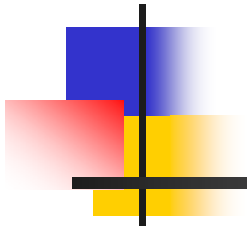
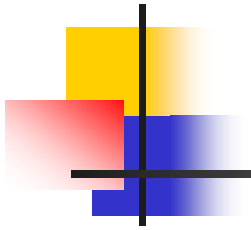


Chapter 11
Quadratic Residues

邱錫彥　老師



Contents

11.1 QR and NQR

Def: If $m \in Z^+$, the integer a is a quadratic residues of m if $(a, m) = 1$ and $x^2 = a \pmod{m}$ has a solution . If $x^2 = a \bmod m$ has no solution , we say a is a quadratic nonresidue of m .

Remark : The set of all quadratic residues of m is demoted by QR_m and the test of all quadratic nonresidue of m is denoted by NOR_m .

Ex : Let $m = 11$

$1^2 = 10^2 = 1 \bmod 11$, $2^2 = 9^2 = 4$, $3^2 = 8^2 = 9$,

$4^2 = 7^2 = 5$,$5^2 = 6^2 = 3$,

$\therefore QR_{11} = \{ 1, 3, 4, 5, 9 \}$, $NQR_{11} = \{ 2, 6, 7, 8, 10 \}$

Problem : Given m and a , how can we determine that $a \in QR_m$ or $a \in NQR_m$?

Lemma : Let p be odd prime and $p \nmid a$, then $x^2 = a \bmod p$ (1) has either no solutions or exactly two incongruent solutions modulo p .

Proof :

(a) If (1) had a solution , then there are two solutions . If x_0 is a solution of (1) , then $-x_0$ is a second in congruent solution . $\because (-x_0)^2 = (x_0)^2 = a$ and $x_0 \neq -x_0 \pmod p$

(b) There are no more than two incongruent solutions.

Assume that x_0 and x_1 are both solutions of $x^2 = a \bmod p$, then

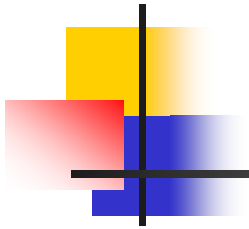
$$x_0^2 = x_1^2 = a \bmod p$$

$$\rightarrow x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) = 0 \bmod p$$

$$\rightarrow p \mid (x_0 + x_1) \; or \quad p \mid (x_0 - x_1)$$

$$\rightarrow x_1 = -x_0 \bmod p \quad or \quad x_1 = x_0 \bmod p$$

$\therefore$ If (1) has a solution , there are exactly two incongruent solution .



Thm : If p is an odd prime m,

then $|QR_p| = |NQR_p| = (p-1)/2$

Proof : we compute $1^2, 2^2, \ldots\ldots, (p-1)^2 \bmod p$, there are p-1 squares to consider and each $x^2 = a \bmod p$, has either zero or two solutions . .∴. $|QR_p| = (p-1)/2$.

Def : Legendre symbol

Let p be an odd prime and $p \nmid a$ ($a \neq 0 \bmod p$) .
The Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \; if \; a \in QR_p \\ -1 \; if \; a \in NQR_p \end{cases}$$

Problem : Given a and p , how to compute (a/p) (or Does a $\in QR_p$?)

Thm : Euler's criterion

Let p be an odd prime and let a be a positive integer not divisible by p. Then

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

Proof :

1. If $a \in QR_p$, then $\exists\, x$, $\ni x^2 = a \bmod p$.

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

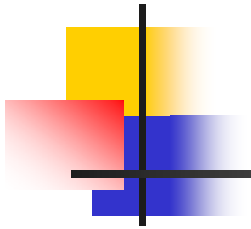
Hence , if $\left(\frac{a}{p}\right) = 1$, then $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$.

2. If $a \in NQR_p$, $x^2 = a \bmod p$ has no solution .
However , for each i , $1 \le i \le p\text{-}1$, $\exists$ a unique integer j , $1 \le i \le p\text{-}1$, $\ni$ $ij = a \bmod p$ and $i \neq j$. We group the integers 1, 2,……, p-1 into (p-1)/2 pairs each with product a . Multiplying these pairs together ,

$$(p-1)! = a^{\frac{p-1}{2}} \bmod p$$

$$(p-1)! = -1 \bmod p \text{ (Wilson's theorem)}$$

$$\therefore a^{\frac{p-1}{2}} = -1 \bmod p, \text{ if } a \in NQR_p.$$

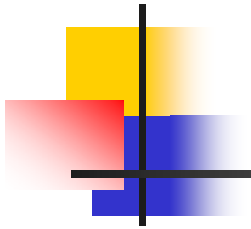


Thm : let p be an odd prime and $a \neq 0 \bmod p$, $b \neq 0 \bmod p$. Then

1. If $a = b \bmod p$, then $(a/p) = (b/p)$
2. $(a/p)(b/p) = (ab/p)$
3. $(a^2/p) = 1$

Proof :

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



Remark : property (2) can be restated as

$$QR \cdot QR = QR$$
$$NQR \cdot QR = NQR$$
$$NQR \cdot NQR = QR$$

THM : If p is an odd prime , then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, p = 1 \bmod 4 \\ -1, p = -1 \bmod 4 \left(= 3 \bmod 4\right) \end{cases}$$

Proof : If $p = 1 \bmod 4$, then $p = 4k + 1$ for some $k \in Z^+$,

thus $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$$

If p = -1 mod 4 , then $p = 4k+3$ for some $k \in Z^+$, thus

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

Thm : Gauss' Lemma

Let p be an odd prime and a an integer with $(a, p) = 1$.
If s is the number of least positive residues of the integers a , $2a$, $3a$, ……, $((p-1)/2)a$ that are greater than $p/2$, then $[a/p]=(-1)^s$

Ex : let $a = 5$, $p = 11$, then $1 \times 5 = 5$; $2 \times 5 = 10$; $3 \times 5 = 4$; $4 \times 5 = 9$; $5 \times 5 = 3 \bmod 11$. $p/2 = 5.5$, $\therefore$ $s = 2$ → $(5/11) = (-1)^2 = 1$.

