ECE297:11 Lecture 3

Mathematical Background: Modular Arithmetic

General Notation

Z – integers

$\exists$ - there exists

$\exists!$ - there exists unique

$\forall$ - for all

$\in$ - belongs to

$\notin$ - does not belong to

Divisibility

$a \mid b$ — *a* divides *b*; *a* is a divisor of *b*

$a \mid b$ iff $\exists\, c \in Z$ such that $b = c \cdot a$

$a \nmid b$ — *a* does not divide *b*; *a* is not a divisor of *b*

Prime vs. composite numbers

An integer $p \geq 2$ is said to be **prime** if its only *positive* divisors are 1 and *p*. Otherwise, p is called **composite**.

Greatest common divisor

Greatest common divisor of *a* and *b*, denoted by **gcd(*a*, *b*)**, is the largest positive integer that divides both *a* and *b*.

$d = \gcd(a, b)$ iff 1) $d \mid a$ and $d \mid b$
2) if $c \mid a$ and $c \mid b$ then $c \le d$

Relatively prime integers

Two integers *a* and *b* are **relatively prime** or **co-prime** if $\gcd(a, b) = 1$

Properties of the greatest common divisor

gcd (a, b) = gcd (a-kb, b)

for any $k \in$ Z

Quotient and remainder

Given integers a and n, $n>0$

$\exists!$ $q, r \in \mathbf{Z}$ such that

$a = q \cdot n + r$ and $0 \leq r < n$

***q* – quotient** $q = \left\lfloor \frac{a}{n} \right\rfloor = a \text{ div } n$

***r* – remainder** $\boldsymbol{r} = a - q \cdot n = a - \left\lfloor \frac{a}{n} \right\rfloor \cdot n =$

(of a divided by n) $= \boldsymbol{a} \textbf{ mod } \boldsymbol{n}$

Integers coungruent modulo n

Two integers a and b are **congruent modulo n**

(**equivalent modulo n**)

written **a ≡ b**

iff

$$a \bmod n = b \bmod n$$

or

$$a = b + kn,\ k \in Z$$

or

$$n \mid a - b$$

Rules of addition, subtraction and multiplication modulo *n*

$$a + b \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$a - b \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$$

$$a \cdot b \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

Laws of modular arithmetic

Regular addition

$a+b = a+c$
iff
$b=c$

Modular addition

$a+b \equiv a+c \pmod{n}$
iff
$b \equiv c \pmod{n}$

Regular multiplication

If $a \cdot b = a \cdot c$
and $a \neq 0$
then
$b = c$

Modular multiplication

If $a \cdot b \equiv a \cdot c$ (mod n)
and gcd $(a, n) = 1$
then
$b \equiv c$ (mod n)

Modular Multiplication: Example

$18 \equiv 42 \pmod{8}$
$6 \cdot 3 \equiv 6 \cdot 7 \pmod{8}$

$3 \not\equiv 7 \pmod{8}$

x	0	1	2	3	4	5	6	7
6 · x mod 8	0	6	4	2	0	6	4	2

x	0	1	2	3	4	5	6	7
5 · x mod 8	0	5	2	7	4	1	6	3

Euclid's Algorithm
for computing gcd(a,b)

i	q_i	r_i
-2		$r_{-2} = max(a, b)$
-1	q_{-1}	$r_{-1} = min(a, b)$
0	q_0	r_0
1	q_1	r_1
…	…	…
t-1	q_{t-1}	$\mathbf{r_{t-1} = gcd(a, b)}$
t		r_t=0

$$\boldsymbol{r_{i+1} = r_{i-1} \bmod r_i}$$

⇕

$$\boldsymbol{q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor}$$

$$\boldsymbol{r_{i+1} = r_{i-1} - q_i \cdot r_i}$$

Euclid's Algorithm
Example: gcd(36, 126)

i	q_i	r_i
-2		$r_{-2} = max(a, b) =126$
-1	$q_{-1} = 3$	$r_{-1} = min(a, b) =36$
0	$q_0 = 2$	r_0 = **18 = gcd(36, 126)**
1	q_1	r_1 = **0**

