Module IV

Quadratic Residues: The Legendre and Jacobi Symbols The apparent difficulty of determining quadratic residues (the Quadratic Residuosity Problem) is the basis for believing the Goldwassor-Micali probabilistic public-key encryption scheme to be secure. For this reason we study quadratic residues.

Definition 1. Let $a \in Z_n^*$. Then a is a quadratic residue modulo n (or a square modulo n) if and only if the equation $x^2 = a$ has a solution in Z_n^*. otherwise it is a quadratic non-residue modulo n. The set of quadratic residues modulo n is denoted by Q_n; the non-residues by $\overline{Q}_n$ (so that $Z_n^* = Q_n \cup \overline{Q}_n$). More generally if gcd(a, n) = 1, a is a quadratic residue if and only if $x^2 \equiv a \pmod n$ has a solution.

Proposition 1. Consider $a \in Z_n^*$ and $b \equiv a \pmod n$. Then b is a quadratic residue if and only if $a \in Q_n$. Futhermore, y is a solution of $y^2 \equiv b \pmod n$ if and only if $y \equiv x \pmod n$ for some $x \in Z_n^*$ such that $x^2 \equiv a \pmod n$.

Proof Suppose $b \equiv a \pmod n$ and $x^2 \equiv a \pmod n$ where $x \in Z_n^*$. Then $x^2 \equiv b \pmod n$ as well so that b is a quadratic residue mod n. Next suppose that $\exists\, \hat{x}$ such that $\hat{x}^2 \equiv b \pmod n$. Now gcd (b, n) = gcd (a, n) = 1 so gcd $(\hat{x}, n) = 1$ as well. Let x denote the unique element of Z_n^* such that $\hat{x} \equiv x \pmod n$. Then $x^2 \equiv \hat{x}^2 \equiv b \equiv a \pmod n$ and $a \in Q_n$ follows. The above argument also shows that if y is a solution of $y^2 \equiv b \pmod n$ then $y \equiv x \pmod n$ where $x \in Z_n^*$ and satisfies $x^2 \equiv a \pmod n$. Of course if $y \equiv x \pmod n$ and $x^2 \equiv a \pmod n$ then $y^2 \equiv x^2 \equiv a \equiv b \pmod n$ thereby concluding the proof of the proposition.

Proposition 2. Let p be an odd prime and α be a generator of Z_p^*. Then $a \in Q_n$ if and only if $a \equiv \alpha^i$ (in Z_p) where $i \le p-1$ and i is even.

Thus $\left|Q_p\right| = \dfrac{p-1}{2} = \left|\overline{Q}_p\right|$.

Proof ($\Leftarrow$): If $a = \alpha^{2k}$ (in Z_p) where $2k \le p-1$ then $x = \alpha^k$ (in Z_p) is a solution.

($\Rightarrow$): If $a \in Q_n$ then $\exists$ x such that $x^2 = a$ in Z_p

But $x = \alpha^j$ for some $0 \le j \le p-2$. Hence $a = \alpha^{2j}$ in Z_p

Write $2j = q(p-1) + r$ such that $0 \le r \le p-2$. Then r is even and

$a = \alpha^{2j} = \alpha^r$ in Z_p.

Example 1. Consider Z_{17}^*; it has 8 generators one of which is 3.

We list the powers of $\alpha = 3$ below:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α^i	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Thus
$Q_{17} = \{1, 9, 13, 15, 16, 8, 4, 2\}$ and
$\bar{Q}_{17} = \{3, 10, 5, 11, 14, 7, 12, 6\}$

Observation 1. If x is a solution of $x^2 = a$ in Z_n the so is $-x$ (because in a ring with identity 1, $(-1)(-1)=1$).

Proposition 3. If p is an odd prime and $a \in Q_p$ then a has exactly two square roots in Z_p^* (i.e. solutions of $x^2 = a$).

Proof Recall from Lemma 2 of Module III that $x^2 - a = 0$ can have at most two solutions. Also $x \neq -x$ in Z_p.

Our next result is a slight modification of Proposition 2. It identifies the elements of Q_p in a more elementary way. We illustrate it first with the aid of the previous example.

Example 1. revisited: Realize that

$Q_{17} = \{1=1^2, 4 = 2^2, 9 = 3^2, 16 = 4^2, 8 = 5^2 \text{(mod 17)}, 2 = 6^2 \text{(mod 17)}, 15 = 7^2 \text{(mod 17)}, 13 = 8^2 \text{(mod 17)}\}$.

Proposition 4. The quadratic residues modulo p, where p is an odd prime, are given by the elements of Z_p^* congruent to $k^2 \text{(mod p)}$ where $k = 1, 2, \ldots, \frac{p-1}{2}$

Proof First we show that these elements are distinct in Z_p.

Indeed, for $1 \leq k < j \leq \frac{p-1}{2}$

$$j^2 - k^2 = (j - k)(j + k)$$

is not divisible by p since $1 \leq j - k, j + k < p - 1$ and so $p \chi j - k$, $p \chi j + k$.

Next we observe that if $x = k$ $(k = 1, \ldots, \frac{p-1}{2})$

then $x^2 \equiv k^2 \text{ (mod p)}$

trivially. As $|Q_p| = \frac{p-1}{2}$ the proof is complete.

Example 2. Consider Z_{13}^*; then

$Q_{13}=\{1^2=1, 2^2=4, 3^2= 9, 4^2\equiv 3(\text{mod } 13), 5^2\equiv 12(\text{mod } 13), 6^2\equiv 10(\text{mod } 13\}$

and so

$\bar{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$.

Exercise 4. (Submit this one) Examine the elements

$$k^2(\text{mod } p) \qquad k = \frac{p+1}{2}, \frac{p+3}{2}, ..., p\text{-}1$$

where p is an odd prime. Are they in Q_p ? Are they distinct? How are the related to the elements in the proposition?

Having studied quadratic residues in Z_p with the aid of the cyclic nature of Z_p^* we adopt the same approach for Z_n where $n = p^k$ for $p \geq 3$ and $n = 2p^k$ for $p \geq 3$. Indeed Z_n^* is cyclic for those values of n and so it has a generator say α. We shall investigate a slightly more general problem in this context:

$x^m \equiv a \ (\text{mod } n)$ - for arbitrary m and $\gcd(a, n) = 1$.

We know, since $a \in Z_n^*$, that $\exists$ i such that $\alpha^i = a$.