Remark : If $i \cdot a = u \bmod p$ and $u > p/2$, replace u by $p-u$, then ,

$$\left\{a, 2a, \cdots\cdots, \frac{p-1}{2}a\right\} = \left\{1, 2, \cdots\cdots, \frac{p-1}{2}\right\}$$

Ex : $1 \times 5 = 5$, $2 \times 5 = 10$ → 1 , $3 \times 5 = 4$ → 9 , $4 \times 5 = 9$ →2 , $5 \times 5 = 3$.

- Proof :
  - Let u_1 , u_2 , ……, u_s be integers of the sequence $a, 2a, \ldots\ldots, \frac{p-1}{2}a$ that are larger than $p/2$. And v_1 , v_2, ……v_t be integers of the sequence , $a, 2a, \ldots\ldots, \frac{p-1}{2}a$ that are less than $p/2$. Then

$$\{p-u_1, p-u_2, \ldots\ldots, p-u_s, v_1, v_2, \ldots\ldots v_t\} = \left\{1, 2, \ldots\ldots, \frac{p-1}{2}\right\}.$$

1. $s + t = (p\text{-}1)/2$, if $u_i = u_j \bmod p$ (or $v_i = v_j \bmod p$) , then $i_a = j_a \bmod p \rightarrow i = -j$, it is impossible since i , $j < (p\text{-}1)/2$

2. $p - u_i \neq v_j$, if $p - u_i = v_j \bmod p$, then ,$ia = p - ja = -ja \bmod p \rightarrow i = -j$, it is impossible since i , $j < (p-1)/2$.

ψ Thus

$$(p-u_1)(p-u_2).....(p-u_s)v_1v_2.....v_t = \left(\frac{p-1}{2}\right)!a^{\frac{p-1}{2}}$$

or $(-1)^s u_1u_2.....u_sv_1v_2.....v_t = \left(\frac{p-1}{2}a\right) \bmod p$

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

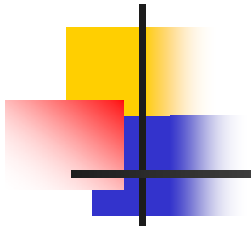
$$\rightarrow \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^s \bmod p$$

- Thm : if p is an odd prime , then $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

- Proof : In the sequence $1\times 2, 2\times 2, \ldots\ldots, \left(\frac{p-1}{2}\right)\times 2$ there are $[p/4]$ integers less than $p/2$, thus

$$s=\frac{p-1}{2}-\left[\frac{p}{4}\right]$$

where [ ] is a floor function . Now we wish to show that $\frac{p-1}{2}-\left[\frac{p}{4}\right]=\frac{p^2-1}{8} \mod 2.$



i. $p = 1 \bmod 8 = 8k+1$, then

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k - 2k = 2k = 0 \bmod 2$$

$$\frac{p^2-1}{8} = \frac{64k^2+16k+1-1}{8} = 0 \bmod 2$$

ii. $p = 8k+3$, then

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k+1-2k = 1 \bmod 2$$

$$\frac{p^2-1}{8} = \frac{64k^2+48k+9-1}{8} = 1 \bmod 2$$

iii. $p = 8k+5$, then

$$\frac{p-1}{2}-\left[\frac{p}{4}\right]=4k+2-2k-1=1 \bmod 2$$

$$\frac{p^2-1}{8}=\frac{64k^2+80k+25-1}{8}=1 \bmod 2$$

iv. $p = 8k+7$, then

$$\frac{p-1}{2}-\left[\frac{p}{4}\right]=4k+3-2k-1=0 \bmod 2$$

$$\frac{p^2-1}{8}=\frac{64k^2+112k+49-1}{8}=0 \bmod 2$$

$$\therefore \left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}-\left[\frac{p}{4}\right]}=(-1)^{\frac{p^2-1}{8}}$$

- Remark :
  1. If $p = 1 \bmod 8$ or $7 \bmod 8$, then $(2/p) = 1$or $2 \in QR_p$
  2. If $p = 3 \bmod 8$ or $5 \bmod 8$, then $(2/p) = -1$or $2 \in NQR_p$
- Let $n = pq$, the product of two distinct primes p and q .
- If $x^2 = a \bmod n$ has a solution $x = x_0$, then there are exactly four incongruent solutions modulo n .

- Proof : let $x_0 = x_1 \bmod p$ and $x_0 = x_2 \bmod q$

$$x^2 = a \bmod n \rightarrow \begin{cases} x^2 = a \bmod p \\ x^2 = a \bmod q \end{cases}$$

If implies that x_1 and $p - x_1$ is the solutions of $x^2 = a \bmod p$.

If implies that x_2 and $q - x_2$ is the solutions of $x^2 = a \bmod q$.

