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.

(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 $x \not\equiv x' \pmod{m}$?

* an inverse of a mod m exists iff a and m are coprime
⇕
gcd(a, m) = 1

a) No $3 \cdot 5 = 15 \equiv 5 \pmod{10}$

b) yes $3 \cdot 5 = 15 \equiv 1 \pmod{14}$

c) yes $(3+14n) \cdot 5 = 15 + 14 \cdot 5n \equiv 1 \pmod{14}$

d) No $\gcd(4, 8) = 4 \neq 1$

e) No $ax \equiv 1 \pmod{m}$ and $ax' \equiv 1 \pmod{m}$

$$ax \equiv ax' \pmod{m}$$
$$ax - ax' \equiv 0 \pmod{m}$$
$$x \cdot a(x - x') \equiv x \cdot 0 \pmod{m}$$
$$(x - x') \equiv 0 \pmod{m}$$
$$x \equiv x' \pmod{m}$$

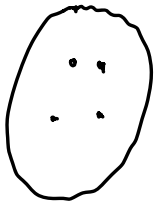
2 Euclid Verification

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!)

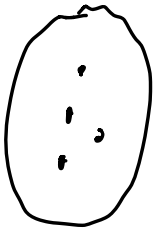
i.e. gcd(a,b) = gcd(b, a mod b)

we will show the common divisors of a, b & b, r are the same.

D(A): Divisors of a, b



D(R): Divisors of b, r



Show D(A) = D(R)

D(A) ⊆ D(R):

- suppose d | a & d | b. This means d | bq, also d | bq + r so d | bq + r − bq ⇒ d | r (from notes)

D(R) ⊆ D(A):

- suppose d | b & d | r. This means d | bq so d | bq + r ⇒ d | a

thus gcd(a,b) = gcd(b,r) □

gcd(a,b) = x a + y b

1 = x a + y b

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 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:

$$\begin{aligned}
\gcd(2328,440) &= \gcd(440,128) && [\mathbf{128} = 1\times\mathbf{2328} + (-5)\times\mathbf{440}]\\
&= \gcd(128,56) && [\mathbf{56} = 1\times\mathbf{440} + \underline{-3}\times\mathbf{128}]\\
&= \gcd(56,16) && [\mathbf{16} = 1\times\mathbf{128} + \underline{-2}\times\mathbf{56}]\\
&= \gcd(16,8) && [\mathbf{8} = 1\times\mathbf{56} + \underline{-3}\times\mathbf{16}]\\
&= \gcd(8,0) && [\mathbf{0} = 1\times\mathbf{16} + (-2)\times\mathbf{8}]\\
&= 8.
\end{aligned}$$

(Fill in the blanks)

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

$$8 = \underline{\quad}\times\mathbf{2328} + \underline{\quad}\times\mathbf{440}.$$

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:

$$\begin{aligned}
8 &= 1\times\mathbf{8} + 1\times\mathbf{0} = 1\times\mathbf{8} + (1\times\mathbf{16} + (-2)\times\mathbf{8})\\
&= 1\times\mathbf{16} - 1\times\mathbf{8}\\
&= \underline{-1}\times\mathbf{56} + \underline{4}\times\mathbf{16}
\end{aligned}$$

1·16 - 1·[1·56 + (-3)·16]

1·16 - 1·56 + 3·16

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

$$= \underline{4}\times\mathbf{128} + \underline{-9}\times\mathbf{56}$$

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

$$\begin{aligned}
&= \underline{-9}\times\mathbf{440} + \underline{31}\times\mathbf{128}\\
&= \underline{31}\times\mathbf{2328} + \underline{-169}\times\mathbf{440}
\end{aligned}$$

(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.

if y = 0 return (x, 1, 0)

else

(d, a, b) = eegcd(y, x mod y)

return (d, b, a - ⌊x/y⌋ b))

(d, a, b) $\quad d = ay + b(x \bmod y)$

$= bx + (a - \lfloor x/y \rfloor b)y$

$\gcd(38,17)$ $(1,-4,9) \Rightarrow \boxed{1 = -4 \cdot 38 + 9 \cdot 17}$

$\gcd(17,4)$ $(1,1,-4)$ $\quad 1 - 4 \cdot 0 = 1$

$\gcd(4,1)$ $(1,0,1)$ $\quad 1 = 0 \cdot 4 + 1 \cdot 1$

$\gcd(1,0)$ $(1,1,0)$ $\quad 1 = 1 \cdot 1 + 0 \cdot 0$

$\uparrow \uparrow \uparrow$

$d \; a \; b$

$\gcd(38,17)$ $\quad$ * Iterative 版 GCD

$38, 17$

① $38 = 0 \cdot 17 + 1 \cdot 38$ $\quad 17, 4 \quad 38 - 2(17) = 4$

$-2(17 = 1 \cdot 17 + 0 \cdot 38)$

$4 = -2 \cdot 17 + 1 \cdot 38$ $\quad 4, 1 \quad 17 - 4(4) = 1$

② $17 = 1 \cdot 17 + 0 \cdot 38$

$-4(4 = -2 \cdot 17 + 1 \cdot 38)$

$\boxed{1 = 9 \cdot 17 - 4 \cdot 38}$

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

$17^{-1} \bmod 38 = 9$