Now if $\exists$ x such that $x^m \equiv a \ (\text{mod } n)$ it readily follows that $\gcd(x, n) = 1$ so that $\exists$ j such that

$x = \alpha^j$. Hence

$$\alpha^{mj} \equiv \alpha^i \ (\text{mod } n)$$

and, therefore

$$\alpha^{mj-i} \equiv 1 \ (\text{mod } n)$$

But this means

$$\varphi(n) = \text{ord } \alpha \mid mj - i$$

i.e. $\quad mj \equiv i \ (\text{mod } \varphi(n))$

These steps are easily seen to be reversible so x is a solution of $x^m \equiv a \pmod n$

if and only if $x = \alpha^j$ such that $m j \equiv i (\mathrm{mod}(\varphi(n))$

Now recall from the Exercise 6 b) of Module II that

$m j \equiv i \pmod{\varphi(n)}$ has a solution for $j \in [\varphi(n)]$

if and only if

$\gcd(m, \varphi(n)) \mid i$

Furthermore there are exactly $\gcd(m, \varphi(n))$ solutions in $[\varphi(n)]$. Realize if $\gcd(m, \varphi(n)) \mid i$ then

$$a^{\varphi(n)/\gcd(m, \varphi(n))} = \alpha^{\varphi(n)\, i/\gcd(m, \varphi(n)} \equiv 1 \pmod n$$

Conversely, if $\gcd(m, \varphi(n)) \not| i$ then $\dfrac{\varphi(n)i}{\gcd(m, \varphi(n)} \not\equiv 0 \pmod{\varphi(n)}$

and so $a^{\varphi(n)/\gcd(m, \varphi(n)} \not\equiv 1 \pmod n$

Summarizing we get the next theorem:

<u>Theorem 1</u>. Let $n = 1, 2, 4, p^k$ $(p \geq 3)$ or $2p^k (p \geq 3)$. If $\gcd(n, a) = 1$ then

$x^m \equiv a \pmod n$ has $\gcd(m, \varphi(n))$ solutions if $a^{\varphi(n)/\gcd(m, \varphi(n))} \equiv 1 \pmod n$.

If α is a primitive in Z_n^* and $a = \alpha^i$ then the solutions are given by α^j where j runs through the solutions of $m j \equiv i \pmod{\varphi(n)}$.

If $a^{\varphi(n)/\gcd(m, \varphi(n)} \not\equiv 1 \pmod n$ then $x^m \equiv a \pmod n$ has no solutions.

<u>Corollary 1.1</u> For the values $n = 1, 2, 4, p^k$, $2p^k$ $(p \geq 3)$ and $a \in Z_n^*$,

$$x^2 \equiv a \pmod n$$

has 2 solutions if $a^{\varphi(n)/2} \equiv 1 \pmod n$.

If α is primitive and $a = \alpha^i$ then the solutions are given by α^j where

$$2j \equiv i \pmod{\varphi(n)}.$$

If $a^{\varphi(n)/2} \not\equiv 1 \pmod m$ then $x^2 \equiv a \pmod n$ has no solutions.

Example 3. $n = 121 = 11^2$. Consider $x^5 \equiv a \pmod{121}$

Find a's such that a solution exists and determine the solutions.

Solution Consider $\gcd(\varphi(121), 5) = \gcd(110, 5) = 5$.

We know that 2 is a generator of $Z^*_{11^2}$. Consider $5j \equiv i \pmod{110}$

i = 0 (i.e. a = 1): j = 0, 22, 44, 66, 88

Therefore $2^{22} \equiv (2^{11})^2 \equiv (112)^2 \pmod{121} = (-9)^2 \pmod{121}$

$= 81 \pmod{121}$

$2^{44} \equiv 27 \pmod{121}$

$2^{66} \equiv 9 \pmod{121}$

$2^{88} \equiv 3 \pmod{121}$ and, of course, 1 are the solutions.

i = 5 (i.e. $a = 2^5 = 32$): j = 1, 23, 45, 67, 89

Therefore $2^1 = 2$

$2^{33} \equiv 41 \pmod{121}$

$2^{45} \equiv 54 \pmod{121}$

$22^{67} \equiv 18 \pmod{121}$

and $2^{89} \equiv 6 \pmod{121}$ are the solutions.

There are 20 more a's for which $x^5 \equiv a \pmod{121}$ has 5 solutions. Of the 110 elements of Z^*_{121} the remaining 88 a's do not yield solutions.

Example 4. $n = 13^2$. In this case $\alpha = 2$ is a primitive.

Consider $\quad x^2 \equiv 2 \pmod{13^2}$

We must check $\quad 2^{78}$

First we write $\quad 78 = 0\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2 + 1\cdot 2^3 + 0\cdot 2^4 + 0\cdot 2^5 + 1\cdot 2^6$

Thus the square and multiply algorithm yields

$b = 1$

$A = 2$

Set $A = 2^2 \pmod{13^2}$

$k_1 = 1 \Rightarrow b = 4\cdot 1 \pmod{13^2}$

Set $A = 4^2 \pmod{13^2}$

$k_2 = 1 \Rightarrow b = 4^3 \pmod{13^2}$

Set $A = 2\cdot 56 \pmod{13^2} = 87 \pmod{13^2}$

$k_3 = 1 \Rightarrow b = (64)(87) \pmod{13^2} = 160 \pmod{13^2}$

Set $A = (87)^2 \pmod{13^2} = 133 \pmod{13^2}$

$k_4 = 0$

Set $A = (133)^2 \pmod{13^2} = 113 \pmod{13^2}$

$k_5 = 0$

Set $A = (113)^2 \pmod{a3^2} = 94 \pmod{13^2}$

$k_6 = 1 \Rightarrow b = (160)(94) \pmod{13^2}$

$\quad = 168 \pmod{13^2} \equiv (-1) \pmod{13^2}$

Conclusion: $x^2 \equiv 2 \pmod{13^2}$ DOESN'T have a solution.

Next consider $\quad x^2 \equiv 4 \pmod{13^2}$. Since $(4)^{78} = (2^{78})^2 \equiv (-1)^2 \pmod{13^2}$

$x^2 \equiv 4 \pmod{13^2}$ has two solutions $\quad x = 2, 167$

Finally we determine $\left|Q_{13^2}\right|$. Since it is necessary and sufficient that $a^{\varphi(n)/2} \equiv 1$ we require the number of a's in $Z^*_{(13)^2}$ having order which divides $\varphi(n)/2$. Thus there are

$$\sum_{d/\frac{\varphi(n)}{2}} \varphi(d) = \sum_{d/78} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(26) + \varphi(39) + \varphi(78)$$

$$= 1 + 1 + 2 + 2 + 12 + 12 + 24 + 24$$

$$= 78$$

such a's.

