David M. Burton - Elementary No. Theory

Quadratic residues

Defⁿ: (valid for composite n also).

Let $a \in \mathbb{Z}_p^*$ (i.e. $(a,p)=1$) where p is an odd prime and $a \not\equiv 0 \pmod p$.

a is said to be a quadratic residue modulo p, or a square modulo p, if $\exists$ an $x \in \mathbb{Z}_p^*$ s.t. $x^2 \equiv a \pmod p$. If no such x exists, then a is called a quadratic non-residue modulo p.

The set of all quadratic residues modulo p is denoted by Q_p and the set of all quadratic non-residues is denoted by $\bar{Q}_p$.

Note that $0 \notin \mathbb{Z}_p^*$, whence $0 \notin Q_p$ & $0 \notin \bar{Q}_p$.

Two basic problems dominate the theory of quadratic residues:

i) Given a prime p, determine which a are quadratic residues mod p & which are quadratic non-residues mod p.

ii) Given a, determine those primes p for which a is a quadratic residue mod p and those for which a is a quadratic non-residue mod p.

Let us begin with some methods for solving problem (i).

Example:

To find the quadratic residues modulo 11 we square the numbers $1, 2, \cdots, 10$ and reduce mod 11. We obtain

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 5, \quad 5^2 \equiv 3 \pmod{11}$$

It suffices to square only the first half of the numbers since

$$6^2 \equiv (-5)^2 \equiv 3, \quad 7^2 \equiv (-4)^2 \equiv 5, \quad 8^2 \equiv (-3)^2 \equiv 9$$

$$9^2 \equiv (-2)^2 \equiv 4, \quad 10^2 \equiv (-1)^2 \equiv 1 \pmod{11}$$

Consequently, the quadratic residues mod 11 are $1, 3, 4, 5, 9$ & the non-residues are

$2, 6, 7, 8, 10$.

This example illustrates the following theorem:

Th. Let p be an odd prime. Then every residue System mod p contains exactly $(p-1)/2$ quadratic residues & exactly $(p-1)/2$ quadratic non-residues mod p. The quadratic residues belong to the residue classes containing the numbers

$$1^2, 2^2, 3^2, \cdots, \left(\frac{p-1}{2}\right)^2. \quad \text{---} \quad (1)$$

proof. First note that the numbers in (1) are distinct mod p. In fact, if $x^2 \equiv y^2 \pmod{p}$

with $1 \le x \le \frac{(p-1)}{2}$ and $1 \le y \le \frac{(p-1)}{2}$, then

$$(x-y)(x+y) \equiv 0 \pmod{p}.$$

But $1 < x+y < p$ so $x-y \equiv 0 \pmod{p}$,

hence $x = y$.

Since $(p-k)^2 \equiv k^2 \pmod{p}$,

every quadratic residue is congruent mod p to exactly one of the numbers in (1).

This completes the proof. □

brief

The following table of quadratic residues Q_p and non-residues $\bar{Q}_p$ was obtained with the help of the above theorem.

	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
Q_p	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12
$\bar{Q}_p$	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11

The Legendre and Jacobi Symbols

The legendre symbol is a useful tool for keeping track of whether or not an integer a is a quadratic residue modulo a prime p.

Def^n: Let p be an odd prime and a an integer. The legendre symbol $\left(\frac{a}{p}\right)$ is defined to be

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

Examples:
$\left(\frac{1}{p}\right)=1$, $\left(\frac{m^2}{p}\right)=1$, $\left(\frac{7}{11}\right)=-1$
$\left(\frac{22}{11}\right)=0$

Note: We use the notation χ for the legendre symbol i.e $\chi(a)=\left(\frac{a}{p}\right)$.

Properties of legendre symbol

Let p be an odd prime and $a, b \in \mathbb{Z}$. Then the Legendre symbol has the following properties:

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 $-1 \in \bar{Q}_p$ 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) → proof

If q is an odd prime distinct from p, then

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

In otherwords, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless both p and q are congruent to 3 modulo 4, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

The Jacobi symbol is a generalization of the Legendre symbol to integers n which are odd but not necessarily prime.

Def: Let $n > 3$ be odd with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then the Jacobi symbol $\left(\frac{a}{n}\right)$ is defined to be

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

Observe that if n is prime, then the Jacobi symbol is just the Legendre symbol.

Properties of Jacobi Symbols.

Let $m \geq 3$, $n \geq 3$ be odd integers, and $a, b \in \mathbb{Z}$. Then the Jacobi symbol has the following properties:

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

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

(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 & n are congruent to 3 modulo 4, in which case $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

It is clear that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ whenever $a \equiv b \pmod p$,

So $\left(\frac{a}{p}\right)$ is a periodic function of a with period p.

Fermat's little theorem (A special case of Euler's Th.)

$$a^{p-1} \equiv 1 \pmod p \quad \text{if} \quad p \nmid a.$$

Since $$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right)$$

it follows that $$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

The next theorem tells us that we get $+1$ if $a \in Q_p$ and -1 if $a \in \bar{Q}_p$.

