COMP147 Discrete Maths

Robin Hirsch, 5.07a MPEB, r.hirsch@ucl.ac.uk

February 20, 2019

Group Definition

Let G be a set and $* : G \times G \to G$ be a binary function. $(G, *)$ is a group if

- for all $f, g, h \in G$ $(f * g) * h = f * (g * h)$ (associativity)
- there is $e \in G$ such that for all $g \in G$ we have $g * e = e * g = g$ (identity)
- for all $g \in G$ there is $g' \in G$ such that $g * g' = g' * g = e$ (two sided inverse)

If $(G, *)$ is a group and for all $f, g \in G$ we have $f * g = g * f$ the group is called Abelian or commutative.

Group Examples

- $(\mathbb{Z}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$
- $(S_n, *)$ where $S_n =$ permutations of$\{0, 1, 2, \ldots, n-1\}$ and $*$ is composition of perms.
- $(GL(n, \mathbb{R}), *)$ automorphisms of vector space $\mathbb{R}^n$ with concatenation
- $(\mathbb{Z}/n\mathbb{Z}, +)$, integers modulo n

Lagrange

The size (order) of a subgroup divides into the order of the group.

Lagrange

The size (order) of a subgroup divides into the order of the group.
The order of an element $g \in G$ is smallest positive interger m such that $g^m = \overbrace{g * g * \ldots * g}^{m} = e$.

Lagrange

The size (order) of a subgroup divides into the order of the group. The order of an element $g \in G$ is smallest positive interger m such that $g^m = \overbrace{g * g * \ldots * g}^{m} = e$. By Lagrange, the order of any element of a group divides the order of the group.

Lagrange

The size (order) of a subgroup divides into the order of the group. The order of an element $g \in G$ is smallest positive interger m such that $g^m = \overbrace{g * g * \ldots * g}^{m} = e$. By Lagrange, the order of any element of a group divides the order of the group.
Hence $g^{|G|} = e$.

Additive group modulo n

$(\mathbb{Z}/n\mathbb{Z}), +)$ is an Abelian Group.

Additive group modulo n

$(\mathbb{Z}/n\mathbb{Z}), +)$ is an Abelian Group.
For $0 \leq k < n$ we have $k \equiv_n k + n \equiv \ldots$.
Use representatives $\{0, 1, \ldots, n-1\}$ of the n equivalence classes.

Multiplicative Group Modulo n

- $G_n = \{i : 1 \leq i \leq n,\ i \text{ is coprime to } n\}$.

Multiplicative Group Modulo n

- $G_n = \{i : 1 \leq i \leq n,\ i \text{ is coprime to } n\}$.
- Define $x * y$ as $(x \cdot y)(\bmod n)$.

Multiplicative Group Modulo n

- $G_n = \{i : 1 \leq i \leq n,\ i \text{ is coprime to } n\}$.
- Define $x * y$ as $(x \cdot y) (\bmod n)$.
- Check $g, h \in G_n$ implies $g \cdot h \in G_n$ (closed), and associative and identity laws hold.

Multiplicative Group Modulo n

- $G_n = \{i : 1 \leq i \leq n,\ i \text{ is coprime to } n\}$.
- Define $x * y$ as $(x \cdot y)(\mod n)$.
- Check $g, h \in G_n$ implies $g \cdot h \in G_n$ (closed), and associative and identity laws hold.
- Prove $x \in G_n$ implies there is $g' \in G$ such that the identity is $g \cdot g' = g' \cdot g$ (inverse law).

