Q

Quadratic residues

Q.1 Legendre symbol

Let

- p be an *odd* prime, $p > 2$,
- g any generator of $\mathbb{Z}_p^\star$.

Remark Q.1. If $a \in \mathbb{Z}_p^\star$ is a square, *id est* there is $b \in \mathbb{Z}_p^\star : b^2 = a$ then a has precisely two roots b and $-b \neq b \pmod p$. In fact, if we denote $f : \mathbb{Z}_p^\star \to \mathbb{Z}_p^\star$ the morphism defined by $f(a) = a^2$, since its kernel $\ker(f) = \{1, -1\}$ satisfies $\# \ker(f) = 2$, we know that

$$\operatorname{Im}(f) = \left\{b^2 : b \in \mathbb{Z}_p^\star\right\} = \mathbb{Z}_p^\star / \ker(f)$$

so that $\# \operatorname{Im}(f) = \frac{p-1}{2}$ and each coset $f^{-1}(a) = \{b : b^2 = a\}$, $a \in \operatorname{Im}(f)$ has 2 elements.

If we choose, as canonical representative of $\mathbb{Z}_p$ the set

$$\{a : -\frac{p}{2} < a < \frac{p}{2}\} \subset \mathbb{Z}$$

then one of the roots has a positive representative, the other a negative representative.

If we instead choose as canonical representative of $\mathbb{Z}_p$ the set

$$\{a : 0 \leq a \leq p-1\} \subset \mathbb{Z}$$

one of the roots has an odd representative, the other an even representative. □

Definition Q.2. Let p be an *odd* prime, $p > 2$. An element $a \in \mathbb{Z}_p^\star$ is called a *quadratic residue modulo* p iff $a \in \operatorname{Im}(f)$, a *nonresidue* if $a \notin \operatorname{Im}(f)$.

We will denote $Q_p \subset \mathbb{Z}_p^\star$ the set $Q_p := \operatorname{Im}(f)$ of the quadratic residues modulo p and $\bar{Q}_p \subset \mathbb{Z}_p^\star$ the set $\bar{Q}_p := \mathbb{Z}_p^\star \setminus Q_p$ of the nonquadratic residues .

The quadratic residuosity/nonresiduosity can be also characterized in terms of any generator g of $\mathbb{Z}_p^\star$:

Lemma Q.3. *$a = g^j$ is a quadratic residue if and only if j is even.*

Proof. $\operatorname{Im}(f) = \left\{b^2 : b \in \mathbb{Z}_p^\star\right\} = \left\{(g^j)^2 : 1 \leq j < p\right\} = \left\{g^{2j} : 1 \leq j < p\right\}.$ □

Example Q.4. Let $p = 11$ and $g = 2$ Then we have

j	1	2	3	4	5	6	7	8	9	10
$-\frac{p}{2} < g^j < \frac{p}{2}$	2	4	−3	5	−1	−2	−4	3	−5	1
$0 \leq g^j \leq p-1$	2	4	8	5	10	9	7	3	6	1

$0 \leq a \leq p-1$						0	1	2	3	4	5	6	7	8	9	10
$-\frac{p}{2} < a < \frac{p}{2}$	−5	−4	−3	−2	−1	0	1	2	3	4	5					
$\operatorname{ind}(a)$	9	7	3	6	5	∗	10	1	8	2	4	9	7	3	6	5

$\pm b$	$\{b, p-b\}$	$a = b^2$	$\operatorname{ind}(a)$
±1	{1, 10}	1	10
±2	{2, 9}	4	2
±3	{3, 8}	−2	6
±4	{4, 7}	5	4
±5	{5, 6}	3	8

Thus the quadratice residues are $Q_{11} := \{4, 5, -2, 3, 1\}$ and the nonresidue $\bar{Q}_{11} := \{2, -3, -1, -4, -5\}$
Moreover we have

$a \in Q_{11}$	1	4	-2	5	3
$0 < \sqrt{a} < \frac{p}{2}$	1	2	3	4	5
$-\frac{p}{2} < -\sqrt{a} < 0$	-1	-2	-3	-4	-5
odd $\sqrt{a}$	1	9	3	7	5
even $\sqrt{a}$	10	2	8	4	6
$\text{ind}(a)$	10	2	6	4	8

□

Example Q.5. Analogously

- for $p = 5, g = 2$ we have :

$\pm b$	$\{b, p-b\}$	$a = b^2$	$\text{ind}(a)$
± 1	$\{1, 4\}$	1	4
± 2	$\{2, 3\}$	-1	2

  so that the quadratice residues are $Q_5 := \{\pm 1\}$ and the nonresidue $\bar{Q}_5 := \{\pm 2\}$.

- while for $p = 7, g = 3$[1] we obtain

j	1	2	3	4	5	6
$-\frac{p}{2} < g^j < \frac{p}{2}$	3	2	-1	-3	-2	1
$0 \le g^j \le p-1$	3	2	6	4	5	1

$0 \le a \le p-1$				0	1	2	3	4	5	6
$-\frac{p}{2} < a < \frac{p}{2}$	-3	-2	-1	0	1	2	3			
$\text{ind}(a)$	4	5	3	$*$	6	2	1	4	5	3

$\pm b$	$\{b, p-b\}$	$a = b^2$	$\text{ind}(a)$
± 1	$\{1, 6\}$	1	6
± 2	$\{2, 5\}$	-3	4
± 3	$\{3, 4\}$	2	2

  Thus the quadratice residues are $Q_7 := \{2, -3, 1\}$ and the nonresidue $\bar{Q}_7 := \{3, -1, -2\}$.

□

Definition Q.6. Let p be an *odd* prime, $p > 2$ and $a \in \mathbb{Z}$. We define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is quadratic residue modulo } p \\ -1 & \text{if } a \text{ is nonresidue modulo } p \end{cases}$$

Proposition Q.7. *(Euler's Criterion)* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Proof. If $p \mid a$, $a^{(p-1)/2} = 0$.
If $p \nmid a$ and $a = g^j$, a is a residue iff j is even, $j = 2h$, iff $h(p-1) = \frac{j(p-1)}{2}$ iff $p-1 \mid \frac{j(p-1)}{2}$ iff $a^{(p-1)/2} = g^{j(p-1)/2} = 1$.
□

Corollary Q.8. *If $p \equiv 3 \pmod 4$ and $a \in Q_p$ its roots are $\pm a^{\frac{(p+1)}{4}}$.*

Proof. We have $\left(\pm a^{\frac{(p+1)}{4}}\right)^2 = a^{\frac{(p+1)}{2}} = a^{\frac{(p-1)}{2}} \cdot a = \left(\frac{a}{p}\right) a = a$. □

Proposition Q.9. *The Legendre symbol satisfies the following properties:*

(1) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(3) $\gcd(b, p) = 1 \implies \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

[1] $2^3 = 8 \equiv 1 \pmod 7$ so that 2 is not a generator.