Exercise 2. (Submit this one) Prove: For $n = 1, 2, 4, p^k, 2p^k (k \geq 3)$

$$|Q_n| = |\bar{Q}_n| = \frac{\varphi(n)}{2}$$

Exercise 3. Prove $(144)^{78} \equiv 1 \pmod{13^2}$

Exercise 4. (Submit this one) Determine if $40 \in Q_{13^2}$

Exercise 5. For n as above $(1, 2, 4, p^k, 2p^k\ (k \geq 3))$ does

$$Q_n = \left\{ 1^2 \pmod{n}, 2^2 \pmod{n}, ..., (\frac{\varphi(n)}{2})^2 \pmod{n} \right\}?$$

Exercise 6. (Submit (*ii*)) Verify that $Q_{11} = \{1, 3, 4, 5, 9\}$

i) Find the solutions of $x^2 \equiv a \pmod{11}$ in Z_{11}^x for each $a \in Q_{11}$

ii) What are the solutions of $x^2 \equiv a$ where $a = 5, a = 9$?

iii) Choose $a \in Z_{121}$, $a > 11$ and determine the solutions of $x^2 \equiv a \pmod{121}$

A convenient way to keep track of whether the number a satisfying $\gcd(a, p) = 1$, is a quadratic residue is afforded by the "Legendre" symbol. It has further use in the event that n is a product of two distinct primes.

Definition 2. Let p be an odd prime and $a \in Z$

Then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } p \mid a \\ 1 \text{ if } a \in Q_p \\ -1 \text{ if } a \in \overline{Q_p} \end{cases}$$

The Legendre symbol has several properties that can greatly simplify the determination of whether a is a quadratic residue modules p.

Proposition 5. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ so a is a quadratic residue module p when

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

and is a quadratic non-residue module p when

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

<u>Proof</u> Recall Fermat's theorem, if gcd (a, p) = 1 then

$$a^{p-1} \equiv 1 \pmod p.$$

But then $a^{\frac{p-1}{2}} \pmod p$ is a root of $x^2 - 1$ in Z_p. As this polynomial has exactly two roots in Z_p, namely 1 and p-1 (= -1) we see that

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \text{ or } a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Now suppose a is a quadratic residue, i.e. $\exists x$ such that $x^2 \equiv a \pmod p$

Suppose $a^{\frac{p-1}{2}} \equiv -1 \bmod p$; then $\left(x^2\right)^{\frac{p-1}{2}} \equiv -1 \pmod p$

i.e. $x^{p-1} \equiv -1 \pmod p$

This condradicts Fermat's Theorem so if a is a quadratic residue then

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Now we know that there are exactly $\frac{p-1}{2}$ quadratic residues in Z_p so each of them satisfies $y^{\frac{p-1}{2}} - 1 = 0$ in Z_p. But this polynormial has at most $\frac{p-1}{2}$ solutions in Z_p and so the quadratic non-residues modulo p are precisely those elements of Z_p^* satisfying $a^{\frac{p-1}{2}} = 1$

Finally then

$\forall a$ such that gcd (a, p) = 1

$a^{\frac{p-1}{2}} \equiv 1 \bmod p$ if and only if a is a quadratic residue because for such an a $\exists$ unique $r \in Z_p^*$ such that $a \equiv r \pmod p$ so that $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \pmod p$.

<u>Another</u> (simpler) <u>proof</u> : We know that $a \in Zp$ is a quadratic residue if and only if $a = \alpha^{2i}$ where α is a generator of Z_p^* and $2i \le p-2$. Thus

a is a quadratic residue

$$\Rightarrow a^{\frac{p-1}{2}} = \alpha^{2i\left(\frac{p-1}{2}\right)} = 1 \text{ in } Zp.$$

On the other hand if $a = \alpha^{2i+1}$ where $2i + 1 \le p-2$

then

$$a^{\frac{p-1}{2}} = \alpha^{2i\left(\frac{p-1}{2}\right)}\alpha^{\frac{p-1}{2}} = -1 \text{ in } Zp.$$

Finally then consider any $a \in Z$ such that $\gcd(a, p) = 1$.
$\exists$ a unique $r \in Zp$ such that $a \equiv r \pmod p$ and $\gcd(p, r) = 1$.
Now $\exists$ x such that

$$
\begin{aligned}
& x^2 \equiv a \pmod p \\
\Leftrightarrow\quad & x^2 \equiv r \pmod p \\
\Leftrightarrow\quad & r^{\frac{p-1}{2}} \equiv 1 \text{ in } Z\,p \\
\Leftrightarrow\quad & a^{\frac{p-1}{2}} \equiv 1 \pmod p
\end{aligned}
$$

Example 5. In Z_{17} the quadratic residues are $Q_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$
Thus the quadratic residues in Z are $\{k + \alpha(17) \mid k \in Q_{17},\ \alpha \in Z\}$.

Some straight-forward but interesting consequences of the previous result are given in the next theorem: Let p be an odd prime.

Theorem 2. (*i*) $\forall$ a, b $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Thus ab is a quadratic residue modulo p if and only if either both a and b are quadradic residues modulo p or neither is.

(*ii*) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(*iii*) if $\gcd(a, p) = 1$ then $\left(\frac{a^2}{p}\right) = 1$ and $\forall b \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

Thus the square of every element of Z_p^* is a quadratic residue modulo p and a^2b is a quadratic residue modulo p if and only if b is a quadratic residue modulo p.

(*iv*) $\left(\frac{1}{p}\right) = 1,\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Thus (-1) (= p-1) is a quadratic residue modulo p if and only if p is of the form 4k+1.
Those of the form 4k+3 yield p's such that $(-1)^{\frac{p-1}{2}} = -1$

Proof (*i*) By the previous theorem $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}}\ b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} = \left(\frac{ab}{p}\right)$

(*ii*) $(b + kp)^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod p$

(*iii*) This follows from (*i*), i.e. $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2$ and $\left(\frac{a}{p}\right) \neq 0 \Rightarrow \left(\frac{a}{p}\right)^2 = 1$

(*iv*) Trivial

Examples (6) $\frac{121}{3} = \left(\frac{(11)^2}{3}\right) = 1$ since gcd (11, 3) = 1

Note: $\left(\frac{11}{3}\right) = (11)^1 \equiv 2 \pmod 3) = -1 \pmod 3$

(7) $\left(\frac{30}{11}\right) = \left(\frac{3}{11}\right)\left(\frac{2}{11}\right)\left(\frac{5}{11}\right)$

$= 3^5 \quad 2^5 \quad 5^5 \pmod{11}$

$= (1 \bmod 11)\,(10 \bmod 11)\,(1 \bmod 11)$

$= -1 \pmod{11}$

so 30 is a quadratic non residue modulo 11.