Multiplicative Group Modulo n

- $G_n = \{i : 1 \leq i \leq n,\ i \text{ is coprime to } n\}$.
- Define $x * y$ as $(x \cdot y)(\mod n)$.
- Check $g, h \in G_n$ implies $g \cdot h \in G_n$ (closed), and associative and identity laws hold.
- Prove $x \in G_n$ implies there is $g' \in G$ such that the identity is $g \cdot g' = g' \cdot g$ (inverse law).
- E.g., $n = 15,\ G_n = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Euler's Totient Function $\phi(n)$

$$\phi(n) = |\{i : 1 \leq i \leq n,\ i \text{ is coprime with } n\}|$$

E.g. $\phi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6.$

$\phi(n)$ — Key Facts

- If m is coprime with n then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$
- If $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_{k_t}^{t}$ where each p_i is prime, then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_t})$$

E.g.

$$\phi(9) = \phi(3^2) = 9 \times (1 - \frac{1}{3}) = 6$$

$$\phi(120) = \phi(2^3 \cdot 3 \cdot 5) = 120 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 32$$

Euler and Lagrange

Recall that $|G_n| = \phi(n)$. If $x \in G_n$ (i.e. $1 \leq x \leq n$ and x is coprime with n) then

$$x^{\phi(n)} = 1 \mod n$$

Hence

$$x^{-1} = x^{\phi(n)-1} \mod n$$

Example

Solve

$$8x = 5 \mod 11$$

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10,$

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10$, so $8^{10} = 1 \mod 11$,

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10$, so $8^{10} = 1 \mod 11$, so $8^9 = 8^{-1} \mod 11$.

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10$, so $8^{10} = 1 \mod 11$, so $8^9 = 8^{-1} \mod 11$.
Powers of 8 modulo 11.

k		$8^k \mod 11$
1		8
2	$64 =_{11}$	9
3	$9 \times 8 =_{11}$	6
4	$9 \times 9 =_{11}$	4
5	$9 \times 6 =_{11}$	-1
9	$4 \times (-1) =_{11}$	7
10	$(-1) \times (-1) =_{11}$	1

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10$, so $8^{10} = 1 \bmod 11$, so $8^9 = 8^{-1} \bmod 11$.
Powers of 8 modulo 11.

k		$8^k \mod 11$
1		8
2	$64 =_{11}$	9
3	$9 \times 8 =_{11}$	6
4	$9 \times 9 =_{11}$	4
5	$9 \times 6 =_{11}$	-1
9	$4 \times (-1) =_{11}$	7
10	$(-1) \times (-1) =_{11}$	1

So $8^{-1} =_{11} 8^9 =_{11} 7$.

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10$, so $8^{10} = 1 \mod 11$, so $8^9 = 8^{-1} \mod 11$.
Powers of 8 modulo 11.

k		$8^k \mod 11$
1		8
2	$64 =_{11}$	9
3	$9 \times 8 =_{11}$	6
4	$9 \times 9 =_{11}$	4
5	$9 \times 6 =_{11}$	-1
9	$4 \times (-1) =_{11}$	7
10	$(-1) \times (-1) =_{11}$	1

So $8^{-1} =_{11} 8^9 =_{11} 7$.
So $x =_{11} 8^{-1} \times 5 =_{11} 7 \times 5 =_{11} 35 =_{11} 2$.

Example

Solve

$$8x = 5 \mod 11$$

$\phi(11) = 10$, so $8^{10} = 1 \mod 11$, so $8^9 = 8^{-1} \mod 11$.
Powers of 8 modulo 11.

k		$8^k \mod 11$
1		8
2	$64 =_{11}$	9
3	$9 \times 8 =_{11}$	6
4	$9 \times 9 =_{11}$	4
5	$9 \times 6 =_{11}$	-1
9	$4 \times (-1) =_{11}$	7
10	$(-1) \times (-1) =_{11}$	1

	8^k
1	8
2	9
3	6
4	4
5	10
6	3
7	2
8	5
9	7

So $8^{-1} =_{11} 8^9 =_{11} 7$.
So $x =_{11} 8^{-1} \times 5 =_{11} 7 \times 5 =_{11} 35 =_{11} 2$.
Solutions are $x = 2 + k \times 11 (k \in \mathbb{Z})$, i.e.
$\{\ldots, -20, -9, 2, 13, 24, \ldots\}$.