(4) $\left(\frac{1}{p}\right) = 1$

(5) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Proof. (1) and (4) are trivial; (2) and (5) follow directly form Euler's Criterion.
Ad (3): $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$. □

Lemma Q.10. *For any odd integer* $m = 2k+1$, $\frac{m^2-1}{8} = \frac{k^2+k}{2} \in \mathbb{N}$

Proof. We have $\frac{m^2-1}{8} = \frac{4(k^2+k)}{8} = \frac{k^2+k}{2}$ which is an integer because $k(k+1)$ is necessarily even for each k. □

Proposition Q.11. *It holds:*

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

Proof. Since

$$\frac{p^2-1}{8} = \frac{p+1}{2} \cdot \frac{p-1}{2} \cdot \frac{1}{2} = \frac{\left(\frac{p-1}{2}+1\right)\left(\frac{p-1}{2}\right)}{2} = \binom{\frac{p-1}{2}}{2} = \sum_{k=1}^{\frac{p-1}{2}} k$$

we have

$$(-1)^{(p^2-1)/8} \prod_{k=1}^{\frac{p-1}{2}} k = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} k} \prod_{k=1}^{\frac{p-1}{2}} k = \prod_{k=1}^{\frac{p-1}{2}} (-1)^k k = \prod_{\substack{k=1 \\ k \text{ even}}}^{\frac{p-1}{2}} k \prod_{\substack{k=1 \\ k \text{ odd}}}^{\frac{p-1}{2}} -k \equiv \prod_{\substack{k=1 \\ k \text{ even}}}^{\frac{p-1}{2}} k \prod_{\substack{k=1 \\ k \text{ odd}}}^{\frac{p-1}{2}} (p-k) = \prod_{k=1}^{\frac{p-1}{2}} 2k = 2^{(p-1)/2} \prod_{k=1}^{\frac{p-1}{2}} k$$

and we obtain the claim dividing out $\prod_{k=1}^{\frac{p-1}{2}} k$. □

Fact Q.12. *For any two odd primes* p, q, *it holds*

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

Q.2 Jacobi symbol

The definition of Legendre symbol was generalized to the case of any integer a and any odd integer n.

Definition Q.13. Let n be an *odd* integer and $n = \prod_{i=1}^{r} p_i^{a_i}$ its prime factorization. For any $a \in \mathbb{Z}$ we define the *Jacobi symbol*

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{a_i}.$$

Lemma Q.14. *Let* $s, t \in \mathbb{N}$ *be odd. Then:*

$$\frac{s-1}{2} + \frac{t-1}{2} \equiv \frac{st-1}{2} \pmod 2$$

and

$$\frac{s^2-1}{8} + \frac{t^2-1}{8} \equiv \frac{s^2t^2-1}{8} \pmod 2$$

Proof. For $s = 2s'+1$ and $t = 2t'+1$, we have $st = 4s't' + 2(s'+t') + 1 = 2(2s't' + s' + t') + 1$ whence

$$\frac{st-1}{2} = 2s't' + (s'+t') \equiv s'+t' = \frac{s-1}{2} + \frac{t-1}{2} \pmod 2.$$

and

$$\frac{s^2t^2-1}{8} = \frac{(2s't'+s'+t')^2 + (2s't'+s'+t')}{2} \equiv \frac{(s'+t')^2 + (s'+t')}{2} \equiv \frac{s'^2+s'}{2} + \frac{t'^2+t'}{2} = \frac{s^2-1}{8} + \frac{t^2-1}{8} \pmod 2.$$

□

Corollary Q.15. *Let n be an* odd *integer, $n = \prod_{i=1}^r p_i^{a_i}$ its prime factorization. Then*

$$\frac{n-1}{2} \equiv \sum_{i=1}^{r} \frac{p_i - 1}{2} a_i \pmod 2 \text{ and } \frac{n^2-1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2 - 1}{8} a_i \pmod 2$$

□

Proposition Q.16. *The Jacobi symbol satisfies the following properties:*

(1) $a \equiv b \pmod n \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

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

(3) $\gcd(b, n) = 1 \implies \left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right)$;

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

(5) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$

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

(7) *for any two odd integers m, n, it holds* $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod 4 \\ \left(\frac{n}{m}\right) & \text{otherwise.} \end{cases}$

Proof. (1-4) are trivial.

Ad (5): $\left(\frac{-1}{n}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right)^{a_i} = \prod_{i=1}^r (-1)^{\frac{p_i-1}{2}a_i} = (-1)^{\sum_{i=1}^r \frac{p_i-1}{2}a_i} = (-1)^{\frac{n-1}{2}}$.

Ad (6): $\left(\frac{2}{n}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right)^{a_i} = \prod_{i=1}^r (-1)^{\frac{p_i^2-1}{8}a_i} = (-1)^{\sum_{i=1}^r \frac{p_i^2-1}{8}a_i} = (-1)^{\frac{n^2-1}{8}}$.

Ad (7): If $\gcd(m, n) \neq 1$ then, by definition $\left(\frac{m}{n}\right) = 0 = \left(\frac{n}{m}\right)$. Otherwise let $m = \prod_{i=1}^r p_i^{a_i}$ and $n = \prod_{j=1}^s q_j^{b_i}$ be their prime factorizations.

We have

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)^{a_i b_j} = \pm \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)^{a_i b_j} = \pm \left(\frac{n}{m}\right)$$

Denote

- $I := \{i : 1 \leq i \leq r : p_i \equiv 3 \pmod 4\}$
- $\iota := \sum_{i \in I} a_i$
- $J := \{j : 1 \leq j \leq s : q_j \equiv 3 \pmod 4\}$
- $\kappa := \sum_{j \in J} b_j$
- $L := \{(i, j) : 1 \leq i \leq r, 1 \leq j \leq s : p_i \equiv q_j \equiv 3 \pmod 4\} = \{(i, j) : i \in I, j \in J\}$
- $\lambda := \sum_{(i,j) \in L} a_i b_j = \sum_{\substack{i \in I \\ j \in J}} a_i b_j = \left(\sum_{i \in I} a_i\right)\left(\sum_{j \in J} b_j\right) = \iota\kappa$

and remark that $\left(\frac{m}{n}\right) = (-1)^\lambda \left(\frac{n}{m}\right) = (-1)^{\iota\kappa}\left(\frac{n}{m}\right)$ so that $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ if and only if both ι and κ are odd.