Theorem (Euler's criterion)

Let p be an odd prime. Then for all a we have

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

proof. Case 1 If $a \equiv 0 \pmod p$ the result is trivial since both members are congruent to 0 mod p.

Case 2 Now suppose that $\left(\frac{a}{p}\right) = 1$.

Then $\exists\ x$ s.t. $x^2 \equiv a \pmod p$ and hence

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod p$$

by Fermat's little theorem. $= \left(\frac{a}{p}\right)$.

Thus the theorem is proved if $\left(\frac{a}{p}\right) = 1$

Case 3 Now suppose that $\left(\frac{a}{p}\right) = -1$ & consider the following polynomial

$$f(x) = x^{\frac{p-1}{2}} - 1$$

Since $f(x)$ is a polynomial of degree $\frac{p-1}{2}$ (with integer co-efficients), the congruence

$$f(x) \equiv 0 \pmod{p}$$

(by Lagrange's Th. (↛ not true for composite modulus))

has at most $\frac{p-1}{2}$ solutions. But the $\frac{p-1}{2}$ quadratic residues mod p are solutions, so the non-residues are not.

Hence $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$.

But $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ so $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ $= \left(\frac{a}{p}\right)$.

This completes the proof.

Theorem Legendre's symbol $\left(\frac{a}{p}\right)$ is a completely multiplicative function of a. [i.e. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$].

proof:- **Case 1** If $p \mid a$ or $p \mid b$, then $p \mid ab$

so $\left(\frac{ab}{p}\right) = 0$ and either $\left(\frac{a}{p}\right) = 0$ or $\left(\frac{b}{p}\right) = 0$.

Therefore, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ if $p \mid a$ or $p \mid b$.

Case 2 If $p \nmid a$ and $p \nmid b$, then $p \nmid ab$ & we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

But each of $\left(\frac{ab}{p}\right)$, $\left(\frac{a}{p}\right)$ & $\left(\frac{b}{p}\right)$ is 1 or -1.

So the difference

$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ is either $0, 2$ or -2

Since this difference is divisible by p, it must be 0.

Evaluation of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$

Theorem For every odd prime p we have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

proof. By Euler's criterion we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p.$$

Since each member of this congruence is 1 or -1, the two members are equal.

Theorem For every odd prime p we have

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

proof. Consider the following $\frac{p-1}{2}$ congruences:

$$\begin{aligned} p-1 &\equiv 1\,(-1)^1 && \pmod p \\ 2 &\equiv 2\,(-1)^2 && \pmod p \\ p-3 &\equiv 3\,(-1)^3 && \pmod p \\ 4 &\equiv 4\,(-1)^4 && \pmod p \\ &\vdots \\ r &\equiv \tfrac{p-1}{2}\,(-1)^{\frac{p-1}{2}} && \pmod p \end{aligned}$$

where r is either $p - \frac{p-1}{2}$ or $\frac{p-1}{2}$.

Multiply these together & note that each integer on the left is even. We obtain

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left\lfloor \frac{p-1}{2} \right\rfloor (-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod{p}$$

This gives us

$$2^{\frac{p-1}{2}} \left\lfloor \frac{p-1}{2} \right\rfloor = \left\lfloor \frac{p-1}{2} \right\rfloor (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Since $\left\lfloor \frac{p-1}{2} \right\rfloor \not\equiv 0 \pmod{p}$, this implies

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

By Euler's criterion, we have

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p},$$

and since each member is 1 or -1, the two members are equal. This completes the proof.

Jacobi Symbol

Defn: Let $n \geq 3$ be odd with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then the Jacobi symbol $\left(\frac{a}{n}\right)$ is defined to be

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

Case n prime $\rightarrow$ Jacobi symbol is just the Legendre symbol.

Fact (Properties of Jacobi symbol)

Let $m \geq 3$, $n \geq 3$ be odd integers, and $a, b \in \mathbb{Z}$.
Then the Jacobi symbol has the following properties:

(i) $\left(\frac{a}{n}\right) = 0, 1$ or -1.

$\left(\frac{a}{n}\right) = 0$ iff $\gcd(a,n) \neq 1$.

(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) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ [Hence $\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \end{cases}$]

(vii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$. [Hence $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } n \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$]

(viii) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$

i.e. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ unless both m, n are congruent to 3 modulo 4, in which case $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

Note: If n is odd and $a = 2^e a_1$ when a_1 is odd, then

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right)$$

~~$= \left(\frac{2}{n}\right)^e \left(\frac{a_1}{n}\right)$~~

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

This observation yields the following recursive algm. for computing $\left(\frac{a}{n}\right)$, which does not require the prime factorization of n.

