

Numerical Algorithms

x	0	1	2	3	4	5	6	7	8	9
x^{-1}		1		7				3		9

Outline

- ◆ Divisibility and primes
- ◆ Modular arithmetic
- ◆ Euclid's GCD algorithm
- ◆ Multiplicative inverses
- ◆ Powers
- ◆ Fermat's little theorem
- ◆ Euler's theorem

Facts About Numbers

◆ Prime number p :

- p is an integer
- $p \geq 2$
- The only divisors of p are 1 and p

◆ Examples

- 2, 7, 19 are primes
- -3, 1, 6 are not primes

◆ Prime decomposition of a positive integer n :

$$n = p_1^{e_1} \times \dots \times p_k^{e_k}$$

◆ Example:

- $200 = 2^3 \times 5^2$

Fundamental Theorem of Arithmetic

The prime decomposition of a positive integer is unique

Greatest Common Divisor

- ◆ The greatest common divisor (GCD) of two positive integers a and b , denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b
- ◆ The above definition is extended to arbitrary integers

- ◆ Examples:

$$\gcd(18, 30) = 6$$

$$\gcd(0, 20) = 20$$

$$\gcd(-21, 49) = 7$$

- ◆ Two integers a and b are said to be relatively prime if

$$\gcd(a, b) = 1$$

- ◆ Example:

- Integers 15 and 28 are relatively prime

Modular Arithmetic

- ◆ Modulo operator for a positive integer n

$$r = a \bmod n$$

equivalent to

$$a = r + kn$$

and

$$r = a - \lfloor a/n \rfloor n$$

- ◆ Example:

$$\begin{array}{lll} 29 \bmod 13 = 3 & 13 \bmod 13 = 0 & -1 \bmod 13 = 12 \\ 29 = 3 + 2 \times 13 & 13 = 0 + 1 \times 13 & 12 = -1 + 1 \times 13 \end{array}$$

- ◆ Modulo and GCD:

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

- ◆ Example:

$$\gcd(21, 12) = 3 \quad \gcd(12, 21 \bmod 12) = \gcd(6, 9) = 3$$

Euclid's GCD Algorithm

- ◆ Euclid's algorithm for computing the GCD repeatedly applies the formula

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

- ◆ Example

- $\gcd(412, 260) = 4$

Algorithm *EuclidGCD(a, b)*

Input integers *a* and *b*

Output $\gcd(a, b)$

if $b = 0$

return *a*

else

return *EuclidGCD(b, a mod b)*

<i>a</i>	412	260	152	108	44	20	4
<i>b</i>	260	152	108	44	20	4	0

Analysis

- ◆ Let a_i and b_i be the arguments of the i -th recursive call of algorithm *EuclidGCD*

- ◆ We have

$$a_{i+2} = b_{i+1} = a_i \bmod a_{i+1} < a_{i+1}$$

- ◆ Sequence a_1, a_2, \dots, a_n decreases exponentially, namely

$$a_{i+2} \leq \frac{1}{2} a_i \text{ for } i > 1$$

Case 1 $a_{i+1} \leq \frac{1}{2} a_i$ $a_{i+2} < a_{i+1} \leq \frac{1}{2} a_i$

Case 2 $a_{i+1} > \frac{1}{2} a_i$ $a_{i+2} = a_i \bmod a_{i+1} = a_i - a_{i+1} \leq \frac{1}{2} a_i$

- ◆ Thus, the maximum number of recursive calls of algorithm *EuclidGCD(a, b)* is

$$1 + 2 \log \max(a, b)$$

- ◆ Algorithm *EuclidGCD(a, b)* executes $O(\log \max(a, b))$ arithmetic operations

Multiplicative Inverses (1)

- ◆ The residues modulo a positive integer n are the set

$$\mathbb{Z}_n = \{0, 1, 2, \dots, (n - 1)\}$$

- ◆ Let x and y be two elements of \mathbb{Z}_n such that

$$xy \bmod n = 1$$

We say that y is the multiplicative inverse of x in \mathbb{Z}_n and we write $y = x^{-1}$

- ◆ Example:

- Multiplicative inverses of the residues modulo 11

x	0	1	2	3	4	5	6	7	8	9	10
x^{-1}		1	6	4	3	9	2	8	7	5	10

Multiplicative Inverses (2)

Theorem

An element x of \mathbb{Z}_n has a multiplicative inverse if and only if x and n are relatively prime

◆ Example

- The elements of \mathbb{Z}_{10} with a multiplicative inverse are 1, 3, 5, 7

Corollary

If p is prime, every nonzero residue in \mathbb{Z}_p has a multiplicative inverse

Theorem

A variation of Euclid's GCD algorithm computes the multiplicative inverse of an element x of \mathbb{Z}_n or determines that it does not exist

x	0	1	2	3	4	5	6	7	8	9
x^{-1}		1		7				3		9

Powers

- ◆ Let p be a prime
- ◆ The sequences of successive powers of the elements of \mathbb{Z}_p exhibit repeating subsequences
- ◆ The sizes of the repeating subsequences and the number of their repetitions are the divisors of $p - 1$
- ◆ Example ($p = 7$)

x	x^2	x^3	x^4	x^5	x^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Fermat's Little Theorem

Theorem

Let p be a prime. For each nonzero residue x of \mathbb{Z}_p , we have $x^{p-1} \bmod p = 1$

◆ Example ($p = 5$):

$$1^4 \bmod 5 = 1$$

$$2^4 \bmod 5 = 16 \bmod 5 = 1$$

$$3^4 \bmod 5 = 81 \bmod 5 = 1$$

$$4^4 \bmod 5 = 256 \bmod 5 = 1$$

Corollary

Let p be a prime. For each nonzero residue x of \mathbb{Z}_p , the multiplicative inverse of x is $x^{p-2} \bmod p$

Proof

$$x(x^{p-2} \bmod p) \bmod p = xx^{p-2} \bmod p = x^{p-1} \bmod p = 1$$

Euler's Theorem

- ◆ The multiplicative group for Z_n , denoted with Z_n^* , is the subset of elements of Z_n relatively prime with n
- ◆ The totient function of n , denoted with $\phi(n)$, is the size of Z_n^*
- ◆ Example

$$Z_{10}^* = \{1, 3, 7, 9\} \quad \phi(10) = 4$$

- ◆ If p is prime, we have

$$Z_p^* = \{1, 2, \dots, (p-1)\} \quad \phi(p) = p-1$$

Theorem

For each element x of Z_n^* , we have $x^{\phi(n)} \bmod n = 1$

- ◆ Example ($n = 10$)

$$3^{\phi(10)} \bmod 10 = 3^4 \bmod 10 = 81 \bmod 10 = 1$$

$$7^{\phi(10)} \bmod 10 = 7^4 \bmod 10 = 2401 \bmod 10 = 1$$

$$9^{\phi(10)} \bmod 10 = 9^4 \bmod 10 = 6561 \bmod 10 = 1$$