Also we have

$$m = \prod_{i=1}^{r} p_i^{a_i} = \prod_{\substack{i=1 \\ i \in I}}^{r} p_i^{a_i} \prod_{\substack{i=1 \\ i \notin I}}^{r} p_i^{a_i} \equiv \prod_{\substack{i=1 \\ i \in I}}^{r} (-1)^{a_i} = (-1)^\iota \pmod 4$$

and, with the same argument, $n \equiv (-1)^\kappa \pmod 4$. Since $m \equiv n \equiv 3 \pmod 4$ if and only if both ι and κ are odd, we obtain the claim. □

Procedure Q.17. (1),(6),(7) allows to compute the Jacoby simbols in an efficient way whose complexity is comparable with the one of the euclidean algorithm. Given $m, n \in \mathbb{N} \setminus \{0\}$

- Set $m' := m, n' := n, \lambda := 1$
- While $\lambda \neq 0$ and $m' \neq 1$ do

- %% $\left(\frac{m}{n}\right) = \lambda\left(\frac{m'}{n'}\right)$
- If $m' = 0$ set $\lambda := 0$.
- If $2 \mid m'$
  * let $k, r : m' = 2^k r$
  * set $\lambda := (-1)^{k(n'^2-1)/8}\lambda, m' := r$
- If $2 \nmid m', m' < n'$ set $\lambda := (-1)^{(m'-1)(n'-1)/4}, u := m', m' := n', n' := u$;
- If $2 \nmid m', m' \geq n'$ set $m' := \mathbf{Rem}(m', n')$

□

Example Q.18. Let $m := 2468, n := 13579 = 37 \star 367$ We have

- $2468 = 2^2 \star 617$, $13579 \equiv 3 \pmod 8$, $\left(\frac{2468}{13579}\right) = (-1)^2\left(\frac{617}{13579}\right) = \left(\frac{617}{13579}\right)$
- $617 \not\equiv 3 \pmod 4$, $\left(\frac{617}{13579}\right) = \left(\frac{13579}{617}\right)$
- $\mathbf{Rem}(13579, 617) = 5$, $\left(\frac{13579}{617}\right) = \left(\frac{5}{617}\right)$
- $617 \not\equiv 3 \pmod 4$, $\left(\frac{5}{617}\right) = \left(\frac{617}{5}\right)$,
- $\mathbf{Rem}(617, 5) = 2$, $\left(\frac{617}{5}\right) = \left(\frac{2}{5}\right)$
- $5 \equiv -3 \pmod 8$ $\left(\frac{2}{5}\right) = -1, \lambda := -1$

so that $\left(\frac{2468}{13579}\right) = -1$.

Remark that

- $2468 = 2^2 \star 617$, $367 \equiv -1 \pmod 8$, $\left(\frac{2468}{367}\right) = 1^2\left(\frac{617}{367}\right) = \left(\frac{617}{367}\right)$
- $\mathbf{Rem}(617, 367) = 250$, $\left(\frac{617}{367}\right) = \left(\frac{250}{367}\right)$
- $250 = 2 * 125$, $367 \equiv -1 \pmod 8$, $\left(\frac{250}{367}\right) = 1\left(\frac{125}{367}\right) = \left(\frac{125}{367}\right)$,
- $125 \not\equiv 3 \pmod 4$, $\left(\frac{125}{367}\right) = \left(\frac{367}{125}\right)$
- $\mathbf{Rem}(367, 125) = 117$, $\left(\frac{367}{125}\right) = \left(\frac{117}{125}\right)$
- $125 \not\equiv 3 \pmod 4$, $\left(\frac{117}{125}\right) = \left(\frac{125}{117}\right)$,
- $\mathbf{Rem}(125, 117) = 8$, $\left(\frac{125}{117}\right) = \left(\frac{8}{117}\right)$
- $117 \equiv -3 \pmod 8$, $\left(\frac{8}{117}\right) = (-1)^3\left(\frac{1}{117}\right), \lambda := -1$

whence $\left(\frac{2468}{367}\right) = -1$ and

- $2468 = 2^2 \star 617$, $37 \equiv -3 \pmod 8$, $\left(\frac{2468}{37}\right) = (-1)^2\left(\frac{617}{37}\right) = \left(\frac{617}{37}\right)$
- $\mathbf{Rem}(617, 37) = 25$, $\left(\frac{617}{37}\right) = \left(\frac{25}{37}\right)$
- $37 \not\equiv 3 \pmod 4$, $\left(\frac{25}{37}\right) = \left(\frac{37}{25}\right)$
- $\mathbf{Rem}(37, 25) = 12$, $\left(\frac{37}{25}\right) = \left(\frac{12}{25}\right)$
- $12 = 2^2 \star 3, 25 \equiv 1 \pmod 8$, $\left(\frac{12}{25}\right) = 1^2\left(\frac{3}{25}\right) = \left(\frac{3}{25}\right)$
- $25 \not\equiv 3 \pmod 4$, $\left(\frac{3}{25}\right) = \left(\frac{25}{3}\right)$
- $\mathbf{Rem}(25, 3) = 1$, $\left(\frac{25}{3}\right) = \left(\frac{1}{3}\right) = 1$

whence $\left(\frac{2468}{37}\right) = 1$.

Remark that we have

$$\left(\frac{2468}{37}\right) = \left(\frac{617}{37}\right) = \left(\frac{25}{37}\right) = \left(\frac{37}{25}\right) = \left(\frac{12}{25}\right) = \left(\frac{3}{25}\right) = \left(\frac{25}{3}\right) = \left(\frac{1}{3}\right) = 1$$

but

$$\left(\frac{1234}{37}\right) = -\left(\frac{617}{37}\right) = -\left(\frac{25}{37}\right) = -\left(\frac{37}{25}\right) = -\left(\frac{12}{25}\right) = -\left(\frac{3}{25}\right) = -\left(\frac{25}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

□

Q.3 Square root modulo p

Given

- p be an *odd* prime, $p > 2$,
- $a \in Q_p$ any quadratic residue $\mathbb{Z}_p^\star$.

we want to compute a value $x \in \mathbb{Z} : x^2 \equiv a \pmod{p}$. In order to do so let us set

- $e, s : p - 1 = 2^e s$, s odd,
- $n \in \bar{Q}_s$ any non-quadratic residue modulo p[2]
- $b := n^s \pmod{p}$
- $r := a^{\frac{s+1}{2}} \pmod{p}$

Lemma Q.19. *With the present notation b is a primitive 2^e-th root of unity.*

Proof. In fact $b^{2^e} \equiv n^{s2^e} = n^{p-1} \equiv 1 \pmod{p}$

If b were not primitive, then $1 \equiv b^{2^\epsilon} \pmod{p}$ for some $\epsilon < e$ which implies that b is an even power of a primitive 2^e-th root of unity, whence $b \in Q_p$ contradicting $\left(\frac{b}{p}\right) = \left(\frac{n}{p}\right)^s = (-1)^s = -1$. □

Lemma Q.20. *With the present notation $(a^{-1}r^2)^{2^{e-1}} = 1$.*

Proof. $(a^{-1}r^2)^{2^{e-1}} = a^{s2^{e-1}} = a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = 1$ □

Algorithm Q.21 (Andleman–Manders–Miller). Since $\frac{r^2}{a}$ is a 2^{e-1}-th root of unity modulo p, our aim is to modify r via a suitable power $b^j, 0 \le j < 2^e$, of the primitive 2^e-th root of unity in order to get $x := b^j r : \frac{x^2}{a} \equiv 1 \pmod{p}$ as required.