Euclidean Algorithm gcd(m, n)

Suppose $m \geq n$ (else swap) and $n \geq 1$

if $m = n$ **then**

  return (n)

else

  return $(GCD(m - n, n))$

Chinese Remainder Theorem

Euclidean Algorithm gcd(m, n), version 2

func gcd(m, n) {

Suppose $m \geq n$ (else swap) and $n \geq 1$

if rem(m, n) $= 0$ **then**

return (n) base case

else

return (gcd(rem(m, n), n))

}

b^{-1} mod a by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

$b^{-1} \bmod a$ by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

- Eventually (some $k \geq 0$) $r_k \neq 0$, $r_{k+1} = 0$ and $r_k = \gcd(a, b)$.

b^{-1} mod a by extended Euclid

$q_i \in \mathbb{Z}^+$

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 \quad \text{one } a & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \quad \text{one } b \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

- Eventually (some $k \geq 0$) $r_k \neq 0$, $r_{k+1} = 0$ and $r_k = \gcd(a, b)$.
- Prove $as_i + bt_i = r_i$ (all i).

b^{-1} mod a by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

- Eventually (some $k \geq 0$) $r_k \neq 0$, $r_{k+1} = 0$ and $r_k = \gcd(a, b)$.
- Prove $as_i + bt_i = r_i$ (all i).
- If $\gcd(a, b) = 1$ then $r_k = 1$.

$b^{-1} \bmod a$ by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

- Eventually (some $k \geq 0$) $r_k \neq 0,\ r_{k+1} = 0$ and $r_k = \gcd(a, b)$.
- Prove $as_i + bt_i = r_i$ (all i).
- If $\gcd(a, b) = 1$ then $r_k = 1$.
- Hence $1 = a.s_k + b.t_k$.

b^{-1} mod a by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

- Eventually (some $k \geq 0$) $r_k \neq 0,\ r_{k+1} = 0$ and $r_k = \gcd(a, b)$.
- Prove $as_i + bt_i = r_i$ (all i).
- If $\gcd(a, b) = 1$ then $r_k = 1$.
- Hence $1 = a.s_k + b.t_k$.
- And $b.t_k = 1 \bmod a$.

b^{-1} mod a by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

where $r_{i+1} < r_i$ (all i).

- Eventually (some $k \geq 0$) $r_k \neq 0,\ r_{k+1} = 0$ and $r_k = \gcd(a, b)$.
- Prove $as_i + bt_i = r_i$ (all i).
- If $\gcd(a, b) = 1$ then $r_k = 1$.
- Hence $1 = a.s_k + b.t_k$.
- And $b.t_k = 1 \bmod a$.
- $b^{-1} = t_k \bmod a$.

gcd(12, 9)

$$r_0 = a \qquad s_0 = 1 \qquad t_0 = 0$$

$$r_1 = b \qquad s_1 = 0 \qquad t_1 = 1$$

$$r_{i+1} = r_{i-1} - q_i r_i \qquad s_{i+1} = s_{i-1} - q_i s_i \qquad t_{i+1} = t_{i-1} - q_i t_i$$