(8) p = 89 = 4(22) + 1 so -1 is a quadratic residue module 89.

p = 59 = 4(14) + 3 so -1 is a quadratic non- residue modulo 59.

Exercise 7. Prove: $\sum_{j=1}^{p-1} \left(\frac{1}{p}\right) = 0$

The ensuing discussion culminates in the so-called Guassian reciprocity law, a result that in many instances simplifies the computation of $\left(\frac{a}{p}\right)$. We require two preliminary results:

(Gauss) Let p be an odd prime and gcd(a, p) = 1. Consider

$$a \bmod p,\ 2a \bmod p, \ldots, \left(\frac{p-1}{2}\right) a \bmod p \in Zp.$$

If n denotes the number of these residues that exceed $\frac{p}{2}$ then

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

Proof Partition these residues into two sets:

$r_1, r_2, \ldots, r_n$ - those that exceed $\frac{p}{2}$

and $s_1, s_2, \ldots, s_k$ - those lying within $\left[\left[\frac{p}{2}\right]\right]$

Of course

$$p - r_1, p - r_2, \ldots, p - r_n \text{ lie within } \left[\left[\frac{p}{2}\right]\right] \text{ and are distinct. Moreover,}$$

the sets $\{p - r_1, \ldots, p - r_n\}$ and $\{s_1, s_2, \ldots, s_k\}$ are <u>disjoint</u>. Indeed, if

$$p - r_i = s_j$$

then

$$\exists\, 1 \le k, \ell \le \frac{p-1}{2} \qquad \text{such that}$$

$$k\,a = q\,p + r_i$$

$$\ell\,a = \hat{q}\,p + s_j$$

so

$$p = r_i + s_j = (k + \ell)\,a - (q + \hat{q})\,p.$$

Thus

$$(k + \ell)a = (1 + q + \hat{q})\,p$$

and so $\qquad p \mid (k+\ell)\,a.$

But $\qquad p \not\mid k+\ell$ (because $k + \ell < p$) and $p \not\mid a$ - a contradiction.

Now the total number of elements in these two sets is $\frac{p-1}{2}$ so

$$\{p-r_1, p-r_2, \ldots, p-r_n, s_1, s_2, \ldots, s_k\} = \left[\frac{p-1}{2}\right]$$

Consider

$$\prod_{i=1}^{n} (p - r_i) \prod_{j=1}^{k} s_j \equiv \prod_{j=1}^{(p-1)/2} j \pmod{p}.$$

so that

$$(-1)^n \prod_{i=1}^{n} r_i \prod_{j=1}^{k} s_j \equiv \prod_{j=1}^{\frac{p-1}{2}} j \pmod{p}$$

But

$$a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \equiv \prod_{i=1}^{n} r_i \prod_{j=1}^{k} s_j \pmod{p}$$

so

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

and finally

$$(-1)^n \; a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

or equivalently

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

The next prerequisite result requires the previous one for its proof.

<u>Theorem 3</u>. If p is an odd prime and $\gcd(a, 2p) = 1$ then $\left(\frac{a}{p}\right) = (-1)^t$

where $t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor$

Also $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

<u>Proof</u> Write $\quad j\,a = \left\lfloor \frac{j\,a}{p} \right\rfloor p + r_{ja}$

so

$$\sum_{j=1}^{(p-1)/2} ja = pt + \sum_{j=1}^{(p-1)/2} r_{ja} = p\,t + \sum_{i=1}^{k} r_i + \sum_{j=1}^{n} s_j$$

Also

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n} (p-s_j) + \sum_{i=1}^{k} r_i = n\,p - \sum_{j=1}^{n} s_j + \sum_{1=1}^{k} r_i$$

Subtracting we get

$$(a - 1) \sum_{j=1}^{(p-1/2} j = p\,(t - n) + 2\sum_{j=1}^{n} s_j.$$

Thus, as a is odd, t and n have the same parity so

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^t$$

If $a = 2$ observe that $aj = 2j \le p\text{-}1 \ \ \forall 1 \le j \le \frac{p-1}{2}$.

Thus $\left\lfloor \frac{aj}{p} \right\rfloor = 0$; so $t = 0$. Therefore

$$\frac{p^2-1}{8} = -n\,p + 2\sum_{j=1}^{n} s_j$$

and so n and $\frac{p^2-1}{8}$ have the same parity. Hence

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

A final prerequisite result is left as

Exercise 8. (Extra Credit)

Proposition 6. If p and q are odd primes then

$$\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{j=1}^{(q-1)/2)} \left\lfloor \frac{j\,p}{q} \right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

Finally we present

Theorem 4. Guass' Reciprocity Theorem If p, q are two distinct odd primes

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

Proof . Exercise 9. (Submit this one)

Remark 1. Write $p = 4m + j \quad j = 1, 3$

$q = 4k + i \quad i = 1, 3$

If both are of the form $4\ell + 3$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

If at least one is of the form $4\ell + 1$ then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

Examples 9. $\left(\frac{5}{229}\right) \equiv 5^{114} \bmod 229$

Instead realize $5 = 4(1) + 1$ so

$$\left(\frac{5}{229}\right) = \left(\frac{229}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$$

so $x^2 \equiv 5 \pmod{229}$ has two solutions.