Remark that if $j, 0 \le j < 2^{e-1}$ is s.t. $(b^j r)^2 \equiv a \pmod{p}$, then, since $b^{2^{e-1}} = -1$, the other square root is $-x = -1 \cdot b^j r = b^{2^{e-1}} b^j r = b^{j+2^{e-1}} r$.

Thus our aim is to determine the unique values $j_0, j_1, \ldots, j_{e-2} \in \{0, 1\}$ under which

$$j := \sum_{i=0}^{e-2} j_i 2^i = j_0 + 2j_1 + 4j_2 + \ldots + 2^{e-2} j_{e-2}$$

satisfies $(b^j r)^2 \equiv a \pmod{p}$.

We already remarked that $t := (a^{-1}r^2)^{2^{e-2}}$ satisfies $t^2 = (a^{-1}r^2)^{2^{e-1}} = 1$ so that $t = \pm 1$.

Thereofore if we set $j_0 := \begin{cases} 0 & \text{if } t = 1 \\ 1 & \text{if } t = -1 \end{cases}$ we have

$$(a^{-1}(b^{j_0} r)^2)^{2^{e-2}} = (b^{j_0})^{2^{e-1}} t = \begin{cases} t & \text{if } t = 1 \\ b^{2^{e-1}} t = -t & \text{if } t = -1 \end{cases}$$

whence $\frac{(b^{j_0} r)^2}{a}$ is a 2^{e-2}-th root of unity.

Assume now we have already found $j_0, j_1, \ldots, j_{h-1}$ such that

$$j' := \sum_{i=0}^{h-1} j_i 2^i = j_0 + 2j_1 + 4j_2 + \ldots + 2^{h-1} j_{h-1}$$

satisfies $(a^{-1}(b^{j'} r)^2)^{2^{e-h-1}} = 1$ so that $\frac{(b^{j'} r)^2}{a}$ is a 2^{e-h-1}-th root of unity. Let us compute $t := (a^{-1}(b^{j'} r)^2)^{2^{e-h-2}} = \pm 1$ and set $j_h := \begin{cases} 0 & \text{if } t = 1 \\ 1 & \text{if } t = -1 \end{cases}$ so that in both case $(a^{-1}(b^{j'+2^h j_h} r)^2)^{2^{e-h-2}} = 1$ and $\frac{(b^{j'+2^h j_h} r)^2}{a}$ is a 2^{e-h-2}-th root of unity.

When finally we get $h = e - 2$ then

$$j := \sum_{i=0}^{e-2} j_i 2^i = j_0 + 2j_1 + 4j_2 + \ldots + 2^{e-2} j_{e-2}$$

satisfies $\frac{(b^j r)^2}{a} = a^{-1}(b^j r)^2 = 1$ and $b^j r$ and $b^{j+2^{e-1}} r$ are the two square roots of a. □

[2] it is sufficient to pick up any random integer $n, \gcd(n, p) = 1$ and test $\left(\frac{n}{p}\right)$ to obtain such a number with probabily 2^{-1}.

Q.4 Williams and Blum integers

Let

- $m \in \mathbb{N} \setminus \{0\}$ be an odd integer;
- $m = \prod_{i=1}^{r} p_i^{a_i}$ its prime factorization.

We can extend in this setting the notion of *quadratic residues*; actually we can give the following

Definition Q.22. Let $m \in \mathbb{N} \setminus \{0\}$ be an odd integer. Any element $a \in \mathbb{Z}_m^\star$ is called a *quadratic residue modulo m* iff there is $b \in \mathbb{Z}_p^\star : b^2 = a$.

We will denote $Q_m \subset \mathbb{Z}_m^\star$ the set of the quadratic residues modulo m and $\bar{Q}_m \subset \mathbb{Z}_m^\star$ the set of the nonquadratic residues. □

but, unlike the Legendre symbol $\left(\frac{a}{p}\right)$, p prime, the Jacobi symbol $\left(\frac{a}{m}\right)$ does not reveal whether or not a is a quadratic residue modulo n.

Remark Q.23. More exactly, if a is a quadratic residue, then[3] $\left(\frac{a}{m}\right) = 1$; however, $\left(\frac{a}{m}\right) = 1$ does not imply that a is a quadratic residue. □

Lemma Q.24. *There are 2^r square roots of the unity in $\mathbb{Z}_m$.*

Proof. ± 1 are the only distinct square roots of the unity in each field $\mathbb{Z}_{p_i^{a_i}}$ and the 2^r Chinese Remainder problems

$$x \equiv \pm 1 \pmod{p_i^{a_i}}$$

give all the distinct square roots of the unity in $\mathbb{Z}_m$. □

Corollary Q.25. *If a is a quadratic residue modulo m, then a has 2^r square roots.* □

Proof. If we denote $f : \mathbb{Z}_m^\star \to \mathbb{Z}_m^\star$ the morphism defined by $f(a) = a^2$, we know that

$$\mathrm{Im}(f) = \left\{ b^2 : b \in \mathbb{Z}_p^\star \right\} = \mathbb{Z}_p^\star / \ker(f)$$

so that each coset $f^{-1}(a) = \{b : b^2 = a\}$, $a \in \mathrm{Im}(f)$, has $\# \ker(f) = 2^r$ elements. □

Let us now specialize ourselve to a squarefree integer n which is the product of two distinct primes:

- p, q be distint two primes,
- $n := pq$.

