Crypto 2 Ü 4

15. NOV. 2011

$c \in \mathbb{Z}_n^*$ is QR mod n, iff $\exists x \in \mathbb{Z}_n^*$:
$x^2 \equiv c \pmod n$

Legendre symbol: $\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod n \\ 1 & a \text{ QR} \pmod n \\ -1 & \text{otherwise} \end{cases}$

Claim: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ $\quad p > 2$, prime

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

ii.) a is QR mod p
Euler's criterion (Prop. 9.2., Ex 8 (HW 3))
$p > 2$, prime $c \in \mathbb{Z}_p^*$ is QR (mod p), iff
$c^{\frac{p-1}{2}} \equiv 1 \pmod p$ ✓

iii.) a is no QR mod p
$a^{\frac{p-1}{2}} = (c^i)^{\frac{p-1}{2}}$ c primitive element, $a = c^i$, $i \in \mathbb{N}_0$
$= (c^{p-1})^{i/2} \equiv 1^{i/2} = \begin{cases} 1 & \text{if } c^i \text{ is QR, see ii.), Euler's crit.} \\ -1 & \text{otherwise} \end{cases}$ ✓

Ex 11.)

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

b.) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(a^{\frac{p-1}{2}} \bmod p\right)\left(b^{\frac{p-1}{2}} \bmod p\right)$
$= \left((ab)^{\frac{p-1}{2}} \bmod p\right) = \left(\frac{ab}{p}\right)$ ✓

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

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

Ex 12.)

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

a.) (Prop. 9.13)

a QR mod p $\Longleftrightarrow$ $\exists i \in \mathbb{N}_0$ with $a \equiv g^{2i} \pmod p$

$\boxed{\text{"}\Rightarrow\text{"}}$ a QR mod p $\Rightarrow$ $\exists k \in \mathbb{Z}_p^*: k^2 \equiv a \pmod p$

g PE $\Rightarrow$ $l \in \mathbb{N}_0 : k = g^l$

$\Rightarrow k^2 = g^{2l} \equiv a \pmod p$

$\boxed{\text{"}\Leftarrow\text{"}}$ $\exists i \in \mathbb{N}_0$ with $a \equiv g^{2i} \pmod p \Rightarrow a \equiv (g^i)^2 \pmod p$

$\Rightarrow$ a is QR mod p

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

p even: $|\mathbb{Z}_p^*| = 1$

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

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

$$A = \{g^0, g^2, \dots, g^{p-3}\} \Rightarrow |A| = \frac{p-1}{2}$$

$\overset{a.)}{\Rightarrow}$ $x \in A$ is QR, $x \in \mathbb{Z}_p^* \setminus A$ is no QR ✓

Crypto 2 Ü4

c.) 1.) a, b QR $\overset{a.)}{\Rightarrow}$ $a = g^i$, $b = g^j$ with i,j even

$\Rightarrow$ i+j even $\Rightarrow$ $ab = g^{i+j} \pmod p$

QR mod p

2.) a,b NQR $\overset{a.)}{\Rightarrow}$ $a = g^i$, $b = g^j$ with i,j odd

$\Rightarrow$ i+j even $\overset{a.)}{\Rightarrow}$ ab QR mod p

3.) WLOG (o.B.d.A) a QR, b NQR

$\overset{a.)}{\Rightarrow}$ $a = g^i$, $b = g^j$, i even, j odd

$\Rightarrow$ i+j odd $\overset{a.)}{\Rightarrow}$ a·b NQR mod p

$\Rightarrow$ claim

Ex 13.) Goldwasser-Micali-Cryptosystem

$n = p \cdot q = 31 \cdot 79 = 2449$, Follow Alg. 7 to find pseudo-square

(a.) 1.) Choose $a \in \mathbb{Z}_p^*$ (at random) and check, if $\left(\frac{a}{p}\right) = -1$

$a = 10$ $\quad \left(\frac{10}{31}\right) \overset{\text{claim}}{\equiv} 10^{\frac{31-1}{2}} \equiv 10^{15} \equiv 1 \pmod p$,

e.g. sqm or Alg. 6

$a = 11$ $\quad \left(\frac{11}{31}\right) \equiv 11^{15} \equiv -1 \pmod p$

2.) $b = 17$, $\left(\frac{b}{q}\right) = \left(\frac{17}{79}\right) \equiv 17^{\frac{79-1}{2}} \equiv 17^{39} \equiv -1$ (mod 79=q)

3.) Compute y mod n, $y \equiv a \bmod p$

$y \equiv b \bmod q$

chinese remainder: $m_1 = p$, $m_2 = q$, $a_1 = a$, $a_2 = b$

$M = m_1 m_2 = n = p \cdot q$, $M_1 = m_2 = q$, $M_2 = m_1 = p$

$\gcd(q,p) = 1 = 11 \cdot q - 28 \cdot p = 11 \cdot 79 - 28 \cdot 31$
(Extended Euclidean Algorithm)

$\Rightarrow y = a \cdot q \cdot 11 - b \cdot p \cdot 28 = 11 \cdot 79 \cdot 11 - 17 \cdot 31 \cdot 28$

$\equiv 2150 \pmod{n}$

y is QR mod n

b.)

$c = (1418, 2150, 2153)$

$\left(\frac{1418}{31}\right) = -1 \Rightarrow m_1 = 1, \left(\frac{2150}{31}\right) = -1 \Rightarrow m_2 = 1$

$\left(\frac{2153}{31}\right) = 1 \Rightarrow m_3 = 0$

$\Rightarrow m = (m_1, m_2, m_3) = (1, 1, 0)$