$$\boldsymbol{r_{i+1} = r_{i-1} \bmod r_i}$$

⇕

$$\boldsymbol{q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor}$$

$$\boldsymbol{r_{i+1} = r_{i-1} - q_i \cdot r_i}$$

Multiplicative inverse modulo *n*

The **multiplicative inverse of *a* modulo *n*** is an **integer [!!!]** x such that

$$a \cdot x \equiv 1 \pmod{n}$$

The multiplicative inverse of *a* modulo *n* is denoted by a^{-1} mod n (in some books $\bar{a}$ or a^*).

According to this notation:

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

Extended Euclid's Algorithm (1)

$$r_i = x_i \cdot a + y_i \cdot n$$

i	q_i	r_i	x_i	y_i
-2		$r_{-2} = n$	$x_{-2}=0$	$y_{-2}=1$
-1	$q_{-1} = \lfloor n/a \rfloor$	$r_{-1} = a$	$x_{-1}=1$	$y_{-1}=0$
0	q_0	r_0	x_0	y_0
1	q_1	r_1	x_1	y_1
…	…	…	…	…
t-1	q_{t-1}	r_{t-1}	x_{t-1}	y_{t-1}
t		$r_t=0$	x_t	y_t

$$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$$

$$r_{i+1} = r_{i-1} - q_i \cdot r_i$$

$$x_{i+1} = x_{i-1} - q_i \cdot x_i$$

$$y_{i+1} = y_{i-1} - q_i \cdot y_i$$

$$r_{t-1} = x_{t-1} \cdot a + y_{t-1} \cdot n$$

Extended Euclid's Algorithm (2)

$$r_{t-1} = x_{t-1} \cdot a + y_{t-1} \cdot n$$

$$r_{t-1} = x_{t-1} \cdot a + y_{t-1} \cdot n \equiv x_{t-1} \cdot a \pmod{n}$$

If $r_{t-1} = \gcd(a, n) = 1$ then

$$x_{t-1} \cdot a \equiv 1 \pmod{n}$$

and as a result

$$x_{t-1} = a^{-1} \bmod n$$

Extended Euclid's Algorithm for computing $z = a^{-1} \bmod n$

i	q_i	r_i	x_i
-2		$r_{-2} = n$	$x_{-2}=0$
-1	$q_{-1} = \lfloor n/a \rfloor$	$r_{-1} = a$	$x_{-1}=1$
0	q_0	r_0	x_0
1	q_1	r_1	x_1
…	…	…	…
t-1	q_{t-1}	$r_{t-1} = 1$	$x_{t-1} = a^{-1} \bmod n$
t		$r_t=0$	$x_t = -n$

$$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$$

$$r_{i+1} = r_{i-1} - q_i \cdot r_i$$

$$x_{i+1} = x_{i-1} - q_i \cdot x_i$$

Note: If $r_{t-1} \neq 1$ the inverse does not exist

Extended Euclid's Algorithm
Example $z = 20^{-1} \bmod 117$

i	q_i	r_i	x_i
-2		$r_{-2} = 117$	$x_{-2} = 0$
-1	$q_{-1} = 5$	$r_{-1} = 20$	$x_{-1} = 1$
0	$q_0 = 1$	$r_0 = 17$	$x_0 = -5$
1	$q_1 = 5$	$r_1 = 3$	$x_1 = 6$
2	$q_2 = 1$	$r_2 = 2$	$x_2 = -35$
3	$q_3 = 2$	$\mathbf{r_3 = 1}$	$\mathbf{x_3 = 41 = 20^{-1} \bmod 117}$
4		$r_4 = 0$	$x_4 = -117$

$$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$$

$$r_{i+1} = r_{i-1} - q_i \cdot r_i$$

$$x_{i+1} = x_{i-1} - q_i \cdot x_i$$

Check: $20 \cdot 41 \bmod 117 = 1$