- By CRT , there are exactly four incongruent solutions of $x^2 = a \bmod n$ satisfying .

$$\left.\begin{aligned} x &= x_1 \bmod p \\ x &= x_2 \bmod q \end{aligned}\right\} \rightarrow M_1 \qquad \left.\begin{aligned} x &= p - x_1 \bmod p \\ x &= x_2 \bmod p \end{aligned}\right\} \rightarrow M_3$$

$$\left.\begin{aligned} x &= x_1 \bmod p \\ x &= q - x_2 \bmod q \end{aligned}\right\} \rightarrow M_2 \qquad \left.\begin{aligned} x &= p - x_1 \bmod p \\ x &= q - x_2 \bmod q \end{aligned}\right\} \rightarrow M_4$$

- Note that $M_1 = -M_4 \bmod n$ and $M_2 = -M_3 \bmod n$

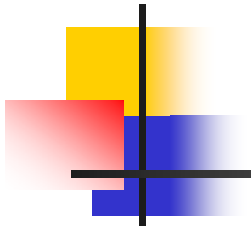
- Problem :
  1. If $a \in QR_p$, how to find $x \ni x^2 = a \bmod p$?
  2. Given $n = pq$ and $a \in QR_n$, can we find a solution $x \ni x^2 = a \bmod n$ without knowing p and q ?
- Sol :

1. a) If $p = 3 \bmod 4$ (or $p = 4k + 3$) , then

$$x = a^{\frac{p+1}{4}} \bmod p \ , \left(a^{\frac{p+1}{4}} \right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}+1} = a \bmod p$$

b) If $p = 1 \bmod 4$, there is an efficient algorithm (probabilistic) to find x (Refer to 近代密碼學及其應用).∴Given p and $a \in QR_p$, find $x \ni x^2 = a \bmod p$ is feasible.

2. If there is an algorithm to find $x \ni x^2 = a \bmod n$, then we first choose M randomly and compute $M^2 = a \bmod m$, then put a and n as the input of the algorithm and obtain the output M' from the algorithm . If $M \neq \pm M' \bmod n$, then $(M+M', n) = p$ or q . $M^2 - (M')^2 = (M-M')(M+M') = 0 \bmod n$

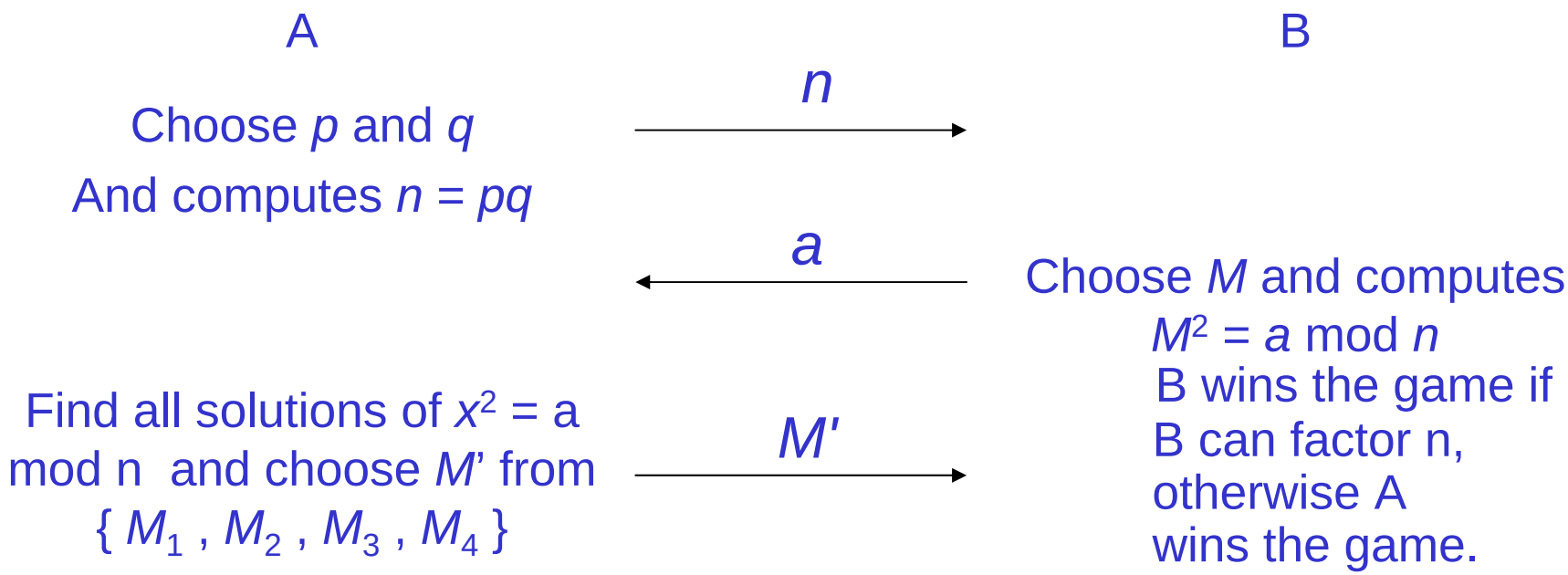


$\therefore n \mid (M-M')(M+M')$ but $n \nmid (M-M')$ and $n \nmid (M+M')$, $(M \neq \pm M' \bmod n) \rightarrow p \mid (M-M')$, $q \mid (M+M')$ or $q \mid (M-M')$, $p \mid (M+M')$

$\therefore$ Given $n = pq$ and $a \in QR_n$, finding $x \ni x^2 = a \bmod n$ is equivalent to factor n . (infeasible) . But if we know p and q , then finding x is feasible.

- Flopping coins electronically :
  - Object : A and B play a protocol by an electrical channel and when the protocol finishes , both A and B have only ½ probability to win the game .

