More Number Theoretic Results

Debdeep Mukhopadhyay

Assistant Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

INDIA -721302

Objectives

- **Euclidean Algorithm**
  - **to compute gcd (Greatest Common Divisor)**
  - **to compute multiplicative inverse**
- **Chinese Remainder Theorem (CRT)**
  - **expressing the whole in parts**
- **Cyclic groups and a test for primitive-ness**

Previous Results Discussed

- **Modular Arithmetic**
- **The set of residues modulo n, that are relatively prime to n is denoted by Z_n^*.**
- **Z_n^* forms a multiplicative group under multiplication.**
- **Any element inside Z_n^* has a multiplicative inverse.**
- **Z_n^* is closed under multiplication.**

The Euclidean Algorithm

EUCLIDEAN ALGORITHM(a, b)

$r_0 \leftarrow a$
$r_1 \leftarrow b$
$m \leftarrow 1$
while $r_m \neq 0$
do $\begin{cases} q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m+1 \end{cases}$
$m \leftarrow m - 1$
return $(q_1, \ldots, q_m; r_m)$
comment: $r_m = \gcd(a, b)$

Proof of Correctness

- $gcd(a,b)=gcd(r_0,r_1)=gcd(q_1r_1+r_2,r_1)= gcd(r_1,r_2)=gcd(r_2,r_3)=\ldots=gcd(r_{m-1},r_m)=r_m$
- **Thus, the EA algorithm can be used to compute the gcd of two positive integers**
  - **Also to check whether an integer modulo n has a multiplicative inverse.**
- **But how can we compute the inverse?**

Example

- **Compute the 28^{-1} mod 75**

  75=2x28+19

  28=1x19+9

  19=2x9+1

  9=9x1
- **So, gcd(28,75)=1. So, what is the inverse?**
- **Can you express the gcd as a linear combination of 28 and 75?**

Example

- 19=75-2x28
- 9=28-19=28-(75-2x28)=-75+3x28
- 1=19-2x9=(75-2x28)-2x(-75+3x28)= 3x75-8x28
- Thus, gcd(28,75)=1=3x75-8x28.
- So, what is 28^{-1} mod 75?

  Answer is -8 mod 75 = 67

So, what is the lesson?

- All the remainders generated by the EA algorithm can be expressed as a linear combination of the +ve integers a and b.
- And the expression is unique.
- The extended EA algorithm generates/computes this linear combination in a systematic fashion

- **Define (t_0, t_1, …,t_m) and (s_0, s_1, …,s_m)**

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases} \qquad s_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } j = 1 \\ s_{j-2} - q_{j-1}s_{j-1} & \text{if } j \geq 2. \end{cases}$$

For $0 \leq j \leq m,$ we have that $r_j = s_j r_0 + t_j r_1,$ where the r_j's are as defined in the Euclidean Algorithm, and the s_j's and the t_j's are as defined in the recurrence.

EXTENDED EUCLIDEAN ALGORITHM(a, b)

```
a0 ← a
b0 ← b
t0 ← 0
t ← 1
s0 ← 1
s ← 0
q ← ⌊a0/b0⌋
r ← a0 − q b0
while r > 0
     do { temp ← t0 − q t
          t0 ← t
          t ← temp
          temp ← s0 − q s
          s0 ← s
          s ← temp
          a0 ← b0
          b0 ← r
          q ← ⌊a0/b0⌋
          r ← a0 − q b0
r ← b0
return (r, s, t)
comment: r = gcd(a, b) and sa + tb = r
```

The Extended EA algorithm

Example

i	r_i	q_i	s_i	t_i
0	75		1	0
1	28	2	0	1
2	19	1	1	-2
3	9	2	-1	3
4	1	9	3	-8

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases}$$

$$s_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } j = 1 \\ s_{j-2} - q_{j-1}s_{j-1} & \text{if } j \geq 2. \end{cases}$$

1=3x75+(-8)x28
Thus, taking modulo 75, 28^{-1} mod 75=-8=67

Improvement

Note that we do not require the s_i's and can take a modulo 75 each time while computing the t_i's. This will make the algorithm efficient.

i	r_i	q_i		t_i
0	75			0
1	28	2		1
2	19	1		-2
3	9	2		3
4	1	9		-8

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases}$$

take a modulo operation with a=75.

The answer is -8 mod 75 = 67…

The Chinese Remainder Theorem (CRT)

- It solves a system of congruences.
- Suppose $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers.
- System of congruences:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\vdots \\
x &\equiv a_r \pmod{m_r}.
\end{aligned}
$$

CRT asserts that there is a unique solution to this system

Example

- $x \equiv 3 \bmod 5$
- $x \equiv 1 \bmod 3$
- $x \equiv\ ? \bmod 15$
- You can verify that the only answer is 13 mod 15. The first thing to explain why there is only one solution.