Example 10. $\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)$

$$\left(\frac{-1}{61}\right) = (-1)^{30} = 1$$

$$\left(\frac{2}{61}\right) = (-1)^{\left[(61^2-1)\right]/8} = (-1)^{\left(\frac{61-1}{4}\right)\left(\frac{62}{2}\right)} = -1$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right)(-1)^{\frac{2}{2}\frac{60}{2}} = \left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right)(-1)^{(3)\,(30)} = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{(3)\,(2)} = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right)$$

$$= (-1)^{\frac{25-1}{8}} = -1$$

Therefore

$$\left(\frac{-42}{61}\right) = 1$$

Another method: $\left(\frac{-42}{61}\right) = \left(\frac{19}{61}\right) = \left(\frac{61}{19}\right)(-1)^{(9)(30)} = \left(\frac{61}{19}\right)$

$$= \frac{4}{19} = \left(\frac{2^2}{19}\right) = 1$$

Exercise 10. (Submit this one) Evaluate $\left(\frac{-23}{83}\right)$, $\left(\frac{51}{71}\right)$, $\left(\frac{71}{73}\right)$, $\left(\frac{-33}{97}\right)$

Exercise 11. Which of the following have solutions?

a) $x^2 \equiv 2 \pmod{61}$

b) $x^2 \equiv -2 \pmod{61}$

c) $x^2 \equiv 2 \pmod{59}$

d) $x^2 \equiv -2 \pmod{59}$

Example 11. In this example we determine all odd primes p such that $3 \in Q_p$.

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

Therefore write $p = 3t + j \qquad j = 1, 2$ so

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) & \text{if } j = 1 \\ \left(\frac{2}{3}\right) & \text{if } j = 2 \end{cases}$$

$$= \begin{cases} 1 & \text{if } j = 1 \\ -1 & \text{if } j = 2 \end{cases}$$

Now

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 4s + 1 \\ -1 & \text{if } p = 4s + 3 \end{cases}$$

Hence $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$

or $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$

Now $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4 \Leftrightarrow p \underline{\equiv 1} \pmod{12}$

and $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$

$\Leftrightarrow \quad p \equiv -1 \pmod 3$ and $p \equiv -1 \pmod 4$

$\Leftrightarrow \quad p \equiv -1 \pmod{12} \equiv \underline{\underline{11}} \pmod{12}$

Finally then $3 \in Q_p \Leftrightarrow p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$

Next we introduce the Jacobi symbol, a generalization of the Legendre symbol, which serves to greatly simplify the computation of the Legendre symbol in many cases.

Definition 3. Let Q be an odd positive number written as $Q = q_1 q_2 \cdots q_s$ where the q_i's are primes, but not necessarily distinct. Then

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_i}\right)$$

is referred to as a Jacobi symbol.

Observation 2. $\left(\frac{a}{Q}\right) = \pm 1$ or 0.

Remarks 2) If Q is a prime then $\left(\frac{a}{Q}\right)$ is just the Legendre symbol.

3) As Q is uniquely representable as a product of primes, aside from order, there is no ambiguity inherent in the definition.

4) $\left(\frac{a}{Q}\right) = 0$ if and only if $\gcd(a, Q) > 1$.

Exercise 12. (Extra Credit) Prove: $a \in Q_p \Rightarrow a \in Q_{p^k} \forall$ odd prime p and all $k \geq 1$

Proposition 7. $a \in Q_Q$ if and only if $a \in Q_{p_i}$ $i = 1, .., r$ where

$$Q = \prod_{i=1}^{r} p_i^{e_i}, \text{ the } p_i\text{'s being distinct.}$$

In other words,

$$a \in Q_Q \Leftrightarrow \left(\frac{a}{p_i}\right) = 1 \quad \forall\ i = 1,.., r.$$

Thus $a \in Q_Q \Rightarrow \left(\frac{a}{Q}\right) = 1$ BUT NOT conversely.

Proof $\exists$ x such that $x^2 \equiv a \pmod{Q}$ implies $x^2 \equiv a \pmod{p_i}$for each i. Thus

$$a \in Q_Q \Rightarrow a \in Q_{p_i} \quad \forall\ i = 1,.., r.$$

Next suppose $a \in Q_{p_i}$ for each $i = 1,.., r$. Then it follows by Exercise 12 that $a \in Q_{p_i^{c_i}}$ for each $i = 1,.., r$. i.e. each congruence $x^2 \equiv a \pmod{p_i^{c_i}}$ has two solutions, day x_i^1, x_i^2. Next consider the system:

$$\begin{aligned}
x &\equiv y_1 \pmod{p_1^{c_1}} && (y_1 = x_1^1 \text{ or } x_1^2)\\
x &\equiv y_2 \pmod{p_2^{c_2}} && (y_2 = x_2^1 \text{ or } x_2^2)\\
&\bullet\\
&\bullet\\
x &\equiv y_r \pmod{p_r^{c_i}} && (y_r = x_r^1 \text{ or } x_r^2)
\end{aligned}$$

We know from the Chinese Remainder Theorem that $\exists$ a unique $x \in Z_Q$ that satisfies these congruences simutaneously.

But then $x^2 \equiv y_1^2 \pmod{p_1^{c_1}} \equiv a \pmod{p_1^{c_1}}$

$x^2 \equiv y_2^{\,2} \pmod{p_2^{c_2}} \equiv a \pmod{p_2^{c_2}}$

•

•

$x^2 \equiv y_r^{\,2} \pmod{p_r^{c_r}} \equiv a \pmod{p_r^{c_r}}$

As $p_1^{c_1}, \ldots, p_r^{c_r}$ are pairwise relatively prime

$x^2 \equiv a \pmod{Q}$ i.e. $a \in Q_Q$.

Corollary 7.1 If $Q = p_1^{c_1}\, p_2^{c_2} \cdots p_r^{c_r}$ where each p_i is an odd prime then for $a \in Q_Q$

$$x^2 \equiv a \pmod{Q}$$

has 2^r solutions.

Proof As per the above proof each system gives a distinct solution and there are 2^r such systems. On the other hand, if x is a solution of $x^2 \equiv a \pmod{Q}$ then

$$x^2 \equiv a \pmod{p_i^{c_i}}$$

for each i. Set $y_i = x \pmod{p_i^{c_i}}$ and observe that

$$y_i^{\,2} \equiv a \pmod{p_i^{c_i}} \text{ and } x \equiv y_i \pmod{p_i^{c_i}} \quad i = 1, \ldots, r$$

i.e. x satisfies one of the systems.

Example 12. $Q = 35 = (5)(7)$. Now

$$4^{\frac{5-1}{2}} \equiv 1 \pmod{5}$$

and

$$4^{\frac{7-1}{2}} \equiv 1 \pmod{7}$$

so $4 \in Q_5 \cap Q_7$. There are four solutions to $x^2 \equiv 4 \pmod{35}$

Consider the solutions of $x^2 \equiv 4 \pmod{5}$

i.e. $x = +3, -3 = 2$

and the solutions of $x^2 \equiv 4 \pmod{7}$

i.e. $x = 2, -2 = 5$

Consider one of the four possible systems, namely

$x \equiv 2 \pmod{5}$

$x \equiv 5 \pmod{7}$

By Gauss' algorithm we require

$$\hat{x} = (2)(7)\cdot(7^{-1} \bmod 5) + (5)\cdot(5)(5^{-1} \bmod 7)$$
$$= (2)(7)(3) + (5)(5)(3) = 117$$

so $x = \hat{x} \pmod{35} = 12$ is a solution

Exercise 13 (Submit this one) Find another.

