Modular Arithmetic

- Several important cryptosystems make use of modular arithmetic. This is when the answer to a calculation is always in the range *0 – m* where m is the **modulus**.
- To calculate the value of *n mod m*, you take away as many multiples of m as possible until you are left with an answer between *0* and *m*.

If n is a negative number then you add as many multiples of m as necessary to get an answer in the range 0 – m.

Examples

17 mod 5 = 2	7 mod 11 = 7
20 mod 3 = 2	11 mod 11 = 0
-3 mod 11 = 8	-1 mod 11 = 10
25 mod 5 = 0	-11 mod 11 = 0

- Two numbers ***a*** and ***b*** are said to be "*congruent modulo **n***" if

  $(a \bmod n) = (b \bmod n)$ □ $a \equiv b \pmod{n}$

- The difference between ***a*** and ***b*** will be a multiple of ***n***

  So $a-b = kn$ for some value of k

E.g: $4 \equiv 9 \equiv 14 \equiv 19 \equiv -1 \equiv -6 \bmod 5$

$73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$

If $a \equiv 0 \pmod{n}$, *then* $n|a$.

Properties of Congruences

1. $a \equiv b \pmod{n}$ *if* $n|(a-b)$
2. $a \equiv b \pmod{n}$ *implies* $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ **imply** $a \equiv c \pmod{n}$

Proof of 1.

If $n|(a-b)$, then $(a-b) = kn$ for some k. Thus, we can write $a = b + kn$. Therefore,

$(a \bmod n)$ = (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = $(b \bmod n)$.

Examples

$23 \equiv 8 \pmod{5}$ because $23 - 8 = 15 = 5 \times 3$

$-11 \equiv 5 \pmod{8}$ because $-11 - 5 = -16 = 8 \times (-2)$

$81 \equiv 0 \pmod{27}$ because $81 - 0 = 81 = 27 \times 3$

Properties of Modular Arithmetic

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Proof of 1.

Let $(a \bmod n) = Ra$ and $(b \bmod n) = Rb$. Then, we can write

$a = Ra + jn$ for some integer j and $b = Rb + kn$ for some integer k.

$$
\begin{aligned}
(a + b) \bmod n &= (Ra + jn + Rb + kn) \bmod n \\
&= [Ra + Rb + (k + j)\, n] \bmod n \\
&= (Ra + Rb) \bmod n \\
&= [(a \bmod n) + (b \bmod n)] \bmod n
\end{aligned}
$$

Examples

$11 \bmod 8 = 3$; $15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

Exponentiation

- Exponentiation is done by repeated multiplication, as in ordinary arithmetic.

$$\textit{To find } (11^7 \bmod 13) \textit{ do the followings}$$

$$11^2 = 121 \equiv 4 \pmod{13}$$

$$11^4 \ (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

Sage algorithm for modular exponentiation that computes $x^n \ mod \ m$

```
def exp(x,n,m):
    y=1; u=x % m
    while (n >0):
        if ((n % 2)=1):
            y=(y*u) % m;
        if (n > 0):
            n=floor(n / 2);
        u=(u*u) % m
Output y
```

- $11^7 \bmod 13$, x=11, n=7, m=13
- y=1, u=x%m=11%13=11
- While n>0 yes,
- If n%2=1, 7%2=1 Yes
- *y=(y*u) % m;=(1*11)%13=11*
- *If n>0 yes, n=n/2=3*
- *u=(u*u) % m=(11*11)%13=4*
- *While n>0 yes,*
- *If n%2=1, 3%2=1, yes*
- *y=(y*u) % m;=(11*4)%13*

- If n>0 yes
- n=n/2=3/2=1
- *u=(u*u) % m=(4*4)%13=3*
- While n>0 yes
- If n%2=1, 1%2=1 yes
- *y=(y*u) % m;=(11*4*3)%13=(11*12)%13=132%13=2*
- *If n>0*
- *n=n/2=1/2=0*
- *u=(u*u) % m=9 %13*

A good thing about modular arithmetic is that the numbers you are working with will be kept relatively small. At each stage of an algorithm, the mod function should be applied.

Thus to multiply $39 * 15 \bmod 11$ we first take mods to get

$39 \bmod 11 = 6$ and $15 \bmod 11 = 4$

The multiplication required is now

$6*4 \bmod 11 = 24 \bmod 11 = 2$

Modular Division

What is $5 \div 3 \bmod 11$?

We need to multiply *5* by the ***inverse*** of $3 \bmod 11$

When you multiply a number by its inverse, the answer is 1.

