Discussion 3A

CS 70, Summer 2024

1 Euclidean Identities

(a) We show that a, b and b, r share the same common divisors. We will show that

$$d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r.$$

Suppose $d \mid a$ and $d \mid b$. Then by **Lemma 1** from Note 7, $d \mid (a - bq)$. That is, $d \mid r$.

Now suppose that $d \mid b$ and $d \mid r$. Then by **Lemma 1** from Note 7, $d \mid (bq + r)$. So $d \mid a$.

(b) **(i)** Without loss of generality, suppose that $a \neq 0$. Then either $a > 0$ or $a < 0$.

(1) If $a > 0$, then $a \cdot 1 + b \cdot 0 > 0$ and so $a \in S$.

(2) If $a < 0$, then $-a \cdot 1 + b \cdot 0 > 0$ and so $-a \in S$.

In either case, there is an element in S and so $S \neq \varnothing$.

(ii) Suppose that $r = a \bmod d \neq 0$. By the division algorithm, there exists $q \in \mathbb{Z}$ such that $a = qd + r$. So $r = a - qd > 0$. But then, since $d \in S$, there are $x, y \in \mathbb{Z}$ such that $d = ax + by$. Therefore

$$\begin{aligned} r &= a - dq \\ &= a(1) + (ax + by)q \\ &= a(1 - xq) + b(yq). \end{aligned}$$

So $r \in S$. Moreover, by the division algorithm, $r < d$. This is a contradiction, since d was the smallest element of S. Therefore in fact $r = 0$ and so $d \mid a$.

The same proof shows that $d \mid b$.

(iii) We will show that $c \mid d$. Since $c \mid a$ and $c \mid b$, we know $a = cj$ and $b = ck$ for some $j, k \in \mathbb{Z}$. Then

$$\begin{aligned} d &= ax + by \\ &= cjx + cky \\ &= c(jx + ky). \end{aligned}$$

Since $j, k, x, y \in \mathbb{Z}$, so is $jx + ky$. Therefore $c \mid d$. So $c \leq d$.

(iv) We have shown in **(ii)** that $d \mid a$ and $d \mid b$, and we have shown in **(iii)** that for any other c such that $c \mid a$ and $c \mid b$, $c \leq d$. So d is the greatest common divisor of a and b.

Therefore we have shown that there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b).$$

2 The Extended Euclidean Algorithm

(a) Taking the equation $54a + 17b = 1$ with respect to the modulus 54, we have that

$$\begin{aligned} 54a + 17b &\equiv 1 \pmod{54} \\ 17b &\equiv 1 \pmod{54}. \end{aligned}$$

By definition, $b \equiv 17^{-1} \pmod{54}$. That is, b is an inverse of 17 modulo 54.

(b) We get

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

(c) We get

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

(d) By parts **(c)** and **(a)**, we know that -19 is a multiplicative inverse of 17 modulo 54. To get it as a remainder modulo 54, we use the fact that $a \equiv m - a \pmod{m}$:

$$-19 \equiv 54 - 19 \equiv 35 \pmod{54}.$$

So $35 = 17^{-1} \bmod 54$.

(e) Use the equations from **(b)**.

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

(f) We get once again that -19 is a multiplicative inverse of 17 modulo 54. This yields the same answer that $35 = 17^{-1} \bmod 54$.

(g) Using the Euclidean algorithm,

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

Now we iteratively substitute into our last equation to get every bolded term in terms of **17** and **39**.

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

Therefore -16 is an inverse of 17 modulo 39. In particular, since $-16 \equiv 23 \pmod{39}$, we have that $23 = 17^{-1} \bmod 39$.

We can instead use the iterative approach by using the equations all the way on the right-hand side of our Euclidean algorithm's output.

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

3 Modular Inverses

(a) Since $3 \cdot 5 \equiv 15 \equiv 5 \pmod{10}$, 3 is not an inverse of 5 modulo 10.

(b) Since $3 \cdot 5 \equiv 15 \equiv 1 \pmod{14}$, 3 is an inverse of 5 modulo 14.

(c) Suppose that for some $x \in \mathbb{Z}$, $4x \equiv 1 \pmod{8}$. Then by Bezout's identity, there are integers $x, y \in \mathbb{Z}$ such that

$$\begin{aligned} 1 &= 4x + 8y \\ 1 &= 4(x + 2y) \\ \frac{1}{4} &= x + 2y. \end{aligned}$$

This is a contradiction, since $x + 2y \in \mathbb{Z}$.

(d) Suppose for contradiction a has an inverse modulo m and that $\gcd(a, m) = d > 1$. Then $d \mid a$ and $d \mid m$, so $a = dj$ and $m = dk$ for some $j, k \in \mathbb{Z}$.

Let $x \in \mathbb{Z}$ be the inverse of a modulo m. Then $ax \equiv 1 \pmod{m}$, so $ax + my = 1$ for some $y \in \mathbb{Z}$. Then

$$\begin{aligned} 1 &= ax + my \\ 1 &= djx + dky \\ 1 &= d(jx + ky). \end{aligned}$$

So $d \mid 1$. But only 1 divides 1, and $d > 1$. So it must instead be the case that $d = 1$.

(e) We show that $a(x + m) \equiv 1 \pmod{m}$.

$$\begin{aligned} a(x + m) &\equiv ax + am && \pmod{m} \\ &\equiv 1 + 0 && \pmod{m} \\ &\equiv 1. && \pmod{m} \end{aligned}$$

So $x + m$ is an inverse modulo m.

(f) Since x is an inverse of a modulo m, $ax \equiv 1 \pmod{m}$ and $ya \equiv 1 \pmod{m}$. Then

$$\begin{aligned} ax &\equiv 1 && \pmod{m} \\ yax &\equiv y && \pmod{m} \\ x &\equiv y && \pmod{m}. \end{aligned}$$