Protocol :



- If $M' \neq \pm M \mod n$, then B can factor n , the probability = ½

11.2 The law of quadratic reciprocity

- Let *p* and *q* are distinct odd primes , if we know (*q/p*)can we know (*p/q*) ?
- The answer was found by Euler by examining numerical evidence . Legendre refoumulated Euler's answer as the law of quadratic reciprocity , but he cannot give a correct proof . Guess provided the first correct proof when he was 18 years old . Now , there are more than 152 proofs of the law of quadratic reciprocity by different approaches .
- Thm : the law of quadratic reciprocity let *p* and *q* be odd primes . Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\bullet\frac{q-1}{2}}$$

or $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & p = 1 \bmod 4 \text{ or } q = 1 \bmod 4 \text{ or both} \\ -1, & p = 3 = q \bmod 4 \end{cases}$$

- The law of reciprocity can be used to evaluate Legendre symbols , if prime factorization can be computed .
- Ex : calculate (713/1009) . Note that 1009 is prime and 713 = 23 $\times$ 31.
- Sol :

1. $\left(\frac{713}{1009}\right)=\left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$

2. $\left(\frac{23}{1009}\right)=\left(\frac{1009}{23}\right),\left(\frac{31}{1009}\right)=\left(\frac{1009}{31}\right),\left(\because 1009=1 \bmod 4\right)$

3. $\left(\frac{1009}{23}\right)=\left(\frac{20}{23}\right)=\left(\frac{2^3\cdot 5}{23}\right)=\left(\frac{5}{23}\right)=\left(\frac{23}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1$

$\left(\frac{1009}{31}\right)=\left(\frac{17}{31}\right)=\left(\frac{31}{17}\right)=\left(\frac{14}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)=\left(\frac{17}{7}\right)=\left(\frac{3}{7}\right)$

$=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1$

4. $\therefore \left(\frac{713}{1009}\right) = (-1)(-1) = 1$

- Before we prove above theorem , we first show the following Lemma.
- Lemma : If *p* is an odd prime and *a* is an odd integer not divisible by *p* , then

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)} \text{ , where } T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left[ja \mid p\right]$$

- Proof : consider a , $2a$, …… , $\frac{p-1}{2}a \pmod p$, let u_1 , u_2 , …… , us be those greater than $p/2$. Then

$$ja = p\left[\frac{ja}{p}\right] + \text{remainder},$$

$$\text{where remainder} \in \{u_1, u_2, \ldots, u_s\} \text{ or } \{v_1, v_2, \ldots, v_t\}$$

$$\therefore \sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j \qquad (1)$$

From Guess' Lemma we know that

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{s} (p - u_j) + \sum_{j=1}^{t} v_j \qquad (2)$$

$$(1)-(2)\rightarrow(a-1)\sum_{j=1}^{\frac{p-1}{2}} j=\sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right]-ps+2\sum_{j=1}^{s} u_j$$

$$=pT(a,p)-ps+2\sum_{j=1}^{s} u_j \qquad (3)$$

Since a and p are odd , we have

$$O=T(a,p)-s \bmod 2$$

$$\therefore T(a,p)=s \bmod 2$$

From Guess' Lemma , $\left(\frac{a}{p}\right)=(-1)^2 \rightarrow \left(\frac{a}{p}\right)=(-1)^{T(a,p)}$

if a is odd .

- Ex : Using above lemma to evaluate (7/11) .
- Sol :

$$\sum_{j=1}^{5}\left[\frac{7j}{11}\right]=\left[\frac{7}{11}\right]+\left[\frac{14}{11}\right]+\left[\frac{21}{11}\right]+\left[\frac{28}{11}\right]+\left[\frac{35}{11}\right]=7 \;\therefore\left[\frac{7}{11}\right]=(-1)^7=-1$$

- Ex : Let p = 7 and q = 11 . Consider (x , y) with $1 \le x \le \left(\frac{7-1}{2}\right)=3$ and $1 \le y \le \left(\frac{11-1}{2}\right)=5$.
- There are 15 pairs .

  (1,1) , (2,1) , (3,1) , (1,2) , (2,2) , (3,2) ,(1,3) , (2,3) , (3,3) , (1,4) , (2,4) , (3,4) , (1,5) , (2,5) , (2,5) , (3,5)

- How many pairs in these pairs satisfy $11x > 7y$ and $11x < 7y$?
- Sol : if $11x > 7y$, then $1 \le y \le {}^{11x}\!/_{7}$. For fixed x , there are $\left[{}^{11x}\!/_{7}\right]$ pairs . So the total number of pairs is

$$\sum_{j=1}^{3}\left[\frac{11j}{7}\right]=\left[\frac{11}{7}\right]+\left[\frac{22}{7}\right]+\left[\frac{33}{7}\right]=1+3+4=8$$

- If $11x < 7y$, then $1 \le x \le {}^{7y}\!/_{11}$. For fixed y , there are $\left[{}^{7y}\!/_{11}\right]$ pairs . So the total number of pairs is

$$\sum_{j=1}^{5}\left[\frac{5j}{11}\right]=\left[\frac{7}{11}\right]+\left[\frac{14}{11}\right]+\left[\frac{21}{11}\right]+\left[\frac{28}{11}\right]+\left[\frac{35}{11}\right]=0+1+1+2+3=7$$

- Consequently , we see that

$$\frac{11-1}{2}\cdot\frac{7-1}{2}=5\times 3=15=\sum_{j=1}^{3}\left[\frac{7j}{11}\right]+\sum_{j=1}^{5}\left[\frac{7j}{11}\right]=8+7.$$

From above Lemma , we have

$$\left[\frac{11}{7}\right]\times\left[\frac{7}{11}\right]=(-1)^{\sum_{j=1}^{3}\frac{11j}{7}}=(-1)^{\frac{11-1}{2}\cdot\frac{7-1}{2}}$$

- Proof of the law of quadratic reciprocity :
  - Consider pairs of integers (x,y) with $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le {}^{p-1}\!/_{2}$

- Then divide the $\frac{p-1}{2}\cdot\frac{q-1}{2}$ pairs into two groups such that $qx > py$ and $qx < py$. (Note that $qx \neq py$; p,q are distinct primes and $1 \le x \le {}^{p-1}\!/_{2}$, $1 \le y \le {}^{q-1}\!/_{2}$)

Then there are $\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{qj}{p}\right]$ pairs satisfying $qx > py$ and $\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{pj}{q}\right]$ pairs astisfying $qx < py$

Since $\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{qj}{p}\right]+\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{pj}{q}\right]=T(q,p)+T(p,q)=\frac{p-1}{2}\cdot\frac{q-1}{2}$

By above Lemma , we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(p,q)}(-1)^{T(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

- Application : use the law of quadratic reciprocity to prove the validity of primality test for Fermat numbers .
- Thm : Pepin's Test

$$\text{The Fermat number } F_m = 2^{2^m} + 1 \text{ is prime iff}$$

$$3^{\frac{F_m - 1}{2}} = -1 \bmod F_m$$

- Proof :

($\rightarrow$) If $3^{\frac{F_m-1}{2}} = -1 \bmod F_m$, then $3^{F_m-1} = 1 \bmod F_m$.

