

Computational Number Theory I

Zeph Grunschlag

Modular Inverses

INPUT: modular base $n > 1$, a any integer

OUTPUT:

- FAIL if a not invertible mod n
- $a^{-1} \bmod n$ otherwise

ModularInverse(a, n) {

(g, s, t) = ExtendedGCD(a, n)

if $g > 1$, return FAIL

return $s \bmod n$

}

3

Extended Euclidean Algorithm

INPUT: non-negative integers (x, y) not both 0

OUTPUT: integers (g, s, t) with $g = \gcd(x, y)$
and s, t satisfying $sx + ty = g$

(g, s, t) ExtendedGCD(x, y) {

if ($y == 0$) return ($x, 1, 1$);

(g, s, t) = ExtendedGCD($y, x \bmod y$);

return ($g, t, s - t \begin{bmatrix} x \\ y \end{bmatrix}$);

}

2

Lagrange, Euler and Fermat

DEF: Let g be an element of a finite group G .

The **order** of g “ $o(g)$ ” is the smallest positive number n such that $g^n = 1$.

Lagrange’s THM: Let $N = |G|$. The order of any element is a divisor of N . I.e. for all $g, o(g) \mid N$.

COR1 - Euler’s THM: Let $G = \mathbb{Z}_n^*$. If m is rel. prime to n , then $o(m) \mid \phi(n)$ so $m^{\phi(n)} \bmod n = 1$

COR2 - Fermat’s little THM: Let $G = \mathbb{Z}_p^*$ with p prime. Then for all $m, m^p \equiv_p m$. If in addition $\gcd(m, p) = 1$ then $m^{p-1} \bmod p = 1$.

4

Primitives Revisited

Let G be a group of cardinality N .

RECALL: g is **primitive** in G iff $o(g) = N$.

Equivalently: all elements are powers of g . G is called **cyclic** if it has a primitive element.

TESTING LEMMA: Let p_1, p_2, \dots, p_t be the prime factors of $N = |G|$. Then an element g is primitive iff: $\forall p_i, g^{\frac{N}{p_i}} \neq 1$.

LEMMA: Suppose g is primitive in G . Then g^i is primitive iff $\gcd(i, N) = 1$.

Theorem: The multiplicative ring of any finite field is cyclic. In particular \mathbb{Z}_p^* is cyclic.

5

Validity of Primitivity Algorithm

LEMMA: If G is cyclic with cardinality factoring into $N = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ then the probability of success is: $\frac{\phi(N)}{N} = \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right)$

COR1: If $G = \mathbb{Z}_m^*$ is cyclic, then the probability of success is $\frac{\phi(\phi(m))}{\phi(m)}$

COR2: If $G = \mathbb{Z}_p^*$ with $p = 2q + 1$ and p, q prime: the probability of success is $\frac{1}{2} - \frac{1}{p-1}$

7

Primitive Generator

A Las Vegas, group theoretic algorithm.

INPUT: cardinality N , prime factors of N

OUTPUT: primitive element g of G (or "FAIL")

EXTERNAL: black boxes for G -exponentiation and for picking elements of G at random

```
GeneratePrimitive(  $N, p_1, p_2, \dots, p_t$  ){
   $g = \text{RandomElementIn}G$ 
  for each prime factor  $p_i$  of  $N$  {
    if ( $g^{\frac{N}{p_i}} == 1$ ) return FAIL
  }
  return  $g$ 
}
```

6

Group Exponentiation

INPUT: Element $g \in G$, exponent $e \geq 0$

OUTPUT: g^e

EXTERNAL: Black box for multiplication

FastExponentiation(g, e){

$x_k x_{k-1} \dots x_0 = \text{Binary}(n)$

$a = g, b = 1$

for $i = 0$ to k {

if $x_i == 1, \{b = a \cdot b\}$ // using black-box

$a = a \cdot a$ // using black-box

}

return b

}

8

Taking e'th Roots For Rel-Prime Exponents

Suppose:

- $a \in \mathbb{Z}_n^*$
- $b = a^e \pmod n$
- and e is invertible mod $\phi(n)$

Then: $a = b^{e^{-1} \pmod{\phi(n)}} \pmod n$

9

Quadratic Residues and Legendre Symbol

DEF: A **quadratic residue** mod p is an integer with a square root in \mathbb{Z}_p^* . Legendre symbol:

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & \text{if } n \pmod p = 0 \\ 1, & \text{else if } \exists m, m^2 \equiv_p n \\ -1, & \text{else} \end{cases}$$

Notation $QR(p) = \{\text{quadratic residues mod } p\}$

LEMMA: For odd p and g primitive $\left(\frac{g^i}{p}\right) = -1^i$.
I.e. g^i is a quadratic residue iff i is even.

10

Square Roots mod- p

Following gives simple Quadratic Residue Test:

COR: $\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \pmod p$

LEMMA1: Let p be an odd prime. For each quadratic residue $n \pmod p$ there are exactly two square roots of n of the form $\pm r$.

LEMMA2: Suppose also that $p \pmod 4 = 3$. If n is a quadratic residue mod p , then a square root of n is obtained by the formula

$$r = n^{\frac{p+1}{4}} \pmod p$$

11