Thus the inverse of 2 is ½ since 2* ½ = 1

The inverse of $3 \bmod 11$ is *4* since $3*4=1 \bmod 11$

Thus $5 \div 3 \bmod 11 = 5*4 \bmod 11 = 9 \bmod 11$

Euclidean algorithm

gcd(a,b) = gcd(b, b mod a)

```
int Euclid(int a, int b) {
   if (b == 0) return a;
   else return Euclid(b, b % a)
}
```

Properties of Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

This set is referred to as the set of **residues**, or **residue classes** (mod n). That is, each integer in Zn represents a residue class.

Properties of Modular Arithmetic

We can label the residue classes (mod n) as:

$[0],[1],[2],\ldots,[n\text{-}1]$, where

$[r] = \{a\text{: } a \text{ is an integer, } a \equiv r \pmod{n}\}$.

E.g.: The residue classes (mod 4) are

$[0] = \{\ldots, -16,-12,-8,-4,0,4,8,12,16, \ldots\}$

$[1] = \{\ldots, -15,-11,-7,-3,1,5,9,13,17, \ldots\}$

$[2] = \{\ldots, -14,-10,-6,-2,2,6,10,14,18, \ldots\}$

$[3] = \{\ldots, -13,-9,-5,-1,3,7,11,15,19, \ldots\}$

Properties of Modular Arithmetic

Property	**Expression**
Cummitative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \text{ x } x) \bmod n = (x \text{ x } w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \text{ x } x) \text{ x } y] \bmod n = [w \text{ x } (x \text{ x } y)] \bmod n$
Distributive Law	$[w \text{ x } (x + y)] \bmod n = [(w \text{ x } x) + (w \text{ x } y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \text{ x } w) \bmod n = w \bmod n$
Additive Inverse (-w)	For each w□ Z_n, there exists a z such that $w + z \equiv 0 \bmod n$

Modular Arithmetic

- A Multiplication Table in Z_n: Summary
  - The numbers that have inverses in Z_n are **relatively prime** to n
    - That is: $gcd(x, n) = 1$
  - The numbers that do NOT have inverses in Z_n have **common prime factors** with n
    - That is: $gcd(x, n) > 1$

Modular Arithmetic

- A Multiplication Table in Z_n: Summary
  - The results have implications for division:
    - Some divisions have no answers
      - $3 * x = 2 \bmod 6$ has no solutions => $2/3$ has no equivalent in Z_6
    - Some division have multiple answers
      - $2 * 2 = 4 \bmod 6$ => $4/2 = 2 \bmod 6$
      - $2 * 5 = 4 \bmod 6$ => $4/2 = 5 \bmod 6$
    - Only numbers that are **relatively prime** to n will be uniquely divisible by all elements of Z_n

Modular Arithmetic

- A Multiplication Table in Z_n: Summary
  - The results have implications for division:
    - Zero divisors exist in some mods:
    - 3 * 2 = 0 mod 6 => 0/3 = 2 and 0/2 = 3 in mod 6
    - 3 * 6 = 0 mod 9 => 0/3 = 6 and 0/6 = 3 in mod 9

Modular Arithmetic

- Finding Inverses in Z_n
  - The numbers that have inverses in Z_n are **relatively prime** to n
  - We can use the Euclidean Algorithm to see if a given "x" is relatively prime to "n"; then we know that an inverse does exist.
  - How can we find the inverse without looking at all the remainders? A problem for large n.

Modular Arithmetic

- Finding Inverses in Z_n
  - The numbers that have inverses in Z_n are **relatively prime** to n
  - We can use the Euclidean Algorithm to see if a given “x” is relatively prime to “n”; then we know that an inverse does exist.
  - How can we find the inverse without looking at all the remainders? A problem for large n.

Modular Arithmetic

- Finding Inverses in Z_n
  - What is the inverse of 15 in mod 26?
  - First use the Euclidean Algorithm to determine if 15 and 26 are relatively prime
    - $26 = 1 * 15 + 11$
    - $15 = 1 * 11 + 4$
    - $11 = 2 * 4 + 3$
    - $4 = 1 * 3 + 1$
    - $3 = 3 * 1 + 0$

Then gcd (26, 15) = 1

Modular Arithmetic

- Finding Inverses in Z_n
  - What is the inverse of 15 in mod 26? Now we now they are relatively prime – so an inverse must exist.
  - We can use the algorithm to work backward to create 1 (the gcd(26, 15)) as a linear combination of 26 and 15:
    - $1 = x * 26 + y * 15$
  - Why would we want to do this?

