Exercise 3 in Advanced Methods of Cryptography - Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-11-07

Solution of Problem 7

p prime, g primitive element modulo p and $a, b \in \mathbb{Z}_p^*$.

a) a is a quadratic residue modulo $p \quad \Leftrightarrow \quad \exists i \in \mathbb{N}_0 : a \equiv g^{2i} \mod p$

Proof. "$\Rightarrow$": a is a quadratic residue modulo p, i.e. $\exists k \in \mathbb{Z}_p^* : k^2 \equiv a \mod p$. g is a primitive element, i.e. $\exists l \in \mathbb{N}_0 : k \equiv g^l \mod p$. Then,

$$k^2 \equiv g^{2l} \equiv a \mod p\,.$$

"$\Leftarrow$": $\exists i \in \mathbb{N}_0 : a \equiv g^{2i} \mod p$. With $a \equiv (g^i)^2 \mod p$, a is a quadratic residue modulo i. □

b) If p is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo p.

Proof. p even: $|\mathbb{Z}_2^*| = 1$

p odd: $\left|\mathbb{Z}_p^*\right| = p - 1$ is even.

$$\mathbb{Z}_p^* = \langle g \rangle = \left\{g^0, g^1, \dots, g^{p-2}\right\}$$

$$A := \left\{g^0, g^2, g^4, \dots, g^{p-3}\right\}, |A| = \frac{p-1}{2}$$

$$x \in A, \text{i.e. } \exists i \in \mathbb{N}_0 : x \equiv g^{2i} \mod p \overset{a)}{\Rightarrow} x \text{ is a quadratic residue modulo } p$$

$$x \in \mathbb{Z}_p^* \setminus A \text{ and assume } x \text{ is quadratic residue modulo } p \overset{a)}{\Rightarrow} \exists i \in \mathbb{N}_0 : x \equiv g^{2i} \mod p$$

$$\Rightarrow x \in A, \text{a contradiction. (Note: } 2i \mod (p-1) \text{ is even)}$$

□

c) $a \cdot b$ is a quadratic residue modulo $p \Leftrightarrow \begin{cases} a, b \text{ are quadratic residues modulo } p \\ a, b \text{ are quadratic nonresidues modulo } p \end{cases}$

Proof. $p = 2$: trivial, as $\left|\mathbb{Z}_p^*\right| = 1$.

$p > 2$: "$\Rightarrow$": Let $a \equiv g^k \mod p$, $b \equiv g^l \mod p$. With $a \cdot b$ quadratic residue modulo p:

$$\exists i \in \mathbb{N}_0 : a \cdot b \equiv g^{2i} \mod p$$
$$\Rightarrow a \cdot b \equiv g^{k+l} \equiv g^{2i} \mod p$$
$$\Rightarrow k + l \equiv 2i \mod (p-1)$$
$$(\text{Note: } p-1 \text{ even } \Rightarrow k+l \mod (p-1) \text{ even})$$
$$\Rightarrow \begin{cases} k, l \text{ even} & \overset{a)}{\Rightarrow} a, b \text{ are quadratic residues} \\ k, l \text{ odd} & \overset{a)}{\Rightarrow} a, b \text{ are quadratic nonresidues} \end{cases}$$

"$\Leftarrow$": a, b are quadratic residues modulo p. Then

$$a \cdot b \equiv g^{2k} \cdot g^{2l} \equiv g^{2(k+l)} \mod p \overset{a)}{\Rightarrow} a \cdot b \text{ quadratic residue modulo } p\,.$$

a, b are quadratic nonresidues modulo p. Then

$$a \cdot b \equiv g^{2k+1} \cdot g^{2l+1} \equiv g^{2(k+l+1)} \mod p \overset{a)}{\Rightarrow} a \cdot b \text{ quadratic residue modulo } p\,.$$

□

Solution of Problem 8

a) Given $x \equiv -x \mod p$, prove that $x \equiv 0 \mod p$.

Proof. The inverse of 2 modulo p exists. Then,

$$\begin{aligned} & -x \equiv x && \mod p \\ \Leftrightarrow \quad & 0 \equiv 2x && \mod p \\ \Leftrightarrow \quad & 0 \equiv x && \mod p\,. \end{aligned}$$

□

b) Given $x, y \not\equiv 0 \mod p$ and $x^2 \equiv y^2 \mod p^2$, prove that $x \equiv \pm y \mod p^2$.