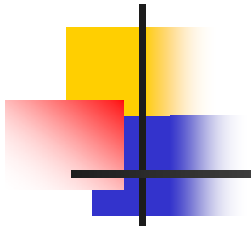
If there exist a prime $p, \ni\ p \mid F_m$, then $3^{F_m-1} = 1 \bmod p$

and hence $ord_p 3 \mid (F_m - 1) = 2^{2^m}$. However,

$$ord_p 3 \nmid 2^{2^{m-1}} = \frac{F_m - 1}{2}$$

Since $3^{\frac{F_m-1}{2}} = -1 \bmod F_m \rightarrow ord_p 3 = F_m - 1 \leq p - 1$

and $p \mid F_m. \rightarrow p = F_m, \therefore F_m$ must be prime.



($\leftarrow$) If F_m is prime, then

$$\left(\frac{3}{F_m}\right)=\left(\frac{F_m}{3}\right)=\left(\frac{2}{3}\right)=-1.\Theta F_m=1\bmod 4$$

and $F_m=2\bmod 3$

$$\text{for } m\geq 1.\therefore\left(\frac{3}{F_m}\right)=3^{\frac{F_m-1}{2}}\bmod F_m\rightarrow 3^{\frac{F_m-1}{2}}$$

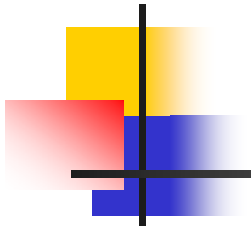
$$=-1\bmod F_m$$

11.3 The Jacobi Symbol

- Def : let $n \in Z^+$ be an odd integer with $n = p_1^{t1}$, p_2^{t2} , ……, p_m^{tm} and let $a \in Z^+$ and (a,n) = 1 , then , the Jacobi symbol $J(a/n)$ is defined by

$$J\left(\frac{a}{n}\right) = J\left(\frac{a}{p_1^{t_1} p_2^{t_2} \ldots\ldots p_m^{t_m}}\right) = \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2} \ldots\ldots \left(\frac{a}{p_m}\right)^{t_m}$$

- Remark :
  1. When n is prime , then $J(a/n) = (a/n)$
  2. When $x^2 = a \bmod n$ has solutions , then $J(a/n) = 1$. However , $J(a/n) = 1$ does not imply that $a \in QR_n$, i.e. $x^2 = a \bmod n$ has solutions.



- Ex : let $a = 2$ and $n = 3 \times 5 = 15$, note that $J(2/15) = (2/3)(2/5) = (-1)(-1) = 1$, but there are no solutions to $x^2 = 2 \bmod 15$, since $x^2 = 2 \bmod 3$ and $x^2 = 2 \bmod 5$ has no solutions .
- Properties of Jacobi symbol :

$$1.\ \text{If } a = b \bmod n, \text{ then } J\left(\frac{a}{n}\right) = J\left(\frac{b}{n}\right)$$

$$2.\ J\left(\frac{ab}{n}\right) = J\left(\frac{a}{n}\right)J\left(\frac{b}{n}\right)$$

$$3.\ J\left(\frac{-1}{n}\right) = (-1)^{\frac{p-1}{2}}$$

$$4.\ J\left(\frac{2}{n}\right) = (-1)^{\frac{p^2-1}{8}}$$

- Proof of (3) :

$$J\left(\frac{-1}{n}\right)=\left(\frac{-1}{p_1}\right)^{t_1}\left(\frac{-1}{p_2}\right)^{t_2}.....\left(\frac{-1}{p_m}\right)^{t_m} \quad \text{by definition}$$

$$=(-1)^{\frac{t_1(p_1-1)}{2}+\frac{t_2(p_2-1)}{2}+.....+\frac{t_m(p_m-1)}{2}}$$

$$\text{But } n=\left[1+(p_1-1)\right]^{t_1}\left[1+(p_2-1)\right]^{t_2}.....\left[1+(p_m-1)\right]^{t_m}$$

$$\because\ p_i-1 \text{ is even , we have } \left[1+(p_i-1)\right]^{t_i}=1+t_i(p_i-1)\bmod 4.$$

$$\text{and } (1+t_i(p_i-1))(1+t_j(p_j-1))=1+t_i(p_i-1)+t_j(p_j-1)\bmod 4.$$

$$\therefore \frac{n-1}{2}=t_1\frac{p_1-1}{2}+t_2\frac{p_2-1}{2}+...t_m\frac{p_m-1}{2}\bmod 2\rightarrow J\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$$

- Thm : the Reciprocity law for Jacobi symbols . Let (*n*,*m*) = 1 and *n* , *m* are odd positive integers , then

$$J\left(\frac{n}{m}\right)J\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

- Ex : find $J\left(\frac{401}{111}\right)$
- Sol : $401 = 111 \times 3 + 2^2 \times 17$