$s_2 = s_0 - 1 \times s_1$

$= 1 - 0 = 1$

$s_3 = s_1 - q_2 s_2$

$= 0 - 3 \times 1 = -3$

$t_2 = t_0 - 1 \times t_1$

$= 0 - 1$

$= -1$

$t_3 = t_1 - q_2 t_2$

$= 1 - 3 \times (-1)$

$= 4.$

$r_0 = 12$

$r_1 = 9$

$r_2 = 12 - \underbrace{1}_{q_1} \times 9 = 3$

$r_3 = 9 - \underbrace{3}_{q_2} \times 3 = 0$

i	r_i	q_i	s_i	t_i
0	12	—	1	0
1	9	1	0	1
2	3	3	1	−1
3	0		−3	4

$3^{-1} \bmod 10$

i	r_i	q_i	s_i	t_i
0	10	–	1	0
1	3	3	0	1
2	1	3	1	−3
3	0		−3	10

So, $1 = 1 \times 10 + (-3) \times 3$
$3^{-1} = (-3) \bmod 10 = 7 \bmod 10.$

Question $5^{-1} \pmod{12}$

i	r_i	q_i	s_i	t_i
0	12		1	0
1	5	2	0	1
2	2	2	1	-2
3	1	2	-2	5
4	0			

$\gcd(12, 5) = 1 = 12 \times (-2) + 5 \times 5$

$5^{-1} \equiv 5 \mod 12$

$\gcd(15, 9)$

i	r_i	q_i	s_i	t_i
0	15		1	0
1	9	1	0	1
2	6	1	1	-1
3	3	2	-1	2
4	0			

Proof by Induction

Base Case: Prove $P(b)$ (often $P(0)$)

Inductive Hypothesis: Assume $P(i)$ is true (some $i \geq b$).

Inductive Step: Prove $P(i+1)$, using IH.

Conclude: For all integers $n \geq b$, $P(n)$.

Induction, Example

$$P(n) = \text{“}2^{n+2} + 3^{2n+1} \text{ is divisible by 7”}$$

- Base case, $P(0)$.
  $$2^2 + 3^1 = 7$$
  which is divisible by 7.

Hypothesis

- I.H. Assume $P(i)$, i.e. assume $2^{i+2} + 3^{2i+1}$ is div. by 7.
- I.S. Prove $P(i+1)$.

Induction Step

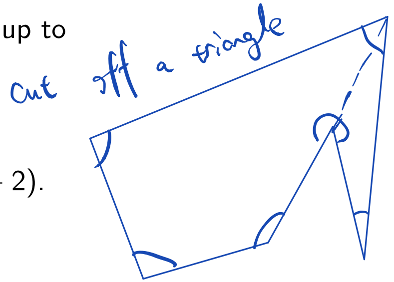
$$\begin{aligned} & 2^{(i+1)+2} + 3^{2(i+1)+1} \\ = \quad & 2 \times 2^{i+2} + 3^2 \times 3^{2i+1} \\ = \quad & 2 \times (2^{i+2} + 3^{2i+1}) + 9 \times 3^{2i+1} - 2 \times 3^{2i+1} \\ = \quad & 2 \times \underbrace{(2^{i+2} + 3^{2i+1})}_{\text{div. by 7, by IH}} + 7 \times 3^{2i+1} \end{aligned}$$

  which is divisible by 7.
- Hence $2^{n+2} + 3^{2n+1}$ is divisible by 7, for all integers $n \geq 0$.

Induction, Second Example

$P(n)$ says 'Int. angles of n-sided polygon sum to $180^\circ \times (n-2)$'

1. Base case $n = 3$, $\checkmark$.
2. IH. Assume interior angle of i-sided polygon always add up to $180^\circ \times (i-2)$ (some $i \geq 3$).
3. IS. Consider $i+1$-sided polygon (draw picture).
   Cut off one triangle to leave i-sided polygon.
   By IH, int. angles of i-sided polygon sum to $180^\circ \times (i-2)$.
   Hence, total int. angles of $i+1$-sided polygon sum to
   $180^\circ \times (i-2) + 180^\circ = 180^\circ \times ((i+1)-2)$.
4. Result follows.



gcd(a, b) by extended Euclid

$$
\begin{aligned}
r_0 &= a & s_0 &= 1 & t_0 &= 0 \\
r_1 &= b & s_1 &= 0 & t_1 &= 1 \\
r_{i+1} &= r_{i-1} - q_i r_i & s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i
\end{aligned}
$$

Claim: $as_i + bt_i = r_i$ and $a.s_{i-1} + b.t_{i-1} = r_{i-1}$, for all $i \geq 1$.