Exercise 14. Find an example for which $\left(\frac{a}{Q}\right) = 1$ but $a \notin Q_Q$.

Exercise 15. (Submit b) How many solutions are there for

(a) $x^2 \equiv -1 \pmod{61}$?

(b) $x^2 \equiv -1 \pmod{365}$?

(c) $x^2 \equiv -1 \pmod{122}$?

Proposition 8. Properties of the Jacobi symbol (Q, Q' are odd and positive)

(1) $\forall\, a, a', Q\left(\left(\frac{a}{Q}\right) \left(\frac{a'}{Q}\right) = \left(\frac{a\,a'}{Q}\right)\right)$.

(2) $\forall\, a, Q, Q'\left(\left(\frac{a}{Q}\right) \left(\frac{a}{Q'}\right) = \left(\frac{a}{Q\,Q'}\right)\right)$.

(3) if $\gcd(a, Q) = 1$ then $\left(\frac{a^2}{Q}\right) = \left(\frac{a}{Q^2}\right) = 1$.

(4) if $\gcd(a\,a', Q\,Q') = 1$ then $\left(\frac{a'a^2}{Q'\,Q^2}\right) = \left(\frac{a'}{Q'}\right)$.

(5) $a' \equiv a \pmod{Q} \Rightarrow \left(\frac{a'}{Q}\right) = \left(\frac{a}{Q}\right)$.

Proof (1) $$\left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right) = \prod_{i=1}^{s}\left(\frac{a}{q_i}\right) \prod_{i=1}^{s} \left(\frac{a'}{q_i}\right)$$
$$= \prod_{i-1}^{s} \left(\frac{a}{q_i}\right)\left(\frac{a'}{q_i}\right) = \prod_{i=1}^{s} \left(\frac{a\,a'}{q_i}\right)$$
$$= \left(\frac{a\,a'}{Q}\right).$$

(2) $$\left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right) \prod_{i=1}^{s'} \left(\frac{a}{q_i'}\right) = \left(\frac{a}{\prod_1^{s} q_i \prod_1^{s'} q_i'}\right).$$

(3) $\gcd(a, Q) = 1 \Rightarrow \gcd(a, q_i) = 1 \ \forall_i$

$$\Rightarrow \left(\frac{a^2}{q_i}\right) = 1 \quad \forall_i \Rightarrow \left(\frac{a^2}{Q}\right) = 1$$

Next $\left(\frac{a}{Q^2}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right)^2 = \prod_{i=1}^{s} 1 = 1$

(4) $\left(\frac{a'a^2}{Q'Q^2}\right) = \prod_{i=1}^{s'} \left(\frac{a'a^2}{q_i'}\right) \prod_{i=1}^{s} \left(\frac{a'a^2}{q_i}\right)^2.$

Now $\gcd(a'a^2, q_i) = 1$ forces the 2nd product to be 1

(since each $\left(\frac{a'a^2}{q_i}\right) = \pm 1$). But

$$\left(\frac{a'a^2}{q_i'}\right) = \left(\frac{a'}{q_i'}\right)\left(\frac{a^2}{q_i'}\right) = \left(\frac{a'}{q_i'}\right)$$

because $\gcd(a, q_i') = 1$ forces $\frac{a}{q_i} = \pm 1$.

Thus

$$\left(\frac{a'a^2}{Q'Q^2}\right) = \prod_{i=1}^{s'} \left(\frac{a'}{q_i'}\right) = \left(\frac{a'}{Q'}\right)$$

(5) $a' \equiv a \pmod{Q} \Rightarrow a' \equiv a \pmod{q_i}$ for $i=1,..,s$

Thus

$$\left(\frac{a'}{q_i}\right) = \left(\frac{a}{q_i}\right) \forall_i \text{ and so}$$

$$\left(\frac{a'}{Q}\right) = \prod_{i=1}^{s}\left(\frac{a'}{q_i}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right) = \left(\frac{a}{Q}\right)$$

Next we present tow more properties of $\left(\frac{a}{Q}\right)$ which happen to be analagous to those of $\left(\frac{a}{p}\right)$:

<u>Proposition 9</u>. If $Q > 0$ and odd then

$$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \quad \text{and} \quad \left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$$

<u>Proof</u> Observe that

$$\left(\frac{-1}{Q}\right) = \prod_{s=1}^{k} \left(\frac{-1}{q_s}\right) \text{ where } Q = \prod_{s=1}^{k} q_s$$

$$= \prod_{s=1}^{k} (-1)^{\frac{q_s-1}{2}}$$

Now suppose t of the q_s's are of the form $4\alpha + 1$ and the remaining k - t are of the form $4\alpha + 3$. Then $\left(\frac{-1}{Q}\right) = (-1)^{k-t}$.

On the other hand since any product of numbers of the form $4\alpha + 1$ is again of the form $4\alpha + 1$ (by induction) and the product of k - t numbers of the form $4\alpha + 3$ is of the form $4\beta + 3^{k-t}$ (by induction) we have

$$(-1)\frac{Q^{-1}}{2} = (-1)^{\frac{(4\alpha+1)(4\alpha+3^{k-t})-1}{2}} = (-1)^{\frac{3^{k-t}-1}{2}}$$

<u>Claim</u> $\frac{3^{k-t}-1}{2}$ has the same parity as k-t (so $\frac{-1}{Q} = (-1)^{\frac{Q-1}{2}}$)

<u>Proof</u> Induction on k - t

Base case k - t = 0 : $\frac{3^{k-t}-1}{2} = 0$

<u>Induction hypothesis</u>: $\frac{3^{k-t-1}-1}{2}$ and k - t - 1 have the same parity.

Consider $\frac{3^{k-t}-1}{2} = \frac{3^{k-t}-3^{k-t-1}}{2} + \frac{3^{k-t-1}-1}{2}$

$$= 3^{k-t-1} + \frac{3^{k-t-1}-1}{2}$$

Since 3^{k-t-1} is odd,

$$\frac{3^{k-t}-1}{2} \text{ and } \frac{3^{k-t-1}-1}{2}$$

have opposite parity. But k - t - 1 and k- t have opposite parity so it follows by the induction hypothesis that k-t and $\frac{3^{k-t}-1}{2}$ have the SAME parity.