Uniqueness

- **X(x)=(x mod 5, x mod 3)**

$$\begin{array}{rclrclrcl}
\chi(0) & = & (0,0) & \chi(1) & = & (1,1) & \chi(2) & = & (2,2) \\
\chi(3) & = & (3,0) & \chi(4) & = & (4,1) & \chi(5) & = & (0,2) \\
\chi(6) & = & (1,0) & \chi(7) & = & (2,1) & \chi(8) & = & (3,2) \\
\chi(9) & = & (4,0) & \chi(10) & = & (0,1) & \chi(11) & = & (1,2) \\
\chi(12) & = & (2,0) & \chi(13) & = & (3,1) & \chi(14) & = & (4,2).
\end{array}$$

Note that the mapping is bijective…

Example

- **M=5x3=15**
- **M_1=15/5=3, 3^{-1}mod 5=2**
- **M_2=15/3=5, 5^{-1}mod 3=2**
- **x=(3x3x2+1x5x2)mod 15**
  =28 mod 15=13

What is the principle?

Generalization

- We shall present a constructive proof
- In fact, CRT gives an explicit formula for X^{-1} mod M, where $M=m_1m_2\ldots m_r$
- Compute, $M_i=M/m_i$, for $1 \le i \le r$
  - Thus, $\gcd(m_i, M_i)=1$
- Compute $y_i=M_i^{-1} \bmod m_i$

- Thus, $M_iy_i \equiv 1 \pmod{m_i}$, for $1 \le i \le r$
- Define,

$$\rho(a_1, \ldots, a_r) = \sum_{i=1}^{r} a_i M_i y_i \bmod M.$$

- Compute, $\rho \bmod m_i \equiv a_i$ [This is because $M_iy_i \equiv 1 \pmod{m_i}$ and $M_iy_i \equiv 0 \pmod{m_j}$]
- Since, the domain and range have the same cardinality and the function X() is onto, by our previous discussion the function is bijective. Thus the solution is unique modulo M.

The CRT Theorem

(Chinese remainder theorem) *Suppose $m_1, \ldots, m_r$ are pairwise relatively prime positive integers, and suppose $a_1, \ldots, a_r$ are integers. Then the system of r congruences $x \equiv a_i \pmod{m_i}$ $(1 \le i \le r)$ has a unique solution modulo $M = m_1 \times \cdots \times m_r$, which is given by*

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \bmod m_i$, for $1 \le i \le r$.

Other Useful Facts

- **Suppose G is a multiplicative group of order n, and gεG. Then the order of g divides n.**
- **Corollary 1: If $b \varepsilon Z_n^*$, then $b^{\Phi(n)} \equiv 1$ (mod n)**
- **Corollary 2: Suppose p is prime and $b \varepsilon Z_p$. Then $b^p \equiv b$ (mod p)**

Cyclic Group

- If p is prime, then Z_p^* is a group of order p-1 and any element in Z_p^* has an order which divides (p-1).
- In fact, if p is prime, then there exists at least one element in Z_p^* which has order equal to p-1.
  - this is called cyclic group…

Primitive Element

- If p is prime, then Z_p^* is a cyclic group.
- Any element α having order p-1 mod p is called a primitive element. Thus α is a primitive element iff:

$$\{\alpha^i : 0 \le i \le p-2\} = \mathbb{Z}_p^*$$

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

- **n=19, There are 6 primitive elements.**
- **Note the order of each element in Z_{19}^*.**
- **Is there a relation?**

Order of any element

- **Any element β in Z_p^* (where p is prime) can be written uniquely in the form $\beta=\alpha^i$, where α is a primitive element and $0 \le i \le p-2$.**
- **The order of β is:**

$$\frac{p-1}{\gcd(p-1,i)}$$

- **β is itself primitive iff gcd(p-1,i)=1. Hence, what is the number of primitive elements modulo p?**

Example

- p=13
- Thus Φ(13-1)= Φ(12)= Φ(3x2^2)=12(1-1/3)(1-1/2)=12x(2/3)x(1/2)=4.
- Question: Is 2 a primitive element of Z_{13}^*?
  - generate all the (p-1) powers of 2.
  - lengthy process if p is large.

Theorem

THEOREM 5.8 *Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p^*$. Then α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes q such that $q \mid (p-1)$.*

- Proved in the class

References

- D. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC
- W. Stallings, "Cryptography and Network Security"

Next Days Topic

- The RSA Cryptosystem