Note- no deterministic poly-time algm. to find quadratic non-residues modulo a prime p,

although we know that half of the elements in Z_p^* are quadratic residues modulo p.

randomized algm. for finding quadratic non-residues modulo p

$a \in_R Z_p^* \rightarrow$ random selection of a

until one is found satisfying

$$\left(\frac{a}{p}\right) = -1.$$

Example- Jacobi Symbol Computation

$a = 158, \quad n = 235.$

$$\left(\frac{158}{235}\right) = \left(\frac{2}{235}\right)\left(\frac{79}{235}\right) = (-1)\left(\frac{79}{235}\right)^{\frac{(79-1)(235-1)}{4}}$$

$$= (-1)\left(\frac{235}{79}\right)(-1)$$

$$= (-1)\left(\frac{77}{79}\right)(-1)$$

$$= \left(\frac{77}{79}\right) = \left(\frac{79}{77}\right)(-1)^{\frac{(77-1)(79-1)}{4}} = \left(\frac{2}{77}\right) = -1$$

$8 \mid 77 \mid 9$
72
3

$8 \mid 235 \mid 29$
16
75
72
3

$79 \mid 235 \mid 2$
158
77

$39 \quad 78 \times 234 \quad 127$
$4 \quad 2$

$38 \quad 76 \times 78$
$4 \quad 1$

Algorithm — Jacobi Symbol computation (& legendre Symbol)

JACOBI (a, n)

Input : an odd integer $n \geq 3$, and an integer a, $0 \leq a < n$.

Output : the Jacobi symbol $\left(\frac{a}{n}\right)$ (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 $(s, \text{JACOBI}(a_1, n_1))$

Note. $\left(\frac{a}{n}\right) = 1 \not\Rightarrow a \in Q_n$

But $a \in Q_n \Rightarrow \left(\frac{a}{n}\right) = 1$

Example

$Q_{21} = \{1, 4, 16\}$

$\left(\frac{5}{21}\right) = 1$ but $5 \notin Q_{21}$

$\left(\frac{5}{3}\right)\left(\frac{5}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{5}{7}\right)$

$= (+1)(-1) = -1$

Def? Let $n \geq 3$ be an odd integer, and let $J_n = \{a \in \mathbb{Z}_n^* \mid \left(\frac{a}{n}\right) = 1\}$

The set of pseudosquares modulo n, denoted by $\tilde{Q}_n$ is defined to be the set $J_n - Q_n$.

Fact. Let $n = pq$, p, q are two distinct primes.

Then $|Q_n| = |\tilde{Q}_n| = \frac{(p-1)(q-1)}{4}$.

i.e. half of the elements in J_n are quadratic residues (squares), and the other half are pseudosquares modulo n.

$$\left(\frac{59}{67}\right) = \left(\frac{67}{59}\right)(-1) = \left(\frac{8}{59}\right) \qquad 33 \times 29$$

$$= \left(\frac{2}{59}\right)^3 = (-1)^3 = -1$$

$\frac{66}{2} \quad \frac{58}{2}$

$8 \mid 59 \mid 7$
$\quad 56$
$\quad\ 3$

$8K+3$

Theorem If P is an odd positive integer, then

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$$

& $$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$$

proof:- Write $P = p_1 p_2 \cdots p_m$ where the prime factors p_i are not necessarily distinct.

$$P = \prod_{i=1}^{m} p_i$$

$$= \prod_{i=1}^{m} (1 + p_i - 1) = 1 + \sum_{i=1}^{m} (p_i - 1) + \sum_{\substack{i=1 \\ i \neq j}}^{m} \sum_{j=1}^{m} (p_i - 1)(p_j - 1) + \cdots$$

Each $(p_i - 1)$ is even.

$$\therefore P \equiv 1 + \sum_{i=1}^{m} (p_i - 1) \pmod 4$$

$$\text{or } \frac{1}{2}(P-1) \equiv \frac{1}{2}\sum_{i=1}^{m} (p_i - 1) \pmod 2 \quad \text{— (A)}$$

$a \equiv b \pmod 2$ $\Rightarrow$ a, b both odd or both even $(-1)^a = (-1)^b$.

$$\therefore \left(\frac{-1}{P}\right) = \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right) = \prod_{i=1}^{m} (-1)^{\frac{(p_i-1)}{2}} = (-1)^{\sum_{i=1}^{m} \frac{(p_i-1)}{2}}$$

$$= (-1)^{\frac{P-1}{2}}$$

equality, be same argument as both side an either 1 or -1 & hence then

Theorem if $ac \equiv bc \pmod m$ & $\gcd(c, m) = d$ then $a \equiv b \pmod{\frac{m}{d}}$

Corollary if $ac \equiv bc \pmod m$ & $c \mid m$, then $a \equiv b \pmod{\frac{m}{c}}$

$$P^2 = \prod_{i=1}^{m}\left(1+p_i^2-1\right)$$

$$= 1 + \sum_{i=1}^{m}(p_i^2-1) + \sum_{i=1}^{m}\sum_{\substack{j=1 \\ i\neq j}}^{m}(p_i^2-1)(p_j^2-1) + \cdots$$

