Discussion 3A

CS 70, Summer 2024

1 Euclidean Identities

In lecture, we used a few identities without proving them. Let's do that now.

(a) In this part, we prove the gcd identity used in Euclid's algorithm.

Let $a, b, q, r \in \mathbb{Z}$ be any integers such that $a = bq + r$. Prove that $\gcd(a, b) = \gcd(b, r)$.

(b) In this part, we will prove Bezout's identity: for any integers $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

If a and b are both zero, we have that $\gcd(0, 0) = 0 = 0x + 0y$ for any $x, y \in \mathbb{Z}$. It remains to show the identity when a and b are not both zero. We will assume this for the remainder of the question.

(i) Let $S = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\}$. Prove that $S \neq \varnothing$.

(ii) Let $d \in S$ be the smallest element of S. Show that d is a *common divisor* of a and b: $d \mid a$ and $d \mid b$.

(*Hint*: Prove that $r = a \bmod d$ must be 0.)

(iii) Let c be any other common divisor of a and b. Show that $c \leq d$.

(iv) Explain how you have shown that there exist x and y such that $\gcd(a, b) = ax + by$.

2 The Extended Euclidean Algorithm

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 $54a + 17b = 1$. Use this to find $17^{-1} \pmod{54}$ in terms of a and b.

(b) Note that $x \bmod y$, by definition, is always x minus a multiple of y. Therefore, in the execution of Euclid's algorithm, each newly introduced value can always be expressed as a "combination" of the previous two.

For example, since $\mathbf{54} \bmod \mathbf{17} = \mathbf{3}$, we have that $\mathbf{54} = 3 \times \mathbf{17} + \mathbf{3}$. Therefore, we can write $\mathbf{3} = 1 \times \mathbf{54} - 3 \times \mathbf{17}$.

Use this fact to fill in the blanks alongside the calculation of $\gcd(54, 17)$.

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

(c) Our goal is to fill out the blanks in

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

To do so, we will work our way up from the bottom of our list our equations. We will repeatedly express our calculated gcd as a combination of the two arguments on each of the previous lines.

Use the equations from **(b)** to fill in the blanks.

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

(d) Use part **(c)** to find the multiplicative inverse of 17 in arithmetic mod 54.

(e) 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 method from parts **(b)** and **(c)** that is oftentimes faster.

We begin by writing equations for our initial arguments, 54 and 17, as a linear combination of themselves:

$$54 = 1 \times \mathbf{54} + 0 \times \mathbf{17} \qquad (E_1)$$
$$17 = 0 \times \mathbf{54} + 1 \times \mathbf{17} \qquad (E_2)$$

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 value on the left-hand side. We can keep iterating until the left-hand side becomes $\gcd(54, 17) = 1$.

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

(f) Use part **(e)** to find the multiplicative inverse of 17 in arithmetic mod 54. Verify that your answer is equivalent to your answer to part **(d)**.

(g) Calculate the gcd of 17 and 39, and determine how to express this in terms of 17 and 39. Use your result to find the multiplicative inverse of 17 in arithmetic mod 39.

3 Modular Inverses

Recall that for $a, m \in \mathbb{Z}$ with $m > 0$, we say that x is an inverse of a modulo m if $ax \equiv 1 \pmod{m}$. In this question, we will investigate the existence and uniqueness of inverses in arithmetic modulo m.

(a) Prove or disprove that 3 is an inverse of 5 modulo 10.

(b) Prove or disprove that 3 is an inverse of 5 modulo 14.

(c) Prove or disprove that 4 has an inverse modulo 8.

(d) We saw in lecture that if $\gcd(a, m) = 1$, then a has an inverse modulo m. Prove that if a has an inverse modulo m, then $\gcd(a, m) = 1$.

(e) Suppose that $x \in \mathbb{Z}$ is an inverse of a modulo m. Prove that $x + m$ is also an inverse of a modulo m.

(f) Suppose that $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ are both inverses of a modulo m. Prove that $x \equiv y \pmod{m}$.