$111 = 17 \times 6+2^5 \times 9$

$17 = 9 \times 1+2^5 \times 1$

$$J\left(\frac{401}{111}\right)=J\left(\frac{2^2\cdot 17}{111}\right)=J\left(\frac{2^2}{111}\right)J\left(\frac{17}{111}\right)=J\left(\frac{2}{111}\right)^2 J\left(\frac{17}{111}\right)=(-1)^{2\cdot\frac{111^2-1}{8}}\cdot J\left(\frac{17}{111}\right)$$

$$J\left(\frac{17}{111}\right)=(-1)^{\frac{17-1}{2}\cdot\frac{111-1}{2}}J\left(\frac{111}{17}\right)=(-1)^{\frac{17-1}{2}\cdot\frac{111-1}{2}}J\left(\frac{2^0}{17}\right)J\left(\frac{9}{17}\right)$$

$$=(-1)^{\frac{17-1}{2}\cdot\frac{111-1}{2}}(-1)^{0\cdot\frac{111-1}{2}}J\left(\frac{9}{17}\right)$$

$$J\left(\frac{9}{17}\right)=(-1)^{\frac{9-1}{2}\cdot\frac{17-1}{2}}J\left(\frac{17}{9}\right)=(-1)^{\frac{9-1}{2}\cdot\frac{17-1}{2}}J\left(\frac{2}{9}\right)^3=(-1)^{\frac{9-1}{2}\cdot\frac{17-1}{2}}(-1)^{3\cdot\frac{9^2-1}{8}}$$

$$\therefore J\left(\frac{401}{111}\right)=(-1)^{2\cdot\frac{111^2-1}{8}+\frac{17^2-1}{8}+3\cdot\frac{9^2-1}{8}+\frac{17-1}{2}\cdot\frac{111-1}{2}+\frac{9-1}{2}\cdot\frac{17-1}{2}}=1$$

- Now, there exist an efficient algorithm for evaluating Jacobi symbols $J(a/b)$. Let (a , b) = 1 and a , b are odd positive integers

1. Let $R_0 = a$ and $R_1 = b$. Using the division algorithm and factoring out the highest power of two dividing the remainder,

$$R_0 = R_1 q_1 + 2^{s_1} R_2 \qquad R_2 < R_1$$

$$R_1 = R_2 q2 + 2^{t_2} R3 \qquad R_3 < R_2$$

$$\vdots \qquad\qquad \vdots$$

$$R_{n-3} = R_{n-2} q_{n-2} + 2^{s_{n-2}} R_{n-1} \qquad R_{n-1} < R_{n-2}$$

$$R_{n-2} = R_{n-1} q_{n-1} + 2^{s_{n-1}} \cdot 1$$

2. Then

$$J\left(\frac{a}{b}\right) = (-1)^{s_1 \frac{R_1^2}{8} + \cdots + s_{n-1} \frac{R_{n-1}^2}{8} + \frac{R_1 - 1}{2}\frac{R_2 - 1}{2} + \cdots + \frac{R_{n-2} - 1}{2}\frac{R_{n-1} - 1}{2}}$$

- Remark :
  1. In above algorithm we do not need to factor *a* or *b* .
  2. If (*a, b*) = 1 , then *J*(*a*/*b*) can be evaluated using $O((\log_2 b)^3)$ bit operations .

11-4 Euler Psudoprimes

- Def : *n* is a pseudoprime to the base *b* if *n* is composite and $b^n = b \bmod n$ (or $b^{n-1} = 1 \bmod n$)
- Def : *n* is a strong pseudopirme to the base *b*

  if *n* is composite

  and either $b^t = 1 \bmod n$ or $b^{2^j t} = -1 \bmod n$ for some

  $0 \le j \le s-1$, where $n-1 = 2^s t$ and t is odd

  (Miller's test)

- Def : *n* is *a* Carmichael number if

Fact : if p is an odd prime and $p \nmid b$, then we have

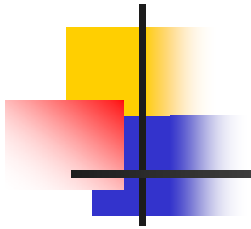
$b^{\frac{p-1}{2}} = \left(\frac{b}{p}\right) = J\left(\frac{b}{p}\right) \bmod p$, thus , if given n and

$\exists (b,n) = 1 \ni b^{\frac{n-1}{2}} \neq J\left(\frac{b}{n}\right) \bmod n$, then n must be composite .

Problem : Do there exist some composite nubmers n , such that the above test is satisfied ?

Def : an odd composite , positive integer n that satisfies

$b^{\frac{n-1}{2}} = J\left(\frac{b}{n}\right) \bmod n$, where b is a positive integer , then



n is called an Euler pseudoprime to the base b.

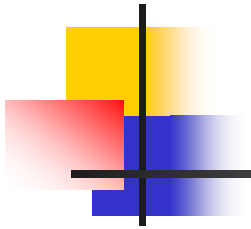
Thm : if n is an Euler pseudoprime to the base b , then n is a pseudo prime to the base b .

Proof : if n is an Euler pseudoprime to the base b , then

$$b^{\frac{p-1}{2}} = J\left(\frac{b}{n}\right) \bmod n \rightarrow b^{n-1} = \left(J\left(\frac{b}{n}\right)\right)^2 = 1 \bmod n.$$

$\therefore n$ is a pseudoprime to the base b.

Remark : Not every pseudoprime is an Euler pseudoprime .



Thm : if n is a strong pseudoprime to the base b, then n is an Euler pseudoprime to this base.

Proof : Omitted .

Remark : not every Euler pseudoprime is a strong pseudorime.

Ex : Let $n = 341$ and $b = 2$ (n is composite)

(1) $2^{340} = 1 \bmod 341 \rightarrow 341$ is pseudoprime to the base 2 .