Proof. We proof the statement by contradiction. First, rewrite the right hand side to become a statement of divisibility.

$$\begin{aligned} & x^2 \equiv y^2 \mod p^2 \\ \Leftrightarrow \quad & p^2 \mid (x^2 - y^2) \\ \Leftrightarrow \quad & p^2 \mid (x-y)(x+y) \end{aligned}$$

p^2 has the three divisors $\{1, p, p^2\}$. Assume that for some a, b, c that $a \mid bc$. If $\gcd(a, b) = 1$, i.e., a and b are relative prime, then $a \mid c$. Set $a = p^2$, $b = x - y$, and $c = x + y$.

i) If $\gcd(p^2, x-y) = 1$, then $p^2 \mid (x+y) \Leftrightarrow x \equiv -y \mod p^2$.

ii) If $\gcd(p^2, x+y) = 1$, then $p^2 \mid (x-y) \Leftrightarrow x \equiv y \mod p^2$.

iii) If $\gcd(p^2, x-y) = p^2$, then $p^2 \mid (x-y) \Leftrightarrow x \equiv y \mod p^2$.

iv) If $\gcd(p^2, x+y) = p^2$, then $p^2 \mid (x+y) \Leftrightarrow x \equiv -y \mod p^2$.

v) If $\gcd(p^2, x-y) = p$, then $p^2 \nmid (x-y)$, but, by assumption, $p^2 \mid (x-y)(x+y)$ and it follows that $p \mid (x+y)$.

$$\Rightarrow\ x - y = k \cdot p \ \wedge\ x + y = l \cdot p \ \Leftrightarrow\ 2x = (k+l) \cdot p \ \Leftrightarrow\ x = \frac{k+l}{2} \cdot p$$
$$\Rightarrow\ x \equiv 0 \mod p, \text{ a contradiction.}$$

vi) If $\gcd(p^2, x+y) = p$, then an analogous argumentation to the previous case can be calculated.

In other words, the last two cases are not possible and the first four cases are the remaining solutions to the original statement of divisibility:

$$x \equiv \pm y \mod p^2$$

□

c) Looking at the protocol, we can show that Bob always loses to Alice, if she chooses $p = q$.

i) Alice calculates $n = p^2$ and sends n to Bob.

ii) Bob calculates $c \equiv x^2 \mod n$ and sends c to Alice. With high probability $p \nmid x \Leftrightarrow x \equiv 0 \mod p$ (therefore, Bob *almost* always loses).

iii) The only two solutions $\pm x$ are calculated by Alice (see below) and sent to Bob. Bob cannot factor n, as

$$\gcd(x - (\pm x), n) = \begin{cases} \gcd(0, n) = n \\ \gcd(2x, n) = \gcd(2x, p^2) = 1 \end{cases}.$$

Alice always wins.

d) If Bob asks for the secret key as confirmation, the square is revealed and Alice will be accused of cheating. Bob can factor n by calculating $p = \sqrt{n}$ as a real number and win the game.

Note: The two solutions $\pm x$ to $x^2 \equiv c \mod p^2$ can be calculated as follows.

Let p be an odd prime and $x, y \not\equiv 0 \mod p$. If $x^2 \equiv y^2 \mod p^2$, then $x^2 \equiv y^2 \mod p$, so $x \equiv \pm y \mod p$.

Let $x \equiv y \mod p$. Then

$$x = y + ap\,.$$

By squaring we get

$$x^2 = y^2 + 2apy + (ap)^2$$
$$\Rightarrow x^2 \equiv y^2 + 2apy \mod p^2\,.$$

Since $x^2 \equiv y^2 \mod p^2$, we obtain

$$0 = 2apy \mod p^2 .$$

Divide by p to get

$$0 = 2ay \mod p .$$

Since p is odd and $p \nmid y$, we must have $p \mid a$. Therefore, $x = y + ap \equiv y \mod p^2$. The case $x \equiv -y \mod p$ is similar.

In other words, if $x^2 \equiv y^2 \mod p^2$, not only $x \equiv \pm y \mod p$, but also $x \equiv \pm y \mod p^2$.

