3.5 Computing square roots in $\mathbb{Z}_n$

박태환

2017.09.18

I. 관련 알고리즘 소개

1. Extended Euclidean Algorithm
2. Computing multiplicative inverses in $\mathbb{Z}_n$
3. Repeated square-and-multiply algorithm for exp. In $\mathbb{Z}_n$
4. Jacobi symbol (and Legendre symbol) Computation
5. Repeated square-and-multiply algorithm for exp. In $\mathbb{F}_{p^m}$

II. Computing square roots in $\mathbb{Z}_n$

1. n: Prime
2. n: composite

- **Extended Euclidean Algorithm**
  - Extended Euclidean Algorithm : can calculated (1) d = gcd(a, b) and (2) integer x and y satisfying ax + by = d
  - Running time: O($(\lg n)^2$)
  - Ex) a = 4864, b = 3458

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	4864	3458	1	0	0	1
1	1406	1	−1	3458	1406	0	1	1	−1
2	646	−2	3	1406	646	1	−2	−1	3
2	114	5	−7	646	114	−2	5	3	−7
5	76	−27	38	114	76	5	−27	−7	38
1	38	32	−45	76	38	−27	32	38	−45
2	0	−91	128	38	0	32	−91	−45	128

Algorithm Extended Euclidean algorithm

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: $d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$, and return(d,x,y).
2. Set $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
   3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, and return(d,x,y).

- Computing multiplicative inverses in $\mathbb{Z}_n$
  - Extended Euclidean Algorithm 활용
  - Multiplicative inverse 계산
  - 앞선 예제의 경우, d > 1, multiplicative inverse does not exist
  - Ex) a = 3, b = 5, d = gcd(3, 5) = 1, n = 10
    3*(7) + 5*(2) = 1 (mod 10), a^{-1} = 7
    3*(7) = 21 = 1 (mod 10)

Algorithm Computing multiplicative inverses in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$.
OUTPUT: $a^{-1} \bmod n$, provided that it exists.

1. Use the extended Euclidean algorithm (Algorithm 2.107) to find integers x and y such that $ax + ny = d$, where $d = \gcd(a, n)$.
2. If $d > 1$, then $a^{-1} \bmod n$ does not exist. Otherwise, return(x).

- **Repeated square-and-multiply algorithm for exp. in $\mathbb{Z}_n$**

$$a^k = \prod_{i=0}^{t} a^{k_i 2^i} = (a^{2^0})^{k_0} (a^{2^1})^{k_1} \cdots (a^{2^t})^{k_t}$$

  - **Ex)** $5^{596}\ mod\ 1234 = 1013$

i	0	1	2	3	4	5	6	7	8	9
k_i	0	0	1	0	1	0	1	0	0	1
A	5	25	625	681	1011	369	421	779	947	925
b	1	1	625	625	67	67	1059	1059	1059	1013

Algorithm Repeated square-and-multiply algorithm for exponentiation in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$, and integer $0 \le k < n$ whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$.
OUTPUT: $a^k \bmod n$.

1. Set $b \leftarrow 1$. If $k = 0$ then return(b).
2. Set $A \leftarrow a$.
3. If $k_0 = 1$ then set $b \leftarrow a$.
4. For i from 1 to t do the following:
   - 4.1 Set $A \leftarrow A^2 \bmod n$.
   - 4.2 If $k_i = 1$ then set $b \leftarrow A \cdot b \bmod n$.
5. Return(b).

- **Jacobi symbol (and Legendre symbol) Computation**
  - **Legendre symbol: tool for keeping track of whether or not an integer a is a quadratic residue modulo a prime *p***

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if } a \in Q_p, \\ -1, & \text{if } a \in \overline{Q}_p. \end{cases}$$

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$. In particular, $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Hence $-1 \in Q_p$ if $p \equiv 1 \pmod 4$, and $-1 \in \overline{Q}_p$ if $p \equiv 3 \pmod 4$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Hence if $a \in \mathbb{Z}_p^*$, then $\left(\frac{a^2}{p}\right) = 1$.

(iii) If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(iv) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Hence $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1$ or $7 \pmod 8$, and $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3$ or $5 \pmod 8$.