• Square of an odd int. is often form $8k+1$

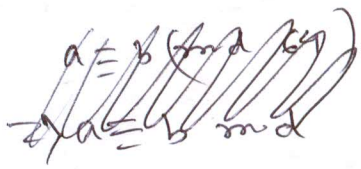
$p_i \to 4k, 4k+1, 4k+2, 4k+3$

Proof: $4k, 4k+1, 4k+2, 4k+3$ — odd — say $8k+1$

$\therefore$ p_i is odd,

each (p_i^2-1) is ~~even~~ divisible by 8 i.e. $p_i^2-1 \equiv 0 \pmod 8$

$$\therefore P^2 \equiv 1 + \sum_{i=1}^{m}(p_i^2-1) \pmod{64}$$



$$\cancel{8}\times\frac{1}{8}(P^2-1) \equiv \frac{1}{8}\sum_{i=1}^{m}(p_i^2-1) \pmod{\cancel{8}\times 8}$$

$c = 8 \mid 64$. ~~$8 \mid a \Rightarrow b \Rightarrow 8k$~~

$$\Rightarrow \boxed{\frac{1}{8}(P^2-1) \equiv \frac{1}{8}\sum_{i=1}^{m}(p_i^2-1) \pmod 2} \quad -(B)$$

$$\therefore \left(\frac{2}{P}\right) = \prod_{i=1}^{m}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{m}(-1)^{(p_i^2-1)/8} = (-1)^{\frac{1}{8}\sum(p_i^2-1)} = (-1)^{\frac{1}{8}(P^2-1)}$$

Theorem (Reciprocity law for Jacobi Symbols)

If P and Q are ~~primes~~ positive odd integers with $\gcd(P,Q)=1$, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{(P-1)(Q-1)}{4}}$.

proof.

Let $P = p_1 p_2 \cdots p_m$, $Q = q_1 q_2 \cdots q_n$, where p_i & q_i are primes.

$$\therefore \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{m}\prod_{j=1}^{n}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^r, \text{ say.}$$

$$r = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{(p_i-1)(q_j-1)}{4} = \sum_{i=1}^{m}\frac{(p_i-1)}{2}\sum_{j=1}^{n}\frac{(q_j-1)}{2} = \frac{1}{4}(P-1)(Q-1) \pmod 2$$

[by (A)]

$\Rightarrow r$, $\frac{1}{4}(P-1)(Q-1)$ have the same parity.

Theorem (Gauss lemma) Let p be an odd prime.

Assume $n \not\equiv 0 \pmod p$ and consider the least positive integer mod p of the following $(p-1)/2$ multiples of n:

$$n, 2n, 3n, \ldots \quad \frac{p-1}{2} n.$$

If m denotes the number of these residues which exceeds $p/2$, then $\left(\frac{n}{p}\right) = (-1)^m$.

proof - consider least +ve residues mod p of numbers

$$n, 2n, 3n, \ldots \quad \frac{p-1}{2} n \pmod p$$

two disjoint sets of least +ve residues

A — residues in A are $< \frac{p}{2}$

B — residues in B are $> \frac{p}{2}$.

Let $A = \{a_1, a_2, \ldots, a_k\}$

where $a_i \equiv t_i n \pmod p$ for some $t_i \le \frac{p-1}{2}$ and $0 < a_i < \frac{p}{2}$.

Let $B = \{b_1, b_2, \ldots, b_m\}$

where $b_i \equiv s_i n \pmod p$ for some $s_i \le \frac{p-1}{2}$ and $\frac{p}{2} < b_i < p$.

As A, B are disjoint,

$$m + k = \frac{p-1}{2}$$

Let $C = \{c_1, c_2, \ldots, c_m\}$, where $c_i = p - b_i$

As $\frac{p}{2} < b_i < p$, $\quad 0 < c_i < \frac{p}{2}$

i.e. elements of C lie in the same interval as the elements of A.

Claim A, C are disjoint.

if not, $c_i = a_j$ for some pair i, j.

Then $p - b_i = a_j$

or $a_j + b_i \equiv 0 \pmod p$ ... (1)

Let $a_j \equiv tn \pmod p$, $1 \le t \le \frac{p-1}{2}$ $\quad 0 < t < \frac{p}{2}$

$b_i \equiv sn \pmod p$, $1 \le s \le \frac{p-1}{2}$ $\quad 0 < s < \frac{p}{2}$

~~Then (1) $\Rightarrow tn + sn = (t+s)n$~~

$\therefore$ (1) $\Rightarrow tn + sn = (t+s)n \equiv 0 \pmod p$

$(\rightarrow\leftarrow)$

as $p \nmid n$ and $0 < t+s < p$

$\therefore$ A, C are disjoint sets.

