CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes **DIS 2D**

## 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 $0 \le x < m$ 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.

**Solution:**

(a) No, because $3 \cdot 5 = 15 \equiv 5 \pmod{10}$.

(b) Yes, because $3 \cdot 5 = 15 \equiv 1 \pmod{14}$.

(c) Yes, because $(3 + 14n) \cdot 5 = 15 + 14 \cdot 5n \equiv 15 \equiv 1 \pmod{14}$.

(d) No. For contradiction, assume $x \in \mathbb{Z}$ is an inverse of 4 modulo 8. Then $4x \equiv 1 \pmod{8}$. Then $8 \mid 4x - 1$, which is impossible.

(e) No. We have $xa \equiv x'a \equiv 1 \pmod{m}$. So

$$xa - x'a = a(x - x') \equiv 0 \pmod{m}.$$

Multiply both sides by $x$, we get

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

$$\implies x - x' \equiv 0 \pmod{m}.$$
$$\implies x \equiv x' \pmod{m}$$

(f) Part (5) already shows that once an inverse modulo $m$ exists, it is unique modulo $m$. We will now show the existence.

Since $a$ and $m$ are relatively prime, we know $\gcd(a,m) = 1$. Hence, there exists $s,t \in \mathbb{Z}$ such that $1 = as + mt$. Therefore, $1 \equiv as + mt \equiv as \pmod{m}$. By definition, $s$ is an inverse of $a$ modulo $m$.

(g) Suppose $x \in \mathbb{Z}$ is an inverse of $a$ modulo $m$, i.e. $xa \equiv 1 \pmod{m}$. Then $m \mid xa - 1$. Then, there exists $b \in \mathbb{Z}$ such that $mb = xa - 1$.

Suppose $n = \gcd(a,m) > 1$. Then

$$mb \equiv xa - 1 \pmod{n}$$
$$\implies 0 \equiv -1 \pmod{n}$$
$$\implies n \mid 1$$

which is impossible.

## 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!)

**Solution:** If we can show that the common divisors of $a$ and $b$ are the same as the common divisors of $b$ and $r$, we will have shown that $\gcd(a,b) = \gcd(b,r)$, because both pairs must have the same greatest common divisor.

Suppose that $d$ divides both $a$ and $b$. Then it follows that $d$ also divides $a - bq = r$. Hence, any common divisor of $a$ and $b$ is also a common divisor of $b$ and $r$.

Conversely, suppose that $d$ divides both $b$ and $r$. Then $d$ also divides $bq + r = a$. Hence, any common divisor of $b$ and $r$ is also a common divisor of $a$ and $b$.

Thus, $\gcd(a,b) = \gcd(b,r)$.

## 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:

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

(Fill in the blanks)

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

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

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:

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

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

$$= \underline{\qquad}\times\mathbf{128} + \underline{\qquad}\times\mathbf{56}$$

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

$$\begin{aligned}
&= \underline{\qquad}\times\mathbf{440} + \underline{\qquad}\times\mathbf{128} \\
&= \underline{\qquad}\times\mathbf{2328} + \underline{\qquad}\times\mathbf{440}
\end{aligned}$$

(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.

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

**Solution:**

(a) -3

-2

-3

(b) $1 \times \mathbf{16} - 1 \times (1 \times \mathbf{56} + (-3) \times \mathbf{16}) = -1 \times \mathbf{56} + 4 \times \mathbf{16}$

$-1 \times \mathbf{56} + 4 \times (1 \times \mathbf{128} + (-2) \times \mathbf{56}) = 4 \times \mathbf{128} - 9 \times \mathbf{56}$

$4 \times \mathbf{128} - 9 \times (1 \times \mathbf{440} + (-3) \times \mathbf{128}) = -9 \times \mathbf{440} + 31 \times \mathbf{128}$

$-9 \times \mathbf{440} + 31 \times (1 \times \mathbf{2328} + (-5) \times \mathbf{440}) = 31 \times \mathbf{2328} - 164 \times \mathbf{440}$

(c) $\gcd(17, 38) = 1 = 13 \times 38 - 29 \times 17$; also, more simply, $-4 \times 38 + 9 \times 17$, but the algorithm produces the former.

(d) It is equal to $-29$, which is equal to 9.