As we can find square roots modulo a prime p, we have $x = b$ solves $x^2 \equiv c \mod p$. We want $x^2 \equiv c \mod p^2$. Square $x = b + ap$ to get

$$b^2 + 2bap + (ap)^2 \equiv b^2 + 2bap \equiv c \mod p$$
$$\Rightarrow b^2 = c \mod p .$$

Since $b^2 = c \mod p$ the number $c - b^2$ is a multiple of p, so we can divide by p and get

$$2ab = \frac{c - b^2}{p} \mod p .$$

Multiplying by the multiplicative inverse modulo p of 2 and b, we obtain:

$$a = \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} \mod p .$$

Therefore, we have $x = b + ap$.

This procedure can be continued to get solutions modulo higher powers of p. It is the numberic-theoretic version of Newton's method for numerically solving equations, and is usually referred to as Hensel's Lemma.

Example: $p = 7$, $p^2 = 49$, $c = 37$. Then

$$b = c^{\frac{p+1}{4}} = 37^{\frac{7+1}{4}} = 37^2 \equiv 4 \mod p ,$$
$$b^{-1} \equiv 2 \mod p , \quad 2^{-1} \equiv 4 \mod p ,$$
$$a = \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} = \frac{37 - 4^2}{7} \cdot 4 \cdot 2 \equiv 3 \mod p$$
$$x = b + ap = 4 + 3 \cdot 7 = 25$$

Check: $x^2 = 25^2 \equiv 37 = c \mod p^2$.

Solution of Problem 9

Recall the definition of the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & , a \equiv 0 \mod p \\ 1 & , a \text{ is a quadratic residue modulo p} \\ -1 & , \text{otherwise} \end{cases} ,$$

with $p > 2$ prime, $a \in \mathbb{N}$. Also, recall that $c \in \mathbb{Z}_n^*$ is a quadratic residue modulo n, if $\exists x \in \mathbb{Z}_n^* : x^2 \equiv c \mod n$.

Claim: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ for $p > 2$ prime.

Proof. (i) $a = 0 \Rightarrow a^{\frac{p-1}{2}} = 0$

(ii) a is a quadratic residue modulo p. With Eulers criterion and $p > 2$ prime:

$$c \in \mathbb{Z}_p^* \text{ is a quadratic residue modulo } p \Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \mod p$$

(iii) a is a quadratic nonresidue modulo p. If a is a quadratic nonresidue modulo p, then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ because

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \mod p$$

and $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$.

□

a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ from claim.

b)

$$\begin{aligned}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &\overset{\text{(claim)}}{=} \left(a^{\frac{p-1}{2}} \mod p\right)\left(b^{\frac{p-1}{2}} \mod p\right)\\ &= (ab)^{\frac{p-1}{2}} \mod p\\ &\overset{\text{(claim)}}{=} \left(\frac{ab}{p}\right)\end{aligned}$$

c) Assumption: $a \equiv b \mod p$.

$$\begin{aligned}\left(\frac{a}{p}\right) &= a^{\frac{p-1}{2}} \mod p\\ &\overset{\text{(Assumption)}}{=} b^{\frac{p-1}{2}} \mod p\\ &= \left(\frac{b}{p}\right)\end{aligned}$$

Solution of Problem 10

The proof references line numbers. Below is the same version of the algorithm computing the Jacobi symbol as in the script, but with line numbers added.

Input: odd integer $n > 2$, integer a, $0 \leq a < n$
Lines 2-4: special case $a = 0 \Rightarrow \left(\frac{a}{n}\right) = 0$.
Lines 5-7: special case $a = 1 \Rightarrow \left(\frac{a}{n}\right) = 1$.