Modular Arithmetic

- Finding Inverses in Z_n
  - Convert $1 = x * 26 + y * 15$ to mod 26 and we get:
  - 1 mod 26 □ (y * 15) mod 26
  - Then if we find y we find the inverse of 15 in mod 26.
  - So we start from 1 and work backward…

Modular Arithmetic

- $26 = 1 * 15 + 11 \Rightarrow 11 = 26 - (1*15)$
- $15 = 1 * 11 + 4 \Rightarrow 4 = 15 - (1*11)$
- $11 = 2 * 4 + 3 \Rightarrow 3 = 11 - (2*4)$
- $4 = 1 * 3 + 1 \Rightarrow 1 = 4 - (1*3)$

Step 1) $1 = 4 - (1 * 3) = 4 - 3$

Step 2) $1 = 4 - (11 - (2 * 4)) = 3 * 4 - 11$

Step 3) $1 = 3 * (15 - 11) - 11 = 3 * 15 - 4 * 11$

Step 4) $1 = 3 * 15 - 4(26 - (1*15)$

Step 5) $1 = 7 * 15 - 4 * 26 = 105 - 104$ >>check

Modular Arithmetic

- Finding Inverses in Z_n
  - So, what is the inverse of 15 in mod 26?
  - 1 = 7 * 15 – 4 * 26 converts to
  - 1 □ 7 * 15 mod 26
  - □ 7 is the inverse of 15 in mod 26
  - Can you use the same result to show that 11 is its own inverse in mod 15?

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - Formalizing the backward steps we get this formula:
    - $y_0 = 0$
    - $y_1 = 1$
    - $y_i = (y_{i-2} - [y_{i-1} * q_{i-2}])$; $i > 1$
  - Related to the "Magic Box" method

Modular Arithmetic

Step 0	26 = 1 * 15 + 11	$y_0 = 0$
Step 1	15 = 1 * 11 + 4	$y_1 = 1$
Step 2	11 = 2 * 4 + 3	$y_2 = (y_0 - (y_1 * q_0))$ $= 0 - 1 * 1 \bmod 26 = 25$
Step 3	4 = 1 * 3 + 1	$y_3 = (y_1 - (y_2 * q_1))$ $= 1 - 25 * 1 = -24 \bmod 26 = 2$
Step 4	3 = 3 * 1 + 0	$y_4 = (y_2 - (y_3 * q_2))$ $= 25 - 2 * 2 \bmod 26 = 21$
Step 5	Note: q_i is in red above	$y_5 = (y_3 - (y_4 * q_3))$ $= 2 - 21 * 1 = -19 \bmod 26 =$ **7**

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - $y_0 = 0$
  - $y_1 = 1$
  - $y_i = (y_{i-2} - [y_{i-1} * q_{i-2}]);\ i > 1$
- Try it for…
  - 13 mod 22
  - 17 mod 97

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - 22 = 1 * 13 + 9 y[0]=0
  - 13 = 1 * 9 + 4 y[1]=1
  - 9 = 2 * 4 + 1 y[2]=0 - 1 * 1 mod 22 = 21
  - 4 = 4 * 1 + 0 y[3]=1 - 21 * 1 mod 22 = 2
  - Last Step : y[4]=21 - 2 * 2 mod 22 = 17

  - Check: 17 * 13 = 221 = 1 mod 22

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - 97 = 5 * 17 + 12 x[0]=0
  - 17 = 1 * 12 + 5 x[1]=1
  - 12 = 2 * 5 + 2 x[2]=0 - 1 * 5 mod 97 = 92
  - 5 = 2 * 2 + 1 x[3]=1 - 92 * 1 mod 97 = 6
  - 2 = 2 * 1 + 0 x[4]=92 - 6 * 2 mod 97 = 80
  - Last Step: x[5]=6 - 80 * 2 mod 97 = 40

    Check: 40 * 17 = 680 = 1 mod 97

- What is the inverse of 15 in mod 26
- 26= 15*1+11
- 15=11*1+4
- 11=4*2+3
- 4=3*1+1
- 1=4*1-3*1=4*1-(11*1-4*2)*1=4*1-11*1+4*2
- = 4*3-11*1=(15*1-11*1)*3-11*1
- =15*3-11*3-11*1=15*3-11*4
- =15*3-11*4=15*3-(26*1-15*1)*4
- =15*3-26*4+15*4
- =15*7-26*4