(v) (*law of quadratic reciprocity*) If q is an odd prime distinct from p, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

- **Jacobi symbol (and Legendre symbol) Computation**
  - **Jacobi symbol** $\left(\frac{a}{n}\right)$ **,** $n \geq 3$**, *be odd with prime factorization*** $n = {p_1}^{e_1}{p_2}^{e_2} \dots {p_k}^{e_k}$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_k}\right)^{e_k}$$

  - ***If n is prime, the Jacobi symbol is just the Legendre symbol***
  - $m \geq 3, n \geq 3$ ***be odd integers and*** $a, b \in \mathbb{Z}$***, the Jacobi symbol has the following properties***

(i) $\left(\frac{a}{n}\right) = 0, 1,$ or -1. Moreover, $\left(\frac{a}{n}\right) = 0$ if and only if $\gcd(a, n) \neq 1$.

(ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. Hence if $a \in \mathbb{Z}_n^*$, then $\left(\frac{a^2}{n}\right) = 1$.

(iii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

(iv) If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(v) $\left(\frac{1}{n}\right) = 1$.

(vi) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$. Hence $\left(\frac{-1}{n}\right) = 1$ if $n \equiv 1 \pmod{4}$, and $\left(\frac{-1}{n}\right) = -1$ if $n \equiv 3 \pmod{4}$.

(vii) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$. Hence $\left(\frac{2}{n}\right) = 1$ if $n \equiv 1$ or $7 \pmod{8}$, and $\left(\frac{2}{n}\right) = -1$ if $n \equiv 3$ or $5 \pmod{8}$.

(viii) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$. In other words, $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ unless both m and n are congruent to 3 modulo 4, in which case $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

- **Jacobi symbol (and Legendre symbol) Computation**
  - **If n is odd and $a = 2^e a_1$, a_1 is odd, then**

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n \bmod a_1}{a_1}\right)(-1)^{(a_1-1)(n-1)/4}.$$

Algorithm Jacobi symbol (and Legendre symbol) computation

JACOBI(a,n)
INPUT: an odd integer $n \geq 3$, and an integer a, $0 \leq a < n$.
OUTPUT: the Jacobi symbol $\left(\frac{a}{n}\right)$ (and hence the Legendre symbol when n is prime).

1. If $a = 0$ then return(0).
2. If $a = 1$ then return(1).
3. Write $a = 2^e a_1$, where a_1 is odd.
4. If e is even then set $s \leftarrow 1$. Otherwise set $s \leftarrow 1$ if $n \equiv 1$ or $7 \pmod 8$, or set $s \leftarrow -1$ if $n \equiv 3$ or $5 \pmod 8$.
5. If $n \equiv 3 \pmod 4$ and $a_1 \equiv 3 \pmod 4$ then set $s \leftarrow -s$.
6. Set $n_1 \leftarrow n \bmod a_1$.
7. If $a_1 = 1$ then return(s); otherwise return($s \cdot$ JACOBI(n_1,a_1)).

- Jacobi symbol (and Legendre symbol) Computation
  - Ex) a = 158, n = 235

$$\begin{aligned}\left(\frac{158}{235}\right) &= \left(\frac{2}{235}\right)\left(\frac{79}{235}\right) = (-1)\left(\frac{235}{79}\right)(-1)^{78\cdot 234/4} = \left(\frac{77}{79}\right)\\ &= \left(\frac{79}{77}\right)(-1)^{76\cdot 78/4} = \left(\frac{2}{77}\right) = -1.\end{aligned}$$

  - Ex) quadratic residues and non-residues

$\left(\frac{5}{21}\right) = 1$ but $5 \notin Q_{21}$. $\quad Q_{21} = \{1, 4, 16\}$

$a \in \mathbb{Z}_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
$a^2 \bmod n$	1	4	16	4	1	16	16	1	4	16	4	1
$\left(\frac{a}{3}\right)$	1	−1	1	−1	−1	1	−1	1	1	−1	1	−1
$\left(\frac{a}{7}\right)$	1	1	1	−1	1	−1	1	−1	1	−1	−1	−1
$\left(\frac{a}{21}\right)$	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1

- **Repeated square-and-multiply algorithm for exp. in $\mathbb{F}_{p^m}$**

Algorithm Repeated square-and-multiply algorithm for exponentiation in $\mathbb{F}_{p^m}$

INPUT: $g(x) \in \mathbb{F}_{p^m}$ and an integer $0 \leq k < p^m - 1$ whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$. (The field $\mathbb{F}_{p^m}$ is represented as $\mathbb{Z}_p[x]/(f(x))$, where $f(x) \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree m over $\mathbb{Z}_p$.)
OUTPUT: $g(x)^k \bmod f(x)$.

