{17} && (E_2)
\end{aligned}$$

We can then use these initial equations (labeled $E_1$ and $E_2$ for ease of reference) to iteratively write reduced values as linear combinations of 54 and 17, until we are able to write an equation for $\gcd(54,17)$, as desired.

In particular, we want to subtract as many multiples of the second equation as possible from the first to create a new equation with a lower LHS value. We can keep iterating until the

LHS becomes $\gcd(54,17) = 1$.

$$\_\_\_\_ = \_\_\_\_ \times \mathbf{54} + \_\_\_\_ \times \mathbf{17} \qquad (E_3 = E_1 - \_\_\_\_ \times E_2)$$
$$\_\_\_\_ = \_\_\_\_ \times \mathbf{54} + \_\_\_\_ \times \mathbf{17} \qquad (E_4 = E_2 - \_\_\_\_ \times E_3)$$
$$1 = \_\_\_\_ \times \mathbf{54} + \_\_\_\_ \times \mathbf{17} \qquad (E_5 = E_3 - \_\_\_\_ \times E_4)$$

What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 54? Verify that your answer is equivalent to the previous part.

(e) Calculate the gcd of 17 and 39, and determine how to express this as a "combination" of 17 and 39. What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 39?

**Solution:**

(a) If we take the equation $54a + 17b = 1 \pmod{54}$, the first term goes to zero (as it is a multiple of 54). This means that we're left with $17b \equiv 1 \pmod{54}$, giving us that $17^{-1} \equiv b \pmod{54}$.

In other words, the coefficients we get from the extended Euclidean algorithm give us the multiplicative inverse directly. This is one of the main reasons why the extended Euclidean algorithm is useful.

(b) Filling in the blanks,

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

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 $\lfloor 54/17 \rfloor$.

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

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

We get that the multiplicative inverse of 17 mod 54 is $-19$, or 35. Note that $-19 \equiv 35 \bmod 54$.

(d) We have the following operations on the equations:

$$\begin{aligned}
54 &= 1 \times \mathbf{54} + 0 \times \mathbf{17} && (E_1)\\
17 &= 0 \times \mathbf{54} + 1 \times \mathbf{17} && (E_2)\\
3 &= 1 \times \mathbf{54} - 3 \times \mathbf{17} && (E_3 = E_1 - 3E_2)\\
2 &= -5 \times \mathbf{54} + 16 \times \mathbf{17} && (E_4 = E_2 - 5E_3)\\
1 &= 6 \times \mathbf{54} - 19 \times \mathbf{17} && (E_5 = E_3 - E_4)
\end{aligned}$$

Notice that the LHS also corresponds to the simplifications in the forward pass of the Euclidean algorithm; we're doing the same calculations (i.e. to determine how much to subtract), and we're also doing the backward pass at the same time. This is why the iterative method can be more intuitive and quicker than the recursive method in the previous parts.

Again, we get that the multiplicative inverse of 17 mod 54 is $-19$, or 35.

(e) With the recursive algorithm, we have

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

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 $1 = 7 \times \mathbf{39} - 16 \times \mathbf{17}$, making the inverse $17^{-1} \equiv -16 \equiv 23 \pmod{39}$.

With the iterative algorithm, we have

$$\begin{aligned}
39 &= 1 \times \mathbf{39} + 0 \times \mathbf{17} && (E_1)\\
17 &= 0 \times \mathbf{39} + 1 \times \mathbf{17} && (E_2)\\
5 &= 1 \times \mathbf{39} - 2 \times \mathbf{17} && (E_3 = E_1 - 2E_2)\\
2 &= -3 \times \mathbf{39} + 7 \times \mathbf{17} && (E_4 = E_2 - 3E_3)\\
1 &= 7 \times \mathbf{39} - 16 \times \mathbf{17} && (E_5 = E_3 - 2E_4)
\end{aligned}$$

## 2 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):

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

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

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

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

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

# 3 Baby Fermat

Note 6

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 $j$?

**Solution:**

(a) There are only $m$ possible values mod $m$, and so after the $m$-th term we should see repetitions.

The Pigeonhole principle applies here - we have $m$ boxes that represent the different unique values that $a^k$ can take on $\pmod{m}$. Then, we can view $a, a^2, a^3, \cdots$ as the objects to put in the $m$ boxes. As soon as we have more than $m$ objects (in other words, we reach $a^{m+1}$ in our sequence), the Pigeonhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value $\pmod{m}$.

(b) We will temporarily use the notation $a^*$ for the multiplicative inverse of $a$ to avoid confusion.

If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod m,\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} && \pmod m,\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} && \pmod m,\\
a^{i-j} &\equiv 1 && \pmod m.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod m$ as $a^{i-j-1}a \equiv 1 \pmod m$. Therefore $a^{i-j-1}$ is the multiplicative inverse of $a \pmod m$.