Base case $i = 1$, $a.1 + b.0 = a$. and $a.0 + b.1 = b$ ✓

I.H. For some $i \geq 1$, $as_i + bt_i = r_i$, $a.s_{i-1} + b.t_{i-1} = r_{i-1}$

I.S.

$$
\begin{aligned}
r_{i+1} &= r_{i-1} - q_i r_i \text{ (def. of } r_{i+1}) \\
&= a.s_{i-1} + b.t_{i-1} - q.(a.s_i + b.t_i) \text{ (I.H.)} \\
&= a.(s_{i-1} - q.s_i) + b.(t_{i-1} - q.t_i) \text{ (factorising)} \\
&= a.s_{i+1} + b.t_{i+1} \text{ (def. of } s_{i+1}, t_{i+1})
\end{aligned}
$$

RSA algorithm

- Randomly pick large primes p, q, let $n = p \times q$.
- Calculate $\phi(n) = (p-1) \times (q-1)$. Don't tell anyone.
- Choose e with $1 < e < \phi(n)$ coprime to $\phi(n)$.
- Compute d such that $e \cdot d \equiv_{\phi(n)} 1$.
  inverse of e
- Public key is (n, e).
- Private key is (n, d).
- Message is m where $0 \leq m < n$.
- Encoding: $m \mapsto m^e \mod n$. quite quickly
- Decoding: $c \mapsto c^d \mod n$.

$Dec(Enc(m)) = Dec(m^e \mod n) = (m^e)^d \mod n = m^{e \cdot d} \mod n = m$.

RSA example 1

- $p = 3,\ q = 5,\ n = 15,\ \phi(15) = 8$

$(p-1)\cdot(q-1)$

RSA example 1

- $p = 3, \ q = 5, \ n = 15, \ \phi(15) = 8$
- Let $e = 3$ (coprime to 8)

encoding key (public)

RSA example 1

- $p = 3,\ q = 5,\ n = 15,\ \phi(15) = 8$
- Let $e = 3$ (coprime to 8)
- From $3 \times d = 1 \bmod 8$ get $d = 3$

$3^{-1} \pmod 8$

decrepation key

RSA example 1

- $p = 3,\ q = 5,\ n = 15,\ \phi(15) = 8$
- Let $e = 3$ (coprime to 8)
- From $3 \times d = 1 \bmod 8$ get $d = 3$
- $Enc(m) = m^3 \bmod 15,\ Dec(c) = c^3 \bmod 15.$

e

d.

RSA example 2

- $p = 7,\ q = 11,\ n = 77,\ \phi(77) = 60,$

RSA example 2

- $p = 7, \ q = 11, \ n = 77, \ \phi(77) = 60,$
- pick $e = 13$ (coprtime to 60)

RSA example 2

- $p = 7,\ q = 11,\ n = 77,\ \phi(77) = 60,$
- pick $e = 13$ (coprtime to 60)
- $13 \times d =_{60} 1$ gives $d = 37$

RSA example 2

- $p = 7,\ q = 11,\ n = 77,\ \phi(77) = 60,$
- pick $e = 13$ (coprtime to 60)
- $13 \times d =_{60} 1$ gives $d = 37$
- $Enc(m) = m^{13} \mod 77,\ \ Dec(c) = c^{37} \mod 77$

Proof that $(m^e)^d = m \mod n$

e / d are inverse

If m is coprime to $\phi(n)$ and $e \cdot d = 1 + k \cdot \phi(n)$ then

$$(m^e)^d = m^{ed} = m^{1+k\phi(n)} = m \cdot (m^{\phi(n)})^k = m \cdot 1^k \mod \phi(n) = m \mod \phi(n)$$

m is co prime -> $m^{\phi(n)}$

If m is not coprime to $n = p \times q$, then $m = a \cdot p$ or $m = b \cdot q$, still works.