1. Set $s(x) \leftarrow 1$. If $k = 0$ then return($s(x)$).
2. Set $G(x) \leftarrow g(x)$.
3. If $k_0 = 1$ then set $s(x) \leftarrow g(x)$.
4. For i from 1 to t do the following:
   - 4.1 Set $G(x) \leftarrow G(x)^2 \bmod f(x)$.
   - 4.2 If $k_i = 1$ then set $s(x) \leftarrow G(x) \cdot s(x) \bmod f(x)$.
5. Return($s(x)$).

Computing square roots in $\mathbb{Z}_n$

- n: Prime(1/5)
  - Algorithm 2.149: Jacobi symbol computation
  - Algorithm 2.142: Computing multiplicative inverse
  - Algorithm 2.143: Repeated square-and-multiply algorithm for exp. in $\mathbb{Z}_n$

Algorithm Finding square roots modulo a prime p

INPUT: an odd prime p and an integer a, $1 \leq a \leq p-1$.
OUTPUT: the two square roots of a modulo p, provided a is a quadratic residue modulo p.

1. Compute the Legendre symbol $\left(\frac{a}{p}\right)$ using Algorithm 2.149. If $\left(\frac{a}{p}\right) = -1$ then return(a does not have a square root modulo p) and terminate.
2. Select integers b, $1 \leq b \leq p-1$, at random until one is found with $\left(\frac{b}{p}\right) = -1$. ($b$ is a quadratic non-residue modulo p.)
3. By repeated division by 2, write $p - 1 = 2^s t$, where t is odd.
4. Compute $a^{-1} \bmod p$ by the extended Euclidean algorithm (Algorithm 2.142).
5. Set $c \leftarrow b^t \bmod p$ and $r \leftarrow a^{(t+1)/2} \bmod p$ (Algorithm 2.143).
6. For i from 1 to $s-1$ do the following:
   - 6.1 Compute $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \bmod p$.
   - 6.2 If $d \equiv -1 \pmod{p}$ then set $r \leftarrow r \cdot c \bmod p$.
   - 6.3 Set $c \leftarrow c^2 \bmod p$.
7. Return($r, -r$).

- **n: Prime(2/5)**
  - **Ex) p = 5, a = 4, assume that b = 3(quadratic non-residue),** $a^{-1} = 4$

$$p - 1 = 2^s t = 5 - 1 = 2^2 1,$$
$$s = 2, t = 1$$
$$c = b^t \ mod\ p = \ 3^1 \ mod\ 5 \ \equiv 3\ mod\ 5$$
$$r = a^{(t+1)/2} \ mod\ p = \ 4^{(1+1)/2} \ mod\ 5 \ \equiv 4\ mod\ 5$$
$$from\ i = 0\ to\ i = s - 1$$
$$d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \ mod\ p = (4^2 \cdot 4)^{2^{2-1-1}} \ mod\ 5 = 4\ mod\ 5 \ \equiv -1\ mod\ 5$$
$$if\ d = -1\ mod\ 5$$
$$r = r \cdot c\ mod\ p = 4 \cdot 3\ mod\ 5 = 12\ mod\ 5 \ \equiv 2\ (mod\ 5)$$

- **n: Prime(3/5)**
  - **Ex)** $p = 7 \equiv 3(mod\ 4), \mathrm{a} = 4$

$$
\begin{aligned}
r &= a^{(p+1)/4}\ mod\ p \\
&= 4^{(7+1)/4}\ mod\ 7 \\
&= 4^2\ mod\ 7 \\
&\equiv 2\ (mod\ 7)
\end{aligned}
$$

Algorithm Finding square roots modulo a prime p where $p \equiv 3 \pmod 4$

INPUT: an odd prime p where $p \equiv 3 \pmod 4$, and a square $a \in Q_p$.
OUTPUT: the two square roots of a modulo p.