$0 < a_i < \frac{p}{2}$ i.e. $1 \le a_i \le \frac{p-1}{2}$ $\quad$ $0 < c_i < \frac{p}{2}$ i.e. $1 \le c_i \le \frac{p-1}{2}$

$$A \cup C = \{a_1, a_2, \dots, a_k; c_1, c_2, \dots, c_m\} = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$$

$$|A \cup C| = m + k = \frac{p-1}{2}$$

$$\therefore a_1 a_2 \cdots a_k c_1 c_2 \cdots c_m = 1 \cdot 2 \cdots \frac{p-1}{2}$$

$$a_1 a_2 \cdots a_k (p-b_1)(p-b_2)\cdots(p-b_m) = \left\lfloor \frac{p-1}{2} \right\rfloor$$

$$\therefore \left\lfloor \frac{p-1}{2} \right\rfloor \equiv a_1 a_2 \cdots a_k (-b_1)(-b_2)\cdots(-b_m) \pmod p$$

$$\equiv (-1)^m a_1 a_2 \cdots a_k b_1 b_2 \cdots b_m \pmod p$$

So $n^{\frac{p-1}{2}} \equiv (-1)^m \pmod p$ (by Euler's criterion)

$$\equiv (-1)^m (n)(2n)(3n)\cdots\left(\frac{p-1}{2}n\right) \pmod p$$

$$\equiv (-1)^m n^{\frac{p-1}{2}} \left\lfloor \frac{p-1}{2} \right\rfloor \pmod p.$$

$\Rightarrow \left(\frac{n}{p}\right) \equiv (-1)^m$

exact value of m is not needed, only its parity is required.

Theorem

If m be the number defined in Gauss' Lemma. Then

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod 2 .$$

In particular, if n is odd we have

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right] \pmod 2 .$$

proof- Note that m is the no. of least +ve ~~integers~~ residues mod p of the numbers

$$n, 2n, 3n, \cdots, \left(\frac{p-1}{2}\right)n .$$

which exceeds $\frac{p}{2}$.

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{\frac{tn}{p}\right\}, \quad 0 < \left\{\frac{tn}{p}\right\} < 1 .$$

↙ integral part ↓ fraction part.

$$\Rightarrow tn = p\left[\frac{tn}{p}\right] + p\left\{\frac{tn}{p}\right\} = p\left[\frac{tn}{p}\right] + r_t , \text{ say,}$$

where $0 \le r_t < p$.

$\Rightarrow r_t = tn - p\left[\frac{tn}{p}\right]$ → least +ve residue of tn mod p.

$$\therefore \left\{ r_1, r_2, \cdots r_{\frac{p-1}{2}} \right\} = \left\{ a_1, a_2, \cdots a_k ; \; b_1, b_2 \cdots, b_m \right\}$$

Also $$\left\{ 1, 2, \cdots, \frac{p-1}{2} \right\} = \left\{ a_1, a_2, \cdots a_k ; c_1, c_2, \cdots, c_m \right\}$$

where $c_i = p - b_i$.

$$\therefore \sum_{t=1}^{\frac{p-1}{2}} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j$$

$$\& \sum_{t=1}^{\frac{p-1}{2}} t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j$$

$$r_t = tn - p\left[\frac{tn}{p}\right]$$

or we get

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = \sum_{t=1}^{\frac{p-1}{2}} \left(tn - p\left[\frac{tn}{p}\right]\right) = n\sum_{t=1}^{\frac{p-1}{2}} t - p\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right]$$

$$mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{m} b_j = \sum_{t=1}^{\frac{p-1}{2}} t$$

~~subtract or adding we get~~ or adding we get

~~$-mp + 2\sum_{i=1}^{k} a_i = (n-1)$~~

$$mp + 2\sum_{i=1}^{k} a_i = (n+1)\sum_{t=1}^{\frac{p-1}{2}} t - p\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right]$$

$$= (n+1)\frac{p^2-1}{8} - p\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right]$$

mod 2 $\quad n+1 \equiv n-1 \pmod 2$ & $p \equiv 1 \pmod 2$

& $-1 \equiv 1 \pmod 2$.

$$\therefore mp \equiv (n-1)\frac{p^2-1}{8} + p\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right] \pmod 2 .$$

Theorem (Quadratic Reciprocity law)

If p & q are distinct odd primes, then

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

proof:- By Gauss lemma, $\left(\frac{q}{p}\right) = (-1)^m$

where $m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tq}{p}\right] \pmod 2$.

Similarly, $\left(\frac{p}{q}\right) = (-1)^n$

where $n \equiv \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{sp}{q}\right] \pmod 2$.

$\therefore \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n}$ and the proof follows if the following claim is proved.

Claim

$$\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tq}{p}\right] + \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{sp}{q}\right] = \frac{p-1}{2}\,\frac{q-1}{2}$$

Let $f(t,s) = qx - py$ $\quad qt - ps$

If x, y are non-zero integers, then $f(x,y)$ is a non-zero integer.