Definition Q.26. The integer $n = pq, p \neq q$, is called

- a *Williams integer* if $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$;
- a *Blum integer* if $p \equiv q \equiv 3 \pmod 4$. □

Remark Q.27. If n is a Blum integer then necessarily both $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd. □

Let

- $a \in Q_n$ be a quadratic residue and let
- $b_p, -\frac{p}{2} < b_p < \frac{p}{2} : a \equiv b_p^2 \pmod p$
- $b_q, -\frac{q}{2} < b_q < \frac{q}{2} : a \equiv b_q^2 \pmod q$

where, up to this moment, b_p and b_q have been chosen randomly among the two possible choices. Then the 4 square roots modulo n are

- $x_1, -\frac{n}{2} < x_1 < \frac{n}{2}$ s.t. $x_1 \equiv b_p \pmod p, x_1 \equiv b_q \pmod q$
- $x_2, -\frac{n}{2} < x_2 < \frac{n}{2}$ s.t. $x_2 \equiv -b_p \pmod p, x_2 \equiv -b_q \pmod q$

[3] In fact

$$a \equiv b^2 \pmod m \implies a \equiv b^2 \pmod{p_i} \text{ for each } i \implies \left(\frac{a}{p_i}\right) = 1 \text{ for each } i \implies \left(\frac{a}{m}\right) = \prod_i \left(\frac{a}{p_i}\right)^{a_i} = 1.$$

– $x_3, -\frac{n}{2} < x_3 < \frac{n}{2}$ s.t. $x_3 \equiv b_p \pmod{p}, x_3 \equiv -b_q \pmod{q}$

– $x_4, -\frac{n}{2} < x_4 < \frac{n}{2}$ s.t. $x_4 \equiv -b_p \pmod{p}, x_4 \equiv b_q \pmod{q}$;

remark that $x_1 = -x_2$ and $x_3 = -x_4$ while $x_1 \neq \pm x_3$.

Lemma Q.28 (Williams)**.** *If the prime p satisfies $p \equiv 3 \pmod{4}$ then*

1. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$;
2. $\left(\frac{-b_p}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b_p}{p}\right) = -\left(\frac{b_p}{p}\right)$.
3. *Among the two square roots (Corollary Q.8) $\pm a^{\frac{(p+1)}{4}}$ of a quadratic residue $a \in Q_p$, just one of them is a quadratic residue too.* □

Let us now assume that n is a Blum integer; then we can wlog assume that $b_p \in Q_p$ is the square roots of a which is a quadratic residue modulo p and that $b_q \in Q_q$ is the square roots of a which is a quadratic residue modulo q and we can consequently rename the 4 square roots modulo n as

– $x := x_1$ satisfying $x \equiv b_p \pmod{p}, x \equiv b_q \pmod{q}$,

– $y := x_3$ satisfying $y \equiv b_p \pmod{p}, y \equiv -b_q \pmod{q,}$

so that

– $-x = x_2$ satisfies $-x \equiv -b_p \pmod{p}, -x \equiv -b_q \pmod{q}$,

– $-y = x_4$ satisfies $-y \equiv -b_p \pmod{p}, -y \equiv b_q \pmod{q}$.

Lemma Q.29 (Williams)**.** *With the present notation we have:*

- $\left(\frac{x}{p}\right) = \left(\frac{b_p}{p}\right) = 1$, $\left(\frac{x}{q}\right) = \left(\frac{b_q}{q}\right) = 1$, $\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right) = 1$.
- $\left(\frac{-x}{p}\right) = \left(\frac{-b_p}{p}\right) = -1$, $\left(\frac{-x}{q}\right) = \left(\frac{-b_q}{q}\right) = -1$, $\left(\frac{-x}{n}\right) = \left(\frac{-x}{p}\right)\left(\frac{-x}{q}\right) = 1$.
- $\left(\frac{y}{p}\right) = \left(\frac{b_p}{p}\right) = 1$, $\left(\frac{y}{q}\right) = \left(\frac{-b_q}{q}\right) = -1$, $\left(\frac{y}{n}\right) = \left(\frac{y}{p}\right)\left(\frac{y}{q}\right) = -1$.
- $\left(\frac{-y}{p}\right) = \left(\frac{-b_p}{p}\right) = -1$, $\left(\frac{-y}{q}\right) = \left(\frac{b_q}{q}\right) = 1$, $\left(\frac{-y}{n}\right) = \left(\frac{-y}{p}\right)\left(\frac{-y}{q}\right) = -1$. □

Theorem Q.30 (Williams)**.** *If $n = pq$ is a Blum integer and $a \in Q_n$ is a quadratic residue modulo n, then*

1. *there are $x, y \in \mathbb{Z}_n^\star, x \neq y : x^2 = y^2 = a$;*
2. $\left(\frac{\pm x}{n}\right) = -\left(\frac{\pm y}{n}\right)$.
3. *Assuming wlog that $\left(\frac{x}{n}\right) = 1$ (and therefore $\left(\frac{y}{n}\right) = -1$) the following conditions are equivalent*
   (a) $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1$;
   (b) $x^{(p-1)(q-1)/4} \equiv 1 \pmod{n}$;
   (c) $\left(\frac{-x}{p}\right) = \left(\frac{-x}{q}\right) = -1$;
   (d) $(-x)^{(p-1)(q-1)/4} \equiv -1 \pmod{n}$.

Proof. (1) and (2) just summarize the remarks above.

Ad (3):

$(a) \implies (b)$ Since $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1$ we have, by Euler's Criterion,

$$x^{(p-1)(q-1)/4} = (x^{(p-1)/2})^{(q-1)/2} \equiv \left(\frac{x}{p}\right)^{(q-1)/2} = 1^{(q-1)/2} = 1 \pmod{p}$$

and

$$x^{(p-1)(q-1)/4} = (x^{(q-1)/2})^{(p-1)/2} \equiv \left(\frac{x}{q}\right)^{(p-1)/2} = 1^{(p-1)/2} = 1 \pmod{q}$$

whence $x^{(p-1)(q-1)/4} \equiv 1 \pmod{n}$.

$(b) \implies (a)$ By assumption we have $x^{(p-1)(q-1)/4} \equiv 1 \pmod p$ and $x^{(p-1)(q-1)/4} \equiv 1 \pmod q$. Since $n = pq$ is a Blum integer, both $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd and such is also $\frac{(p-1)(q-1)}{4}$. Therefore

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

and

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

$(a) \iff (c)$ is a trivial consequence of $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = -1$

$(b) \iff (d)$ is a trivial consequence of the fact that $\frac{(p-1)(q-1)}{4}$ is odd.

$(c) \implies (d)$ While the proof is complete, I consider helpful to develop the argument which is obtained by adapting the one used for $(a) \implies (b)$.

Since $\left(\frac{-x}{p}\right) = \left(\frac{-x}{q}\right) = -1$ we have, by Euler's Criterion,

$$(-x)^{(p-1)(q-1)/4} = ((-x)^{(p-1)/2})^{(q-1)/2} \equiv \left(\frac{-x}{p}\right)^{(q-1)/2} = (-1)^{(q-1)/2} = -1 \pmod p$$

and

$$(-x)^{(p-1)(q-1)/4} \equiv \left(\frac{-x}{q}\right)^{(p-1)/2} = (-1)^{(p-1)/2} = -1 \pmod q$$

whence $x^{(p-1)(q-1)/4} \equiv -1 \pmod n$.

