

1 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of a modulo m** .

Now, we will investigate the existence and uniqueness of inverses. (From part a to part d, you are not allowed to use the theorem that will be proved in e and f).

- (a) Is 3 an inverse of 5 modulo 10?
- (b) Is 3 an inverse of 5 modulo 14?
- (c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?
- (d) Does 4 have inverse modulo 8?
- (e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m . Is it possible that $x \not\equiv x' \pmod{m}$?
- (f) Prove the following theorem: if $\gcd(a, m) = 1$ and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m . (That is, there is a unique integer $0 \leq x < m$ that is an inverse of a modulo m ; if $x' \in \mathbb{Z}$ is an inverse of a modulo m , then $x' \equiv x \pmod{m}$.)
- (g) Prove the converse of (f) is true: let $a, m \in \mathbb{Z}$ and $m > 1$; if an inverse of a modulo m exists, then a and m are relatively prime.

2 Euclid Verification

Let $a = bq + r$ where a, b, q and r are integers. Prove $\gcd(a, b) = \gcd(b, r)$.

(This shows that the Euclidean algorithm works!)

3 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 $x \bmod y$, 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:

$$\begin{aligned}
\gcd(2328, 440) &= \gcd(440, 128) & [128 &= 1 \times 2328 + (-5) \times 440] \\
&= \gcd(128, 56) & [56 &= 1 \times 440 + ____ \times 128] \\
&= \gcd(56, 16) & [16 &= 1 \times 128 + ____ \times 56] \\
&= \gcd(16, 8) & [8 &= 1 \times 56 + ____ \times 16] \\
&= \gcd(8, 0) & [0 &= 1 \times 16 + (-2) \times 8] \\
&= 8.
\end{aligned}$$

(Fill in the blanks)

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

$$8 = ____ \times 2328 + ____ \times 440.$$

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:

$$\begin{aligned}
8 &= 1 \times 8 + 0 \times 0 = 1 \times 8 + (1 \times 16 + (-2) \times 8) \\
&= 1 \times 16 - 1 \times 8 \\
&= ____ \times 56 + ____ \times 16
\end{aligned}$$

[Hint: Remember, $8 = 1 \times 56 + (-3) \times 16$. Substitute this into the above line.]

$$= ____ \times 128 + ____ \times 56$$

[Hint: Remember, $16 = 1 \times 128 + (-2) \times 56$.]

$$\begin{aligned}
&= ____ \times 440 + ____ \times 128 \\
&= ____ \times 2328 + ____ \times 440
\end{aligned}$$

- (c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

- (d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?