(2) $2^{170} = 1 \bmod 341$, and $J\left(\frac{2}{341}\right) = (-1)^{\frac{n^2-1}{8}} = (-1) \rightarrow 341$

is not an Euler pseudoprime to the base 2 .

Ex : let $n = 1105$ and $b = 2$(n is composite)

(1) $2^{552} = 1 \bmod 1105$, and $J\left(\frac{2}{1105}\right) = (-1)^{\frac{1105^2-1}{8}} = 1 \rightarrow 1105$

is an Euler pseudoprime to base 2 .

(2) $2^{552} = 1 \bmod 1105$ but $2^{\frac{1105-1}{2^2}} = 2^{276} = 781 \neq 1 \bmod 1105$

$\rightarrow 1105$ is not a strong pseudoprime .

Thm : if $n = 3 \bmod 4$ andn is an Euler pseudoprime to the base b , then n is a strong pseudoprime to the base b .

proof : if $n = 3 \bmod 4$, then $n - 1 = 2t$, there t is odd .

$\because$ n is an Euler

pseudoprime to the base b , $\therefore b^t = b^{\frac{n-1}{2}} = J\left(\frac{b}{n}\right) \bmod n$

if $J\left(\frac{b}{n}\right) \rightarrow = -1$, then $b^{2^{s-1}t} = -1 \bmod n$

$\rightarrow n$ is a strong pseudoprime .

Lemma : If n is an odd positive integer and is not a perfect square , then $\exists b \in Z^+$, with $(b, n) = 1$ and $J\left(\frac{b}{n}\right) = -1.$

Proof : (1) if n is prime , then b exists .

(2) if n is composite and is not a perfect square ,

we write $n = rs$ where p is an odd prime and t is odd .

let $t \in NQR_p$, t exists . let $b = t \bmod r$ $\quad b = 1 \bmod s$

Then $J\left(\frac{b}{r}\right) = J\left(\frac{b}{p^t}\right) = \left(J\left(\frac{b}{p}\right)\right)^t = -1$ and $J\left(\frac{b}{s}\right) = 1$

$\therefore J\left(\frac{b}{n}\right) = J\left(\frac{b}{r}\right)J\left(\frac{b}{s}\right) = -1 \rightarrow b$ exists .

Lemma : Let n be an odd composite integer .

Then $\exists b$ with $(b,n)=1$ and $b^{\frac{n-1}{2}} \neq J\left(\frac{b}{n}\right) \bmod n$

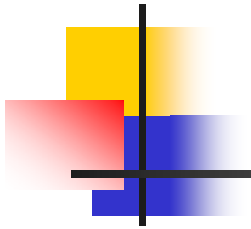
Proof : Assume that $\forall b, 1<b<n, (b,n)=1,$ satisfy

$b^{\frac{n-1}{2}} = J\left(\frac{b}{n}\right) \bmod n$ Then $b^{n-1} = \left(J\left(\frac{b}{n}\right)\right)^2 = (\pm 1)^2 = 1 \bmod n$

n is an odd composite integer ,

$\therefore n$ must be a Carmichael number $\rightarrow n = q_1 q_2 \ldots\ldots q_r$,

where $q_1 q_2 \ldots\ldots q_r$ are istinct odd primes .



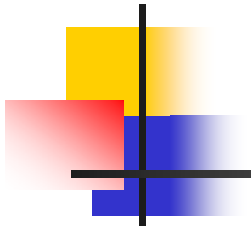
In this case $b^{\frac{n-1}{2}} = 1 \bmod n$ must be hold for all $1 \le b \le n-1$ and $(b,n) = 1$. If $b^{\frac{n-1}{2}} = -1 \bmod n$, then we can find an integer a,

$(a,b) = 1$ э $a = b \bmod q_1$ $\quad a = 1 \bmod (q_1 q_2 \ldots\ldots q_r)$

$\rightarrow a^{\frac{n-1}{2}} \neq b^{\frac{n-1}{2}} = -1 \bmod q_1$ and $a^{\frac{n-1}{2}} = 1 \bmod (q_1 q_2 \ldots q_r)$

$\rightarrow a^{\frac{n-1}{2}} \neq \pm 1 \bmod n$, It is a contradiction $\therefore b^{\frac{n-1}{2}} = 1 \bmod n$

$= J\left(\frac{b}{n}\right)$, for all $(b,n) = 1$.

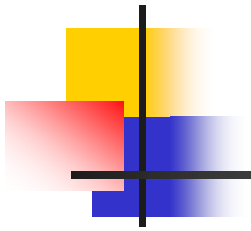


However , above Lemma tells us that this is impossible ,

since $\exists b \ni J\left(\frac{b}{n}\right) = -1 \bmod n$. There must be at least one

integer $b, (b,n) = 1 \ni b^{\frac{n-1}{2}} \neq J\left(\frac{b}{n}\right) \bmod n$

Thm : Let n be an odd composite integer , Then the number of bases b which n is an Euler pseudoprime does not exceed $\frac{\Phi(n)}{2}$.