Next consider

$$\left(\frac{2}{Q}\right) = \prod_{s=1}^{k} \left(\frac{2}{q_s}\right) = \prod_{s=1}^{k} (-1)^{\frac{q_s^2-1}{8}}$$

Observe that if q_s is prime then $q_s = 8\alpha +1, 8\alpha + 3, 8\alpha + 5$ or $8\alpha + 7$. Furthermore, by direct calculation,

$$\frac{q_s^2 - 1}{8} \text{ is odd if and only if } q_s = 8\alpha + 3 \text{ or } 8\alpha + 5$$

Let k_3 be the # of q's of the form $8\alpha + 3$ and k_5 the number of the q's of the form $8\alpha + 5$. Of course k_1 and k_7 have similar meanings. Now

$$\left(\frac{2}{Q}\right) = (-1)^{k_3+k_5}$$

Next consider $\dfrac{Q^2-1}{8} = \dfrac{\prod_{s=1}^{k} q_s^2 - 1}{8}$. Now

$$\begin{aligned} q_s^2 &= 16\beta + 1 && \text{if } q_s = 8\alpha + 1 \\ &= 16\beta + 9 && \text{if } q_s = 8\alpha + 3 \\ &= 16\beta + 25 && \text{if } q_s = 8\alpha + 5 \\ &= 16\beta + 49 && \text{if } q_s = 8\alpha + 7 \end{aligned}$$

Therefore

$$\begin{aligned} \prod_{s-1}^{k} q_s^2 &= \left(16\beta_1 + 1^{k_1}\right)\left(16\beta_2 + 9^{k_3}\right)\left(16\beta_3 + 25^{k_5}\right)\left(16\beta_4 + 49^{k_7}\right) \\ &= 16\varphi + 9^{k_3} \cdot 25^{k_5}\ 49^{k_7}, \text{ for some } \varphi \end{aligned}$$

and so

$$\frac{\prod_{s=1}^{k} q_s{}^2 - 1}{8} = 2\varphi + \frac{9^{k_3}\ 25^{k_5}\ 49^{k_7} - 1}{8}$$

Thus

$$\frac{\prod_{s=q}^{k} q_s{}^2 - 1}{8} \text{ has the same parity as}$$

$$\frac{9^{k_3}\ 25^{k_5}\ 49^{k_7} - 1}{8}$$

<u>Claim</u> $\frac{9^{k_3}\ 25^{k_5}\ 49^{k_7}\ -1}{8}$ has the parity as $k_3 + k_5$ (thereby proving the result)

<u>Proof</u> Consider the case $k_3 + k_5 = 0$, i.e. $k_3 = k_5 = 0$.

We prove that $\frac{49^{k_7} - 1}{8}$ is even by induction on k_7.

Now $k_7 = 0$ yields $\frac{49^0 - 1}{8} = 0$, which is even. As for the induction step:

$$\frac{49^{k_7+1} - 1}{8} = \frac{49^{k_7+1} - 49^{k_7}}{8} + \frac{49^{k_7} - 1}{8}$$

$$= 49^{k_7}\frac{(48)}{8} + \frac{49^{k_7} - 1}{8}$$

$$= (6)\cdot\left(49^{k_7}\right) + \frac{49^{k_7} - 1}{8}$$

Since $k_3 + k_7$ changes parity as $k_3 + k_7$ increases by 1, it is only necessary to prove that

$$\frac{9^{k_3}\ 25^{k_5}\ 49^{k_7} - 1}{8}$$

does the same.

Consider

$$\frac{9^{k_3+1}\ 25^{k_5}\ 49^{k_7} - 1}{8}$$

$$= \frac{9^{k_3+1}\ 25^{k_5}\ 49^{k_7}\ -\ 9^{k_3}\ 25^{k_5}\ 49^{k_7}}{8} + \frac{9^{k_3}\ 25^{k_5}\ 49^{k_7}\ -\ 1}{8}$$

$$= 9^{k_3}\ 25^{k_5}\ 49^{k_7}\ \frac{[9\ -\ 1]}{8} + \frac{9^{k_3}\ 25^{k_5}\ 49^{k_7}\ -\ 1}{8}$$

The first term is odd. Next consider

$$\frac{9^{k_3}\ 25^{k_5+1}\ 49^{k_7}\ -\ 1}{8}$$

$$= 9^{k_3} 25^{k_5}\ 49^{k_7}\ \frac{[25\ -\ 1]}{8} + \frac{9^{k_3}\ 25^{k_5}\ 49^{k_7}\ -\ 1}{8}$$

and observe that the first term is odd. This completes the proof.

Next we prove the reciprocity theorem for the Jacobi symbol.

Proposition 10. $\left(\frac{P}{Q}\right)\left(\frac{Q}{\underline{P}}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{Q-1}{2}\right)}$ $\forall$ odd $\underline{P}$ and Q such that gcd ($\underline{P}$, Q) = 1.

Proof Write $\underline{P} = \prod_{i=1}^{r} p_i$ and $Q = \prod_{j=1}^{s} q_j$. Then

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{\underline{P}}{q_j}\right) = \prod_{j=1}^{s} \prod_{i=1}^{r} \left(\frac{p_i}{q_j}\right)$$

$$= \prod_{j=1}^{s} \prod_{i=1}^{r} \left(\frac{q_j}{p_i}\right) (-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_i-1}{2}\right)}$$

(because $p_i \neq q_j$). Thus

$$\left(\frac{\underline{P}}{Q}\right) = \left[\prod_{j=1}^{s} \prod_{i=1}^{r} \left(\frac{q_j}{p_i}\right)\right] [-1]^{\sum_{j=1}^{s} \sum_{i=1}^{r} \left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}$$

$$= \left(\frac{Q}{\underline{P}}\right) (-1)^{\sum_{j=1}^{s} \sum_{i=1}^{r} \left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}$$

But

$$\sum_{j=1}^{s} \sum_{i=1}^{r} \left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right) = \sum_{j=1}^{s} \left(\frac{q_j-1}{2}\right) \sum_{i=1}^{r} \left(\frac{p_i-1}{2}\right).$$

Now we know that $\sum_{i=1}^{r} \left(\frac{p_i-1}{2}\right)$ has the same parity as $\frac{P-1}{2}$; likewise for $\frac{Q-1}{2}$ and $\sum_{j=1}^{s} \left(\frac{q_j-1}{2}\right)$

This completes the proof.