$(d) \implies (c)$ By assumption we have $(-x)^{(p-1)(q-1)/4} \equiv -1 \pmod p$ and $(-x)^{(p-1)(q-1)/4} \equiv -1 \pmod q$; since $\frac{(p-1)(q-1)}{4}$ is odd,

$$\left(\frac{-x}{p}\right) = \left(\frac{-x}{p}\right)^{(p-1)(q-1)/4} = \left(\frac{(-x)^{(p-1)(q-1)/4}}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}} = -1$$

and

$$\left(\frac{-x}{q}\right) = \left(\frac{-x}{q}\right)^{(p-1)(q-1)/4} = \left(\frac{(-x)^{(p-1)(q-1)/4}}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{(q-1)}{2}} = -1.$$

□

Proposition Q.31. *If $n = pq$ is a Blum integer and $a \in Q_n$ is a quadratic residue modulo n, $a^{\frac{(p-1)(q-1)+4}{8}}$ is the single root of a which is a quadratic residue.*

Proof. The Theorem above imples that, among the four rooots of $a \in Q_n$, one and only one is a quadratic residue, namely the root x which satisfies both $\left(\frac{x}{n}\right) = 1$ and $x^{(p-1)(q-1)/4} \equiv 1 \pmod n$.

Let us now verify that $a^{\frac{(p-1)(q-1)+4}{8}}$ satisfies these conditions and is a root of a:

- $a^{\frac{(p-1)(q-1)+4}{8}}$ is a quadratic residue because such is a; therefore $\left(\frac{a^{\frac{(p-1)(q-1)+4}{8}}}{n}\right) = 1$.
- Since $a \in Q_n$, then $a \in Q_p$ and $a \in Q_q$. Therefore

$$a^{\frac{(p-1)(q-1)}{4}} = (a^{\frac{(p-1)}{2}})^{\frac{(q-1)}{2}} \equiv \left(\frac{a}{p}\right)^{\frac{(q-1)}{2}} = 1 \pmod p$$

  and, similarly, $a^{\frac{(p-1)(q-1)}{4}} = (a^{\frac{(q-1)}{2}})^{\frac{(p-1)}{2}} \equiv \left(\frac{a}{q}\right)^{\frac{(p-1)}{2}} = 1 \pmod q$ whence $a^{\frac{(p-1)(q-1)}{4}} \equiv 1 \pmod n$. Thus $x^{(p-1)(q-1)/4} = \left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^{(p-1)(q-1)/4} = \left(a^{(p-1)(q-1)/4}\right)^{\frac{(p-1)(q-1)+4}{8}} \equiv 1^{\frac{(p-1)(q-1)+4}{8}} = 1 \pmod n$.
- We have

$$\left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^2 = a^{\frac{(p-1)(q-1)+4}{4}} = aa^{\frac{(p-1)(q-1)}{4}} = a(a^{\frac{(p-1)}{2}})^{\frac{(q-1)}{2}} \equiv a\left(\frac{a}{p}\right)^{\frac{(q-1)}{2}} = a \pmod p$$

  and, similarly, $\left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^2 \equiv a\left(\frac{a}{q}\right)^{\frac{(p-1)}{2}} = a \pmod q$ whence $\left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^2 \equiv a \pmod n$.

□

Corollary Q.32. *If n is a Blum integer then the map*

$$\Phi : Q_n \to Q_n, \quad x \mapsto x^2$$

is a bijective whose inverse satsfies

$$\Phi^{-1}(x) = x^{\frac{(p-1)(q-1)+4}{8}}.$$

□

Definition Q.33. Let n be a Blum integer and let $a \in Q_n$. The unique square root of a in Q_n is called the *principal square root of a modulo n.*

Proposition Q.34 (Williams)**.** *Let $n = pq$ be a Blum integer; then the following conditions are equivalent*

1. *n is a William integer;*
2. *$n \equiv -3 \pmod 8$;*
3. *$\left(\frac{2}{n}\right) = -1$;*
4. *for each $a \in \mathbb{Z}_n$ exactly one element among a and $2a$ is a quadratic resuidue;*
5. *for each $a \in \mathbb{Z}_n$ $a \in Q_n \iff 2a \notin Q_n$.*

Proof. In order to prove the equivalence $1 \iff 2 \iff 3$ it is sufficient to remark that for a Blum integer $n = pq$ since $p \equiv q \equiv 3 \pmod 4$ we have four possible alternatives:

- $p \equiv q \equiv 3 \pmod 8 \implies n \equiv 1 \pmod 8 \implies \left(\frac{2}{n}\right) = 1$;
- $p \equiv q \equiv 7 \pmod 8 \implies n \equiv 1 \pmod 8 \implies \left(\frac{2}{n}\right) = 1$;
- $p \equiv 3 \pmod 8, q \equiv 7 \pmod 8 \implies n \equiv -3 \pmod 8 \implies \left(\frac{2}{n}\right) = -1$;
- $p \equiv 7 \pmod 8, q \equiv 3 \pmod 8 \implies n \equiv -3 \pmod 8 \implies \left(\frac{2}{n}\right) = -1$

The equivalence $3 \iff 4 \iff 5$ is trivial. □

Corollary Q.35 (Williams)**.** *Let n be a Williams integer; then for each $a \in \mathbb{Z}_n$ either $2(2a+1) \in \bar{Q}_n$ or $4(2a+1) \in \bar{Q}_n$.* □

Lemma Q.36 (Williams)**.** *Let*

$$\mathcal{M} := \{a \in \mathbb{N} : 4(2a+1) < n\}$$

and let $e, d \in \mathbb{N}$ be s.t. $\gcd(e, \phi(n)) = 1$ and $ed \equiv \frac{(p-1)(q-1)+4}{8} \pmod{\phi(n)}$ Consider the maps

- $\mathcal{E}_1 : \mathcal{M} \to \mathbb{Z}_n : \mathcal{E}_1(a) \mapsto \begin{cases} 4(2a+1) & \textit{iff } \left(\frac{2a+1}{n}\right) = 1 \\ 2(2a+1) & \textit{iff } \left(\frac{2a+1}{n}\right) = -1 \end{cases}$
- $\mathcal{E}_2 : \{b : 0 \le b \le n-1\} \to \{b : 0 \le b \le n-1\} : \mathcal{E}_2(b) \equiv b^{2e} \pmod n$
- $\mathcal{D}_2 : \{b : 0 \le b \le n-1\} \to \{b : 0 \le b \le n-1\} : \mathcal{D}_2(b) \equiv b^{d} \pmod n$
- $\mathcal{D}_1 : \{c : 0 \le c \le n-1\} \to \mathcal{M} : \mathcal{D}_1(c) \mapsto \begin{cases} \frac{\frac{c}{4}-1}{2} & \textit{iff } c \equiv 0 \pmod 4 \\ \frac{\frac{n-c}{4}-1}{2} & \textit{iff } c \equiv 1 \pmod 4 \\ \frac{\frac{c}{2}-1}{2} & \textit{iff } c \equiv 2 \pmod 4 \\ \frac{\frac{n-c}{2}-1}{2} & \textit{iff } c \equiv 3 \pmod 4 \end{cases}$

For each $a \in \mathcal{M}, \mathcal{D}_1\mathcal{D}_2\mathcal{E}_2\mathcal{E}_1(a) = a$.