As x takes values $1, 2, \ldots \frac{p-1}{2}$ & y takes values $1, 2, \ldots \frac{q-1}{2}$, $f(x,y)$ takes $\frac{p-1}{2}\cdot\frac{q-1}{2}$ values no two of which are equal as $f(x,y) - f(x',y') = f(x-x', y-y') \neq 0$ for $x \neq x'$ & $y \neq y'$.

$f(x,y)$ → total $\frac{p-1}{2} \cdot \frac{q-1}{2}$ distinct values

as $x \to 1, \cdots, \frac{p-1}{2}$

and $y \to 1, \cdots, \frac{q-1}{2}$.

how many are < 0 & how many are > 0.

for each fixed x,

$f(x,y) > 0$ iff $qy < px$

or $y \leq \left[\frac{qx}{p}\right]$

$\therefore$ Total no. of +ve values is $\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right]$

Similarly, total no. of −ve values is $\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$

$\therefore \frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$

Hence proved.

Security: factoring hard

Rabin Cryptosystem

- $n = pq$, p, q primes, $p, q \equiv 3 \pmod 4$
- $\mathcal{P} = \mathcal{C} = Z_n^*$, $\mathcal{K} = \{(n, p, q)\}$.
  - n: public, p, q: secret.
- for $K = (n, p, q)$,

$$e_K(x) = x^2 \bmod n$$

$$d_K(y) = \sqrt{y} \bmod n.$$

This restriction simplifies some aspects of computation analysis of cryptosystem.

Note
- restriction on p, q can be omitted.
- $\mathcal{P} = \mathcal{C} = Z_n^*$

Decryption

$y = x^2 \bmod n$, x unknown.

$\Rightarrow$ quadratic equn. in Z_n.

- decryption requires extracting sq. roots modulo n.

equivalent + solve using (Chinese remainder Th.)

$$y = z_1^2 \bmod p$$
$$y = z_2^2 \bmod q.$$

i.e. if y is a quadratic residue modulo p and modulo q.

$a \in Z_n^*$ a QR mod n if $\exists\, x \in Z_n^*$ s.t. $a = x^2 \bmod n$ o.w a is QNR

CRT. (Gauss) algo.

$m_1, \ldots, m_r \rightarrow$ pairwise relatively prime

$a_1, \ldots, a_r \rightarrow \in Z$.

$$\left.\begin{aligned} x &= a_1 \bmod m_1 \\ x &= a_2 \bmod m_2 \\ &\vdots \\ x &= a_r \bmod m_r \end{aligned}\right\}$$

has a unique soln. modulo $M = m_1 \times \cdots \times m_r$ given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \bmod m_i$ for $1 \le i \le r$.

- $p = 3 \bmod 4$, $q = 3 \bmod 4$.

decryption is easy.

$$\left(\pm y^{\frac{p+1}{4}}\right)^2 = y^{\frac{p+1}{2}} = y \cdot y^{\frac{p-1}{2}} \equiv \left(\frac{y}{p}\right) = y \bmod p$$

As $\left(\frac{y}{p}\right) \equiv y^{\frac{p-1}{2}} = 1 \bmod p$ by ~~fermat's little theorem~~ Euler's criterion.

if y is a quadratic residue modulo p.

& in this case $\pm y^{\frac{p+1}{4}}$ are the two sq. roots of $y \bmod p$

Similarly, $\pm y^{\frac{q+1}{4}}$ are the two sq. roots of $y \bmod q$

- find 4 sq. roots modulo $n = pq$ using CRT.

- Euler's criterion yields only an answer 'yes' or 'no' → quadratic residue or not?

→ does not help us to compute the sq. roots of QRs modulo p.

- ~~$p, q = 3k+3$~~ ~~$p = 3 \bmod$~~.

if $p = 4k_1 + 3$, $q = 4k_2 + 3$

→ ~~gives~~ efficiently computable (sq. roots modulo $n = pq$).

- if $p = 1 \bmod 4$, no known poly-time deterministic algm to compute sq. roots of quadratic residues modulo p. (There is a poly-time Las Vegas algm, however)

Example: $n = 77 = \underset{=p}{7} \times \underset{=q}{11}$

$e_k(x) = x^2 \bmod 77$

$d_k(y) = \sqrt{y} \bmod 77$.

To decrypt $y = 23$

$7 = 4\times 1 + 3$, $\quad 11 = 4\times 2 + 3$

$\therefore$ ~~$(23)^{\frac{p+1}{4}} = \pm 23$~~

$(23)^{\frac{7+1}{4}} = (23)^2 \bmod 7 = 2^2 \bmod 7 = 4 \bmod 7$

$(23)^{\frac{11+1}{4}} = (23)^3 \bmod 11$ ~~$= 2^3 \bmod 7 = \; \bmod 7$~~.