1. Compute $r = a^{(p+1)/4} \bmod p$ (Algorithm 2.143).
2. Return$(r, -r)$.

- **n: Prime(4/5)**
  - **Ex 1)** $p = 13 \equiv 5(mod\ 8), \mathrm{a} = 3$

$$\mathrm{d} = a^{(p-1)/4}\ mod\ p$$
$$= 3^{(13-1)/4}\ mod\ 13$$
$$= 3^3\ mod\ 13\ \equiv 1\ (mod\ 13)$$
$$\mathrm{r} = a^{(p+3)/8}\ mod\ p$$
$$= 3^{(13+3)/8}\ mod\ 13$$
$$= 3^2\ mod\ 13\ \equiv 9\ (mod\ 13)$$
$$r^2 = 9^2\ mod\ 13\ \equiv 3\ (mod\ 13)$$

  - **Ex 2)** $p = 13 \equiv 5(mod\ 8), \mathrm{a} = 4$

$$\mathrm{d} = a^{(p-1)/4}\ mod\ p$$
$$= 4^{(13-1)/4}\ mod\ 13$$
$$= 4^3\ mod\ 13\ \equiv 12\ (mod\ 13)$$
$$\mathrm{r} = 2a(4a)^{(p-5)/8}\ mod\ p$$
$$= 2 * 4 * (4 * 4)^{(13-5)/8}\ mod\ 13$$
$$= 128\ mod\ 13\ \equiv 11\ (mod\ 13)$$
$$r^2 = 11^2\ mod\ 13\ \equiv 4\ (mod\ 13)$$

Algorithm Finding square roots modulo a prime p where $p \equiv 5 \pmod 8$

INPUT: an odd prime p where $p \equiv 5 \pmod 8$, and a square $a \in Q_p$.
OUTPUT: the two square roots of a modulo p.

1. Compute $d = a^{(p-1)/4} \bmod p$ (Algorithm 2.143).
2. If $d = 1$ then compute $r = a^{(p+3)/8} \bmod p$.
3. If $d = p - 1$ then compute $r = 2a(4a)^{(p-5)/8} \bmod p$.
4. Return$(r, -r)$.

Computing square roots in $\mathbb{Z}_n$

- n: Prime(5/5)
  - For finding square roots modulo p(when $p-1=2^s t$ with large)
  - Algorithm 2.227: Repeated square-and-multiply algorithm for exp. in $\mathbb{Z}_n$

Algorithm Finding square roots modulo a prime p

INPUT: an odd prime p and a square $a \in Q_p$.
OUTPUT: the two square roots of a modulo p.

1. Choose random $b \in \mathbb{Z}_p$ until $b^2 - 4a$ is a quadratic non-residue modulo p, i.e., $\left(\frac{b^2-4a}{p}\right) = -1$.
2. Let f be the polynomial $x^2 - bx + a$ in $\mathbb{Z}_p[x]$.
3. Compute $r = x^{(p+1)/2} \bmod f$ using Algorithm 2.227. (Note: r will be an integer.)
4. Return($r, -r$).

- n: composite(1/2)
  - Square Root Modulo n Problem(SQROOT): given a composite integer *n* and a quadratic residue a modulo *n* (i.e. $a \in Q_n$), find a square root of a modulo *n*
  - If the factors p and q of n are known, SQROOT can be solved efficiently by first finding square roots and combining them using CRT(Chinese Remainder Theorem)

Algorithm Finding square roots modulo n given its prime factors p and q

INPUT: an integer n, its prime factors p and q, and $a \in Q_n$.
OUTPUT: the four square roots of a modulo n.

1. Use Algorithm 3.39 (or Algorithm 3.36 or 3.37, if applicable) to find the two square roots r and $-r$ of a modulo p.
2. Use Algorithm 3.39 (or Algorithm 3.36 or 3.37, if applicable) to find the two square roots s and $-s$ of a modulo q.
3. Use the extended Euclidean algorithm (Algorithm 2.107) to find integers c and d such that $cp + dq = 1$.
4. Set $x \leftarrow (rdq + scp) \bmod n$ and $y \leftarrow (rdq - scp) \bmod n$.
5. Return($\pm x \bmod n$, $\pm y \bmod n$).

Computing square roots in $\mathbb{Z}_n$

- n: composite(2/2)
  - Ex) p=3, q= 5, n=15, a=4
    (1) Calc. r, -r, s, -s(r =2, s=2)

    (2) Calc. c and d by using the Extended Euclidean Alg.
    (c=2, d=14, 3*2 5*14=76 = 1(mod 15))

    (3) Calc. x = (rdq + scp) mod n
    x = (2*14*5) + (2*2*3) = 152 = 2 (mod 15)
    $$x^2 = 2^2 \equiv 4 \ (mod\ 15)$$
    (3) Calc. y = (rdq - scp) mod n
    y = (2*14*5) - (2*2*3) = 128 = 8 (mod 15)
    $$y^2 = 8^2 = 64 \equiv 4 \ (mod\ 15)$$

Thank you!