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 $x \bmod y$, 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:

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

(Fill in the blanks)

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

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

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:

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

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

$$\begin{aligned}
\underline{\qquad} &= \underline{\qquad}\times\mathbf{54} + \underline{\qquad}\times\mathbf{17} && (E_3 = E_1 - \underline{\qquad}\times E_2) \\
\underline{\qquad} &= \underline{\qquad}\times\mathbf{54} + \underline{\qquad}\times\mathbf{17} && (E_4 = E_2 - \underline{\qquad}\times E_3) \\
1 &= \underline{\qquad}\times\mathbf{54} + \underline{\qquad}\times\mathbf{17} && (E_5 = E_3 - \underline{\qquad}\times E_4)
\end{aligned}$$

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?

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).

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?