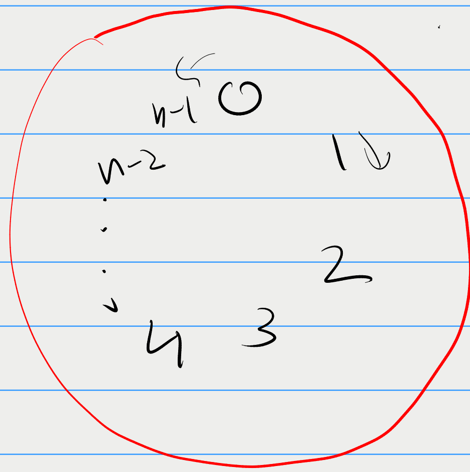
Discussion 2D

Modular Arithmetic Review

mod n



$-1 \bmod 2$

$ab \bmod 2$

$a+b \bmod n$

$a \bmod n + b \bmod n$

7.1

$a \equiv c \pmod{m}$ $\quad b \equiv d \pmod{m}$ $\quad a+b \equiv c+d \pmod{m}$

mod p $\quad p$ is a prime

$x \in \{0, \dots, p-1\}$ $\quad \gcd(x,p) = 1$

$\underline{ax + by} = 1$ $\quad \gcd(a,b) = 1$

$a \equiv x \pmod{m}$

$a = qm + x$

$\boxed{\gcd(m,x) = 1}$

x has a unique mod m inverse

$\exists$

$a \cdot a^{-1} \equiv 1 \pmod{m}$

1 Modular Inverses

$-1 \bmod 3$

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**.

$a \cdot a^{-1} \equiv 1 \bmod (m)$
$3 \cdot 5 \equiv 15 \bmod (10)$
$5 \bmod (10) \not\equiv 1$
No.

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).

$xa \equiv x'a \equiv 1 \pmod{m}$
$x a x' \equiv x' a x \equiv x$
$x \equiv x' \pmod{m}$

(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 $x \not\equiv x' \pmod{m}$? no

* This looks a lot like what we do when showing uniqueness. hmmm.....

(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 $x' \equiv x \pmod{m}$.)

Proof

(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.

(a) $a \cdot a^{-1} \equiv 1 \bmod m$

$5 \cdot 3 \equiv 15 \equiv 5 \bmod 10$

$\boxed{\text{no.}}$

$\gcd(a, m) = 1$

$as + mt = 1$

(b) $5 \cdot 3 \equiv 15 \equiv 1 \bmod 14$

yes.

$s, t \in \mathbb{N}$

$ax + by = 1$

$\gcd(a, b)$

$n = \gcd(1)$

$(3 + 14n) \cdot 5 \equiv 1 \bmod 14$

$3 \cdot 5 + \cancel{14(n \cdot 5)}$

$15 + 0 \equiv 15 \bmod 14 \equiv 1$

$n \mid (as + mt) = 1$

(c)

$2 \mid as + mt$

(d) $\gcd(a, m) = 1$

$\gcd(4, 8) = 4$ does not have inverse

e) $a \pmod{m}$

x, x'

$ax \equiv 1 \pmod{m}$

$ax' \equiv 1 \pmod{m}$

$\underbrace{ax' \equiv ax}\equiv 1 \pmod{m}$

$\cancel{x}\cancel{a}x' \equiv x \cancel{ax'}$

$x' \equiv x \pmod{m}$

f) $\gcd(a, m) = 1$ $\quad s, t \in \mathbb{Z}$

$as + mt = 1$

$as + \cancel{mt}^{0} \equiv 1 \pmod{m}$

$as \equiv 1 \pmod{m}$

s is the inverse of a

$s = x$

g) $as \equiv 1 \mod m$

$as - 1 \equiv 0 \mod m$ $\quad b \in \mathbb{Z}$

$m \mid as - 1$

$mb = as - 1$ $\quad \boxed{\gcd(m, a) = n = 1}$

$\cancel{mb}^{0} \equiv \cancel{as}^{0} - 1 \pmod{n}$

$0 \equiv -1 \pmod{n}$

$1 \equiv 0 \pmod{}$

$n \mid 1$

$n = 1$

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!)

* strengthen the hypothesis

hint! try to prove something stronger

all of the divisors of a and b are equivalent to divisors of b and r

A divide a, b

B divide b, r

Wish to show:

$$\boxed{\begin{array}{l} A = B \\ \text{so} \\ A \supseteq B \ \wedge \ B \supseteq A \end{array}}$$

$A \subseteq B$ First.

$d \in A$, $\rightarrow d \mid a \ \wedge \ d \mid b$ then

$\rightarrow r = a - bq$ ✓ ∂

$d \mid r$

So d is a common divisor of b and r

therefore applies $\forall\, d \in A$, since d is arbitrary

$B \subseteq A$

$d' \in B$ $\quad d' \mid b \ \wedge \ d' \mid r$ then

$a = bq + r$ ✓

thus $d' \mid a$ so d' is a common divisor for a and b

so max of A = max B

$\gcd(a,b) = \gcd(b,r)$ $\forall\, d' \in B$, $B \subseteq A$, thus $B = A$

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:

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

(Fill in the blanks)

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

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

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:

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

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

$$= \_\_\_\_ \times\mathbf{128}+ \_\_\_\_ \times\mathbf{56}$$

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

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

(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?

Error somewhere

0 a b c c d
1 b z x y >
2
3
5 a b c

$$s = \begin{cases} i = a & i = b \\ i \neq a & i = a \end{cases}$$

PrintHW(P, x)

$|E| = |N|$

program

P'(x) :

if x stops
print hello world
else