Proof. The element $b := \mathcal{E}_1(a)$ satisfies

1. b is even,
2. $0 \le b \le n-1$ and
3. $\left(\frac{b}{n}\right) = 1$

and

$$c := \mathcal{D}_2\mathcal{E}_2\mathcal{E}_1(a) = \mathcal{D}_2\mathcal{E}_2(b) \equiv b^{2ed} \equiv (b^2)^{\frac{(p-1)(q-1)+4}{8}} \pmod{n}$$

satisfies (Proposition Q.31)

4. $c \in Q_n$,
5. $c^2 \equiv b^2$
6. $\left(\frac{c}{n}\right) = 1$

thus

- $c \equiv \pm b \pmod{n}$ and
- $c = b \iff c$ is even, while $c = n - b \iff c$ is odd.

Thus:

- if $4 \mid c$ then $c = b = 4(2a+1)$ and $a = \frac{\frac{c}{4}-1}{2}$.
- if $c \equiv 1 \pmod{4}$ then $b = n - c \equiv pq - c \equiv 3 \star 3 - 1 \equiv 0 \pmod{4}$ and $n - c = b = 4(2a+1)$ whence $a = \frac{\frac{n-c}{4}-1}{2}$
- if $c \equiv 2 \pmod{4}$ then $c = b = 2(2a+1)$ and $a = \frac{\frac{c}{2}-1}{2}$
- if $c \equiv 3 \pmod{4}$ then $b = n - c \equiv pq - c \equiv 3 \star 3 - 3 \equiv 2 \pmod{4}$ and $n - c = b = 2(2a+1)$ whence $a = \frac{\frac{n-c}{2}-1}{2}$.

□

Q.5 Periodicity of quadratic residues

Definition Q.37. For each $n \in \mathbb{N}, n > 1$

- $\mathrm{ord}_n(x)$ denotes for each $x \in \mathbb{Z}_n^*$ the least positive integer $e \in \mathbb{N}^* : x^e \equiv 1 \pmod{n}$;
- the *Euler totient function* $\phi(n)$ is the cardinality of the set

$$\{j \in \mathbb{N} : 1 \leq j \leq n, \gcd(n, j) = 1\}.$$

- the *Carmichael function* $\lambda(n)$ is the minimal value $e \in \mathbb{N}^* : x^e \equiv 1 \pmod{n} \forall x \in \mathbb{Z}_n^*$.

Fact Q.38. *We have*
$$\begin{cases} \phi(1) = 1 \\ \phi(2) = 1 \\ \phi(2^\alpha) = 2^{\alpha-1} \\ \phi(p) = p - 1 & \textit{for any prime } p \\ \phi(p^\alpha) = p^{\alpha-1}(p-1) & \textit{for any prime } p \\ \phi(n) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1) = n\prod_{i=1}^r (1 - \frac{1}{p_i}) & \textit{for } n = \prod_{i=1^r} p_i^{\alpha_i} \end{cases}$$
□

Fact Q.39. *We have*
$$\begin{cases} \lambda(1) = 1 \\ \lambda(2) = 1 \\ \lambda(4) = 2 \\ \lambda(2^\alpha) = 2^{\alpha-2} & \alpha \geq 2 \\ \lambda(p) = p - 1 & \textit{for any prime } p \\ \lambda(p^\alpha) = p^{\alpha-1}(p-1) & \textit{for any prime } p \\ \lambda(n) = \mathrm{lcm}(\lambda(p_i^{\alpha_i}), \ldots, \lambda(p_r^{\alpha_r})) & \textit{for } n = \prod_{i=1}^r p_i^{\alpha_i} \end{cases}$$
□

Notation Q.40. For each Blum number $n = pq$ and each $x \in Q_n$ consider the sequence $x_0, x_1, \ldots, x_i, \ldots$ of elements in Q_n defined by $x_i := x^{2^i}$ so that, in partciular $x_0 = x$ and remark that

- the sequence is periodic since Q_n is finite and that
- since $x_i \equiv x_j \pmod{n} \implies x_{i-1} = \Phi(x_i) \equiv \Phi(x_j) = x_{j-1} \pmod{n}$, the sequence can be naturally exteneded to a sequence

$$\ldots, x_{-i}, \ldots, x_{-1}, x_0, x_1, \ldots, x_i, \ldots \tag{Q.1}$$

by setting $x_i = \Phi(x_{i+1}) \forall i < 0$.

□

Definition Q.41. The *period* of $x \in Q_n$ is denoted $\bar{\pi}(x)$ and is the least period of the sequence (Q.1).

Lemma Q.42 (Blum-Blum-Shub)**.** *For a Blum number $n = pq$ and each $x \in \mathbb{Z}_n^*$*

$$\operatorname{ord}_n(x) = \frac{\lambda(n)}{2} \text{ and } \operatorname{ord}_{\frac{\lambda(n)}{2}}(2) = \lambda(\lambda(n)) \implies \lambda(\lambda(n)) \mid \pi(x).$$

Proof. Since $x \equiv x_{\bar{\pi}(x)} \equiv x^{2^{\bar{\pi}(x)}} \pmod{n}$ we have $x^{2^{\bar{\pi}(x)}-1} \equiv 1 \pmod{n}$ and $\frac{\lambda(n)}{2} = \operatorname{ord}_n(x) \mid 2^{\bar{\pi}(x)} - 1$.

Thus $2^{\bar{\pi}(x)} \equiv 1 \bmod \frac{\lambda(n)}{2}$. Also $\lambda(\lambda(n)) = \operatorname{ord}_{\frac{\lambda(n)}{2}}(2)$ is the least exponent $e : 2^e \equiv 1 \pmod{\frac{\lambda(n)}{2}}$ which implies, as claimed, $\lambda(\lambda(n)) \mid \bar{\pi}(x)$. □

Lemma Q.43 (Blum-Blum-Shub)**.** *For a Blum number $n = pq$ and each $x \in \mathbb{Z}_n^*$ $\bar{\pi}(x) \mid \lambda(\lambda(n))$.*

Proof. Since $a \equiv b^2 \pmod{n} \implies a^{\operatorname{ord}_n(b)} = b^{2\operatorname{ord}_n(b)} \equiv 1 \pmod{n} \implies \operatorname{ord}_n(a) \mid \operatorname{ord}_n(b)$, we have

$$\operatorname{ord}_n(x) = \operatorname{ord}_n(x_{\bar{\pi}(x)}) \mid \operatorname{ord}_n(x_{\bar{\pi}(x)-1}) \mid \cdots \mid \operatorname{ord}_n(x_1) \mid \operatorname{ord}_n(x) \implies \operatorname{ord}_n(x_i) = \operatorname{ord}_n(x) \forall i.$$

Let $e \in \mathbb{N}$ and $m \in \mathbb{N}$ odd s.t. $\operatorname{ord}_n(x) = 2^e m$; if we assume that $e > 0$ we have $1 \equiv x^{2^e m} = x_1^{2^{e-1} m} \bmod n$ which contradicts $\operatorname{ord}_n(x_1) = \operatorname{ord}_n(x)$. Thus $\operatorname{ord}_n(x)$ is odd.