Proof : let b with $1 < b < n, (b, n) = 1$ and $b^{\frac{n-1}{2}} \neq J\left(\frac{b}{n}\right) \bmod n.$

(b must be existed from above Lemma)

Let $a_1 a_2 \ldots\ldots a_m$ denoted the positive integers less than n

satisfying $1 \leq a_j \leq n, (a_j, n) = 1$ and $a_j^{\frac{n-1}{2}} = J\left(\frac{a_j}{n}\right) \bmod n,$

for $j = 1, 2, \ldots\ldots, m.$

Let $r_1 r_2 \ldots\ldots r_m$ satisfy $r_j = a_j b \bmod n.$ Then the integers

$r_j^{\frac{n-1}{2}} \neq J\left(\frac{r_j}{n}\right) \bmod n.$

If it is true , then

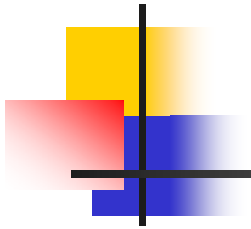
$$r_j^{\frac{n-1}{2}} = (a_j b)^{\frac{n-1}{2}} = a_j^{\frac{n-1}{2}} = J\left(\frac{a_j}{n}\right) J\left(\frac{b}{n}\right) \bmod n$$

$$\rightarrow b^{\frac{n-1}{2}} = J\left(\frac{b}{n}\right) \bmod n .$$

Thus $S_1 = \{a_1, \ldots, a_n\}, S_2 \{r_1, r_2, \ldots, r_m\}, S_1 \cap S_2 = \Phi$

$$\rightarrow 2m \le \Phi(n) \rightarrow m \le \frac{\Phi(n)}{2}$$

Thm : the Solovay - Strassen probabilistic primality test .



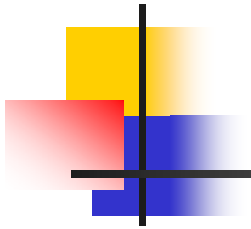
Let n be a positive integer , select b from $\{1,2,...,n-1\}$.

Determinewhether $b^{\frac{n-1}{2}} = J\left(\frac{b}{n}\right) \bmod n.$

If it is fails then n is composite . If n is composite ,

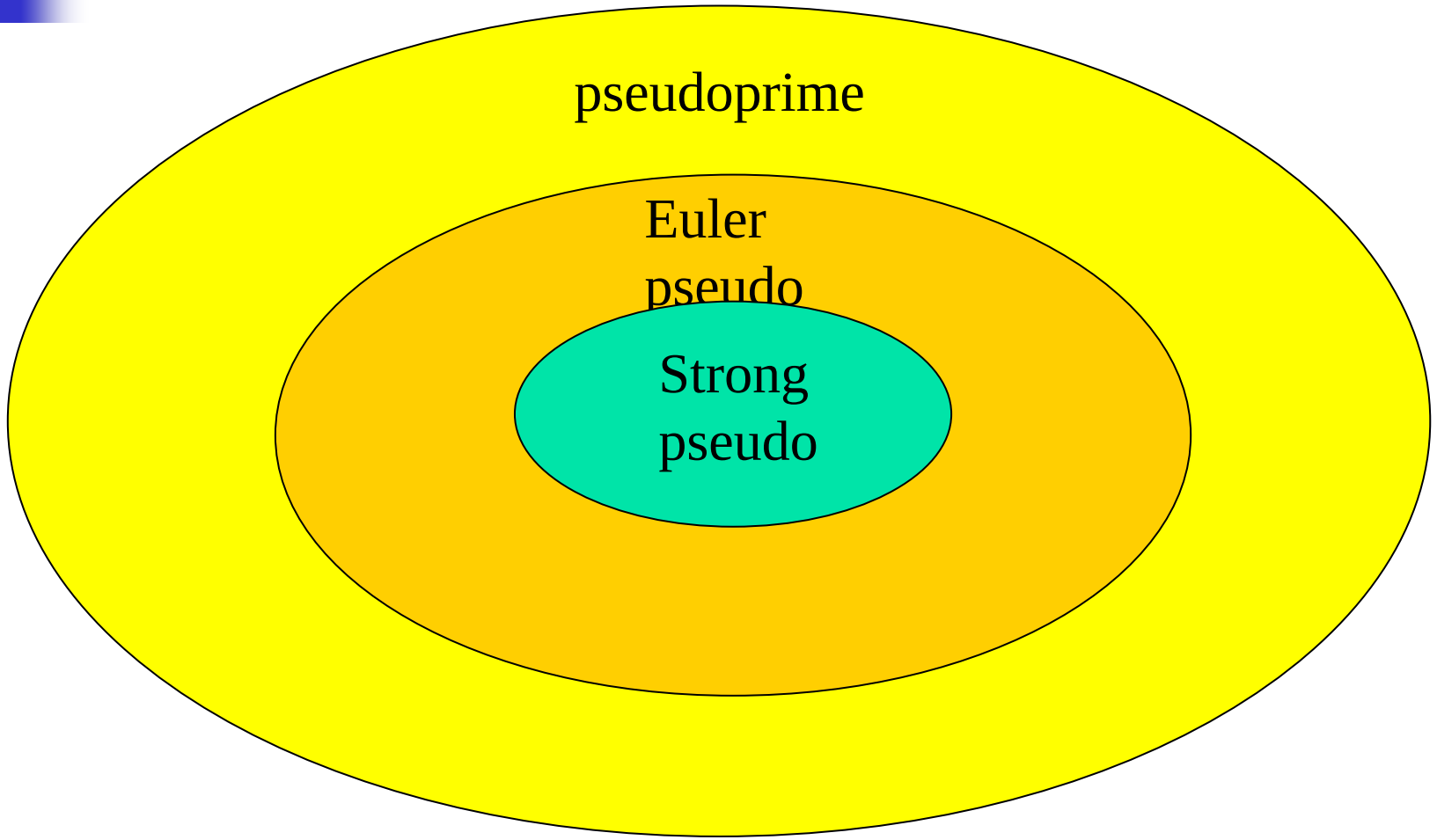
then the probability that it holds is less than $\frac{1}{2}$.

Repeat the k times , the probability that n is composite and passes the test is less then $\frac{1}{2^k}$



Remark :

1. The complexity of the Solovay - Strassen probalbilistic primality test is $O\left(k\left(\log_2 n\right)^3\right)$ bit operations which is the same as the Rabin test .
2. The Solovay - Strassen test is less efficient than the Rabin test


pseudoprime
Euler
pseudo
Strong
pseudo