$= 1^3 \bmod 11 = 1 \bmod 11$

Apply CRT

$$\begin{cases} x = \pm 4 \bmod 7 \\ x = \pm 1 \bmod 11 \end{cases}$$

Compute u, v using Extended Euclidean algm.

if $au + bv = 1$
$\downarrow \bmod b$
$au \equiv 1 \pmod b$.
$\Rightarrow u = a^{-1} \bmod b$.

$11 \times x \equiv 1 \bmod 7$
$11 \equiv 4 \bmod 7$
$4x \equiv 1 \bmod 7$
$x \equiv 2 \bmod 7$

$7 \times x \equiv 1 \bmod 11$
$7 \equiv -4 \bmod 11$
$-4x \equiv 1 \bmod 11$
$x \equiv -2 \equiv 9 \bmod 11$

~~$x = 10 \bmod 77$~~

Sol^n. $\pm 10, \pm 32 \bmod 77$.

Idea $x = 4 \times 11 \times y_1 + 1 \times 7 \times y_2 \bmod 77$

$y_1 = 11 \bmod 7$
$11^{-1} \bmod 7$
$11 \equiv 4 \bmod 7$
$4^{-1} \bmod 7$
$4 \times 2 \equiv 1 \bmod 7$
2

$y_2 = 7 \bmod 11$
$7^{-1} \bmod 11$
$7 \times 8 \equiv 1 \bmod 11$
8

$= 4 \times 11 \times 2 + 1 \times 7 \times 8 \bmod 77$
$= 67 \bmod 77$
$= -10 \bmod 77$

$88 - 56 = 32$

$\gcd(7, 11) = 1$
$\Rightarrow 7u + 11v = 1$
$7u \equiv 1 \pmod{11}$
$u = 7^{-1} \bmod 11$

$88 + 56 = 144$
$77 \mid 144 \mid 77$
67

Disadvantage:

- encryption fun. e_K is not injective, so decryption cannot be done in an unambiguous fashion.
- for a valid ciphertext y ($= x^2 \bmod n$ for plaintext $x \in Z_n^*$), there are 4 sq. roots of y modulo n.

  $\Rightarrow$ 4 possible plaintexts that encrypt to y.
- No way for the decrypter to distinguish which of these 4 possible plaintexts is the 'right' plaintext. (unless the plaintext contains sufficient redundancy to eliminate 3 of these possible values).

finding

Sq. root mod $n = pq$ when $p = 2$

$a \equiv x^2 \pmod{2q}$ iff $\begin{cases} a \equiv x^2 \pmod 2 \\ a \equiv x^2 \pmod q \end{cases}$

$\Downarrow$

x is the sq. root of a modulo $n = 2q$.

$\Downarrow$

given a, find x.

- check if $a \in \{0^2, 1^2, 2^2, \ldots, (\frac{q-1}{2})^2\} \pmod q$.
  - if $a \equiv x^2 \pmod q$, then a has unique sq. root mod $2q$ obtained by CRT to solve the system

    i.e. $\sqrt{a} \equiv 0 \pmod q$ $\quad x \equiv 0 \pmod q$

    $x \equiv \sqrt{a} \pmod 2$
  - if $a = x^2 \pmod q$, $x \neq 0$, then a has two sq. roots mod $2q$ obtained by using CRT to solve the system $\begin{cases} x = \sqrt{a} \pmod q \\ x = \sqrt{a} \pmod 2 \end{cases}$ and $\begin{cases} x = -\sqrt{a} \pmod q \\ x \equiv \sqrt{a} \pmod 2 \end{cases}$.

Example:

Find $\sqrt{68} \pmod{86}$.

Ans: 5, 38, 38, 48.

All integers have unique sq. root mod 2.

Example: find $\sqrt{68} \bmod 86$

Soln.

$$86 = 2 \times 43.$$

$$\left.\begin{aligned} 68 &= x^2 \bmod 2 \\ 68 &= x^2 \bmod 43 \end{aligned}\right\}.$$

$68 = x^2 \bmod 2 \Rightarrow x = 0 \bmod 2.$

$68 = x^2 \bmod 43. \Rightarrow x = ? \bmod 43.$

Check whether $68 \in \left\{0^2, 1^2, 2^2, \ldots, \left(\frac{43-1}{2}\right)^2\right\}$. → expensive

Note that — $43 = 4.10 + 3$

$\therefore x = \pm 68^{\frac{43+1}{4}}$ are sq. root of $68 \bmod 43$.