By definition $\bar{\pi}(x)$ is the least integer e s.t. $2^e \equiv 1 \bmod \operatorname{ord}_n(x)$; since $\gcd(2, \operatorname{ord}_n(x)) = 1$, $2 \in \mathbb{Z}^*_{\operatorname{ord}_n(x)}$ and $\bar{\pi}(x) \mid \lambda(\operatorname{ord}_n(x)$.

Moreover $\operatorname{ord}_n(x) \mid \lambda(n)$ and $\bar{\pi}(x) \mid \lambda(\operatorname{ord}_n(x) \mid \lambda(\lambda(n))$ by definition of Carmichael function. □

Corollary Q.44 (Blum-Blum-Shub)**.** *For a Blum number $n = pq$ and each $x \in \mathbb{Z}_n^*$*

$$\operatorname{ord}_n(x) = \frac{\lambda(n)}{2} \text{ and } \operatorname{ord}_{\frac{\lambda(n)}{2}}(2) = \lambda(\lambda(n)) \implies \pi(x) = \lambda(\lambda(n)).$$

□

Definition Q.45. A prime number p is a *Sophie Germain prime* if $2p + 1$ is also prime. □

Definition Q.46 (Blum-Blum-Shub)**.** Let $n = pq$ be a Blum integer. Thus there are integers $p_2, q_2, p_1 := 2p_2+1, q_1 := 2q_2 + 1$ such that

$$p = 2p_1 + 1 = 2(2p_2 + 1) + 1 = 4p_2 + 3 \text{ and } q = 2q_1 + 1 = 2(2q_2 + 1) + 1 = 4q_2 + 3.$$

The Blum integer n is called *special* if (equivalently)

- p, p_1, p_2, q, q_1, q_2 are primes;
- p_1, p_2, q_1, q_2 are Germain primes.

Theorem Q.47. *Let $n = pq$ a special Blum integer. If 2 is a quadratic residue modulo at most one of $p_1 = \frac{p-1}{2}, q_1 = \frac{q-1}{2}$ then $\operatorname{ord}_{\frac{\lambda(n)}{2}}(2) = \lambda(\lambda(n))$.*

Proof. By definition of special Blum integers we have $\lambda(n) = 2p_1q_1$, $\frac{\lambda(n)}{2} = p_1q_1$, $\lambda(\frac{\lambda(n)}{2}) = 2p_2q_2$. Carmichael Theorem implies that $\operatorname{ord}_{\frac{\lambda(n)}{2}}(2) \mid \lambda(\frac{\lambda(n)}{2}) = 2p_2q_2$.

- Assume $\boxed{\operatorname{ord}_{\frac{\lambda(n)}{2}}(2) \mid 2p_2}$ so that $2^{2p_2} \equiv 1 \bmod p_1q_1$ whence $2^{2p_2} \equiv 1 \bmod q_1$. Since we have also $2^{2q_2} = 2^{q_1-1} \equiv 1 \bmod q_1$ we have $4 = 2^2 = 2^{\gcd(2p_2, 2q_2)} \equiv 1 \bmod q_1$ which contradicts the fact that $q_1 \geq 5$.
- If $\boxed{\operatorname{ord}_{\frac{\lambda(n)}{2}}(2) \mid 2q_2}$ a similar argument implies that $4 = 2^2 = 2^{\gcd(2p_2, 2q_2)} \equiv 1 \bmod p_1$ contradicting $p_1 \geq 5$.
- Assume $\boxed{\operatorname{ord}_{\frac{\lambda(n)}{2}}(2) \mid p_2q_2}$ and let wlog assume $\boxed{p_2 < q_2}$ so that $2^{p_2q_2} \equiv 1 \bmod p_1q_1$ whence $2^{p_2q_2} \equiv 1 \bmod p_1$. Since q_2 is odd,
  $$1 \equiv 2^{p_2q_2} \equiv (2^{p_2})^{q_2} \bmod p_1 \implies 2^{p_2} \not\equiv -1 \bmod p_1$$
  whence $\left(\frac{2}{p_1}\right) \equiv 2^{(p_1-1)/2} = 2^{p_2} = 2^{p_2} \equiv 1 \bmod p_1$ and $2 \in Q_{p_1}$.
  If $p_2 = 2$ and $p = 11$ this contradicts $\left(\frac{2}{5}\right) = -1$.
  If $p_2 \neq 2$ then p_2 is odd and the same argument allows to deduce that also $2 \in Q_{q_1}$. Since, for $p_2 \neq 2$, we have proved $2 \in Q_{p_1}$ we have a contradiction with the assumption that 2 is a quadratic residue modulo at most one among $p_1 = \frac{p-1}{2}, q_1 = \frac{q-1}{2}$

□

Corollary Q.48. *For a special Blum integer* $n = pq$*, if 2 is a quadratic residue modulo at most one of* $p_1 = \frac{p-1}{2}, q_1 = \frac{q-1}{2}$*, then there is* $x \in Q_n : \bar{\pi}(x) = \lambda(\lambda(n))$. □

Remark Q.49. In their definition of special numbers, Blum-Blum-Shub require that all the primes are odd. Since

- $p_2 = 2$ is a Germain prime,
- such is also $p_1 = 5$ and
- $2 \in \bar{Q}_5$,

this restriction removes the special Blum numbers $n = pq, p < q$ where $p = 11$ and $2 \in Q_{q_1}$. An instance of such number is $n = 517 = 11 \cdot 47$ which satifies $\left(\frac{2}{23}\right) = 1$; in fact $2^{44} \equiv 1 \bmod 5 \cdot 23$ while[4] $2^{22} \not\equiv 1 \bmod 5 \cdot 23$. □

[4] $2^5 = 32$, $2^{10} \equiv 32^2 = 1024 \equiv 1139 \equiv -11 \bmod 115$, $2^{11} \equiv 2(-11) = -22 \bmod 115$, $2^{22} \equiv (-22)^2 = 484 \equiv 24 \bmod 115$ and $2^{44} \equiv 24^2 = 576 \equiv 1 \bmod 115$.