Algorithm 1 Computing the Jacobi (and Legendre) symbol

Input: An odd integer $n > 2$ 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)

procedure JACOBI(a, n)
    if $(a = 0)$ **then**
        return 0
    end if
    if $(a = 1)$ **then**
        return 1
    end if
    Write $a = 2^e a_1$, where a_1 is odd
    if (e is even or $n \equiv 1 \pmod 8$ or $n \equiv 7 \pmod 8$) **then**
        $s \leftarrow 1$
    else
        $s \leftarrow -1$
    end if
    if ($n \equiv 3 \pmod 4$ and $a_1 \equiv 3 \pmod 4$) **then**
        $s \leftarrow -s$
    end if
    $n_1 \leftarrow n \mod a_1$
    if $(a_1 = 1)$ **then**
        return s
    end if
    return $s \cdot$JACOBI(n_1, a_1)
end procedure

Line 8: Decomposition of $\left(\frac{a}{n}\right)$

$$\left(\frac{a}{n}\right) = \left(\frac{2^e a_1}{n}\right) \overset{\text{Remark 9.9}}{=} \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) \qquad a_1, n \text{ are odd}$$

$$\overset{\text{Hint}}{=} \underbrace{\left(\frac{2^e}{n}\right)}_{\substack{\text{line 9--13}\\ \text{(Note 1)}}} \underbrace{(-1)^{\frac{a_1-1}{2}\frac{n-1}{2}}}_{\substack{\text{line 14--16}\\ \text{(Note 2)}}} \underbrace{\underbrace{\left(\frac{n}{a_1}\right)}\overset{a_1 \geq 2}{=} \left(\frac{n \mod a_1}{a_1}\right) = \left(\frac{n_1}{a_1}\right)}_{\substack{\text{line 17--21}\\ \text{(Note 3)}}}$$

$$= \left(\frac{2}{n}\right)^e \left(\frac{n \mod a_1}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}}$$

Note 1:

$$\left(\frac{2^e}{n}\right) = \left(\frac{2}{n}\right)^e \overset{\text{Hint}}{=} \left((-1)^{\frac{n^2-1}{8}}\right)^e$$

e even: $\left(\frac{2}{n}\right)^e = 1$ (line 9-10)

e odd: $\left(\frac{2}{n}\right)^e = \left(\frac{2}{n}\right)^{2k+1} = \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, $\quad k \in \mathbb{N}_0 : e = 2k+1$

Note that $\frac{n^2-1}{8}$ is integer as, with $n = 2l+1$, $l \in \mathbb{N}$,

$$(2l+1)^2 - 1 = 4l^2 + 4l + 1 - 1 = 4l(l+1) \equiv 0 \mod 8\,.$$

With $n = 8m + k$, where $m \in \mathbb{N}_0$, $k \in \{1, 3, 5, 7\}$, we can write

$$\frac{n^2-1}{8} = \frac{(8m+k)^2 - 1}{8} = \frac{(8m)^2 + 16mk + k^2 - 1}{8}$$
$$= \frac{16m(4m+k) + k^2 - 1}{8} = \underbrace{2m(4m+k)}_{\text{even}} + \frac{k^2-1}{8}\,,$$

and it follows that

$$(-1)^{\frac{n^2-1}{8}} = (-1)^{\frac{(n \mod 8)^2 - 1}{8}}\,.$$

In other words, we can find all possibile outcomes of $(-1)^{\frac{n^2-1}{8}}$, n odd integer, by looking at $(-1)^{\frac{k^2-1}{8}}$ for $k \in \{1, 3, 5, 7\}$.

k	k^2-1	$\frac{k^2-1}{8}$	$\left(\frac{2}{n}\right) = (-1)^{\frac{k^2-1}{8}}$	line
1	0	0	1	9,10
3	8	1	-1	11,12
5	24	3	-1	11,12
7	48	6	1	9,10

Note 2:

$$(-1)^{\frac{a_1-1}{2}\frac{n-1}{2}} = -1 \Leftrightarrow \frac{a_1-1}{2}\frac{n-1}{2} \text{ odd} \Leftrightarrow \frac{a_1-1}{2} \wedge \frac{n-1}{2} \text{ odd}$$
$$\Leftrightarrow a_1 \equiv 3 \mod 4 \;\wedge\; n \equiv 3 \mod 4 \quad (\text{lines } 14-16)$$

Note 3 (line 18f):

If $\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{1}{n}\right) = \left(\frac{2^e}{n}\right)$ with $(-1)^{\frac{a_1-1}{2}\frac{n-1}{2}} = 1 \overset{\text{line 19}}{\Rightarrow} \left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right) \cdot 1$. Else $\left(\frac{a}{n}\right) = s \cdot \left(\frac{a_1}{n}\right)$.