$= \pm 68^{11}$

Calculate 68^{11} (Use fast exponentiation)

$68 = 25 \bmod 43$

$(68)^2 = 25 \times 25 = 23 \bmod 43$

$(68)^2 = 23 \times 23 = 13 \bmod 43.$

$(68)^3 = 13 \times 13 = 40 \bmod 43.$

$\Rightarrow (68)^{11} = 25 \times 23 \times 40$

$= 38 \bmod 43$

$x = \pm 38 \bmod 43.$

Apply CRT

i) $\begin{cases} x = 0 \bmod 2 \\ x = 38 \bmod 43. \end{cases}$

Soln → $x = \{0 \times 43 \times (43^{-1} \bmod 2) + 38 \times 2 \times (2^{-1} \bmod 43)\} \bmod 86$

$= (38 \times 2 \times 22) \bmod 86$

$= 38 \bmod 86.$

$22 \times 2 = 44 = 1 \bmod 43$

$2^{-1} \bmod 43 = 22$

ii) $\begin{cases} x = 0 \bmod 2 \\ x = -38 \bmod 43 = 5 \bmod 43. \end{cases}$

Soln → $x = (5 \times 2 \times 22) \bmod 86$

$= 48 \bmod 86.$

- Fast modular exponentiation (to find high powers).
- Extended Euclidean Algm. (to find modular inverse)

Example: find $\sqrt{23} \bmod 77$ (77 = 7 × 11)

To find x s.t.

$23 = x^2 \bmod 7$

$23 = x^2 \bmod 11$

$7 = 4.1 + 3$

$11 = 4.2 + 3.$

Sq. roots of 23 mod 7 → $x = \pm(23)^{\frac{7+1}{4}} \bmod 7$

Sq. roots of 23 mod 11 → $x = \pm(23)^{\frac{11+1}{4}} \bmod 7.$

i.e. $x = \pm 4 \bmod 7$

$x = \pm 1 \bmod 11.$

Apply CRT $\begin{cases} x = 4 \bmod 7 \\ x = 1 \bmod 11 \end{cases}$

$x = 4.11\,(11^{-1} \bmod 7) + 1.7.(7^{-1} \bmod 11)$

$= 4.11.2 + 1.7.8 = 67 \bmod 77 = -10 \bmod 77$

$\sqrt{y} \bmod n$

$n = pq$

$p, q = 3 \bmod 4.$

$\left(\pm y^{\frac{p+1}{4}}\right)^2 = y^{\frac{p+1}{2}} = y^{\frac{p-1}{2}} \cdot y$

$= y \bmod p$

as by Euler's criterion

Legendre symbol $\left(\frac{y}{p}\right) = y^{\frac{p-1}{2}} \bmod p$

$= 1$ if $y \in QR_p.$

$\pm y^{\frac{p+1}{2}}$ are the sq. roots of $y \bmod p.$

Probabilistic encryption

- encryption is made probabilistic.
  - many possible encryptions of each plaintext
  - not feasible to test whether a given ciphertext is an encryption of a particular plaintext
  - no information about plaintext should be computable from the ciphertext (in poly. time).

Decisional composite residuosity assumption.

← Goldwasser-Micali Probabilistic Public-key encryption

(GM bit encryption)

- $n = pq$, p, q are primes
- $m \in \widetilde{QR}(n)$ i.e. $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$. secret
  pseudosquare mod n
- $P = \{0,1\}$, $C = Z_n^*$, $K = \{(n, p, q, m) : n = pq,$ p, q primes, $m \in \widetilde{QR}(n)\}$
- $p, q \rightarrow$ secret, $m, n \rightarrow$ public

$PK = (m, n)$

$SK = (p, q)$

Encryption Choose $r \in_R Z_n^*$, message $x \in \{0,1\}$

$$e_{PK}(x, r) = m^x r^2 \bmod n$$

Decryption

$$d_{SK}(y) = \begin{cases} 0 & \text{if } y \in QR(n) \\ 1 & \text{if } y \in \widetilde{QR}(n) \end{cases}$$

Correctness On receiving $y \in QR(n) \cup \widetilde{QR}(n)$, decryptor can use his knowledge of factorization of n to determine whether $y \in QR(n)$ or whether $y \in \widetilde{QR}(n)$ by computing:

$$\left(\frac{y}{p}\right) = y^{\frac{p-1}{2}} \bmod p$$

then $y \in QR(n) \iff \left(\frac{y}{p}\right) = 1.$

$n = pq$ $\quad J_n = \{ a \in Z_n^* \mid \left(\frac{a}{n}\right) = 1 \}$.

$= QR(n) \cup \tilde{QR}(n)$

$QR(n)$ ↓ squares mod n ↓ $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$

$\tilde{QR}(n)$ ↓ pseudosquares mod n ↓ $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1.$

- $y \in QR(n) \cup \tilde{QR}(n) \Rightarrow \left(\frac{y}{n}\right) = 1.$

$\therefore y \in QR(n) \iff \left(\frac{y}{p}\right) = 1.$

- Security: ⓐ $n = pq$ & $\left(\frac{y}{n}\right) = +1$ given

DCR (Dec. composite residuosity)

Decide whether $y \in QR(n)$ or not

- Homomorphic property: if C_0, C_1 → encryptions of m_0, m_1 then $C_0 C_1$ → encryption of $m_0 \oplus m_1$
- Applicable to complex design more crypto primitive.