Example 13. $\left(\frac{105}{317}\right)$. Realize $105 = (5)\ (3)\ (7)$ and 317 is prime so

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = (-1)^{\frac{(105)^2-1}{8}}$$

But $\frac{(105)^2-1}{8} = \frac{11024}{8} = 1378$. Thus

$$\left(\frac{105}{317}\right) = 1;$$

so $105 \in Q_{317}$

Example 14. $\left(\frac{-23}{83}\right) = \left(\frac{-1}{83}\right)\left(\frac{23}{83}\right) = -\left(\frac{23}{83}\right) = \left(\frac{83}{23}\right)$

$$= \left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = (-1)^{\frac{(23)^2-1}{8}}\left(\frac{7}{23}\right)$$

$$= \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -(-1)^{\frac{49-1}{8}} = -1$$

so $60 \in \overline{Q}_{83}$

Alternatively $\left(\frac{-23}{83}\right) = \left(\frac{60}{83}\right) = \left(\frac{5}{83}\right)\left(\frac{2^2}{83}\right)\left(\frac{3}{83}\right)$

$$= -\left(\frac{83}{5}\right)\left(\frac{83}{3}\right) = -\left(\frac{3}{5}\right)\left(\frac{2}{3}\right)$$

$$= -\left(\frac{5}{3}\right)(-1)^{\frac{9-1}{8}} = \left(\frac{2}{3}\right) = -1$$

Exercise 16. (Extra Credit) Consider $Q = p\,q$ where p and q are odd primes

Prove: (1) $\left|Q_Q\right| = \dfrac{(p-1)(q-1)}{4}$

(2) Let $J_Q = \left\{ a \in Z^*_{pq} \,\middle|\, \left(\dfrac{a}{Q}\right) = 1 \right\}$

Prove: $\left|J_Q\right| = \dfrac{(p-1)(q-1)}{2}$

The set J_Q - Q_q is called the set of pseudo-squares. Of course $\left|J_Q - Q_Q\right| = \dfrac{(p-1)(q-1)}{4}$

Hint Let $A_{p,1} = \left\{ a \in Z^*_{pq} \,\middle|\, \left(\dfrac{a}{p}\right) = \underline{1} \right\}$

$$A_{p,-1} = \left\{ a \in Z^*_{pq} \,\middle|\, \left(\dfrac{a}{p}\right) = -1 \right\}$$

and define $A_{q,1}$, $A_{q,-1}$ in the same manner.

Observe that

$$Z^*_{pq} = \left(A_{p,1} \cap A_{q,1}\right) \dot{\cup} \left(A_{p,1} \cap A_{q,-1}\right)$$
$$\dot{\cup} \left(A_{p,-1} \cap A_{q,1}\right) \dot{\cup} \left(A_{p,-1} \cap A_{q,-1}\right)$$

- Next prove each of the 4 sets in the above expression is non-$\emptyset$
- Next prove $\left|A_{p,1} \cap A_{q,1}\right| = \left|A_{p,i} \cap A_{q,j}\right| \quad i = \pm 1, j = \pm 1$

  e.g. chose $b \in A_{p,1} \cap A_{q,-1}$ and define

$$\partial: \; A_{p,1} \cap A_{q,1} \rightarrow A_{p,1} \cap A_{q,-1}$$
$$a \rightarrow a\,b \pmod{pq}$$

Prove ∂ is a bijection

Exercise 17: (Submit this one) Find $\left(\dfrac{158}{235}\right)$

A Special Case - Blum Integer

Definition 4. If $n = pq$ where p and q are primes both congruent to 3 modulo 4 then n is called a Blum integer.

Theorem If n is a Blum integer then $a \in Q_n \Rightarrow a$ has 4 square roots exactly one of which belongs to Q_n; that particular square root is called the principle square root.

Proof Since $n = pq$ we know that there are $2^2 = 4$ square roots for each $a \in Q_n$.

Claim Each of the sets $\left(A_{p,1} \cap A_{q,1}\right)$, $\left(A_{p,1} \cap A_{q,-1}\right)$, $\left(A_{p,-1} \cap A_{q,1}\right)$ and $\left(A_{p,-1} \cap A_{q,-1}\right)$ contains exactly one square root.

Proof of claim; Exercise 18. (Extra Credit)

Hint: First consider the case $a = 1$. Recall 1, p-1 are the square roots of 1 modulo p and 1, q-1 are the square roots of 1 modulo q. Also each square root of 1 modulo pq is the solution of the Chinese Remainder theorem system

$$x \equiv x_1 \pmod p$$
$$x \equiv x_2 \pmod q$$

where $x_1 = 1$ or p-1 and $x_2 = 1$ or q-1. Prove the solution for $x_1 = 1$, $x_2 =$ q-1 belongs to $A_{p-1} \cap A_{q-1}$ etc.

Corollary For a Blum integer $n = pq$ the function f: $Q_n \to Q_n$, $f(x) = x^2$, is a bijection and $f^{-1}(x) = x^{\left[(p-1)(q-1)+4\right]/8} \pmod n$

Proof Exercise 19 (Extra Credit)

Exercise 20. Find all square roots of 4 in Z_{21}; which is the principal one?

We complete this excursion in number theory by stating an algorithm for the computation of $\left(\frac{a}{Q}\right)$, where Q is odd, which DOESN'T require the factorization of Q. First -a preliminary result.

Lemma 2. If n is odd and $a = 2^e\ a_1$, where a_1 is odd, then

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

Proof Of course

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

But

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

Algorithm 1. Jacob (a, n)

INPUT: n odd, $n \geq 3$ and $0 \leq a < n$

OUTPUT: $\left(\frac{a}{n}\right)$

1. if $a = 0$ return 0
2. if $a = 1$ return 1
3. Write $a = 2^e a_1$, a_1 odd
4. if e is even set $s \leftarrow 1$. Otherwise set $s \leftarrow 1$ if $n \equiv 1$ or 7 (mod 8) or set $s \leftarrow -1$ if $n \equiv 3$ or 5 (mod 8)
5. if $n \equiv 3 \pmod 4$ and $a_1 \equiv 3 \pmod 4$ set $s \leftarrow -s$
6. Set $n_1 \leftarrow n \bmod a$
7. if $n_1 = 1$ return s; else return $s \left(\frac{n_1}{a_1}\right)$

Remark 5. The complexity is $O\left((\lg n)^2\right)$.