Certain Quadratic Residues for Twin Primes

Ali Astaneh Ph.D.(Lon), Vancouver BC, Canada

The well over a century old unsettled "twin prime" conjecture claims that there are infinitely many twin prime numbers of the form $(p, p+2)$. It is readily concluded at secondary math level that any such twin pair of primes, except for the first two pairs (2,3) and (3,5), should be of the form $(6n-1, 6n+1)$ for some integer n. This article presents necessary condition(s) on the integral parameter n if $(6n-1, 6n+1)$ are to be a twin prime pair. For Example Proposition 2 of the article shows that when the twin prime is of the particular form $(12n-1, 2n+1)$ and n is an odd, then n is necessarily a quadratic residue both $mod\ (6n-1)$ and $mod\ (6n+1)$.
The article has been arranged to present a Lemma first followed by two Propositions, and a final main Theorem. The idea behind this arrangement has been the more straightforward proof of the Lemma would be an adequate warm up to follow the proofs of the two propositions, which in turn make it easier to follow the proof of the Theorem. And a Corollary to the main Theorem will extend the similar assertion of Proposition 2 to all factors of both and the odd integral parameter n.
A few concrete numerical Examples are brought up after Propositions and the Theorem to show how they are applied in practice.
Since all proofs for the Lemma, the two Propositions, and the main Theorem make use of celebrated Gausse's Lemma on quadratic residues for prime numbers, it would be in order first to recall that, given a prime number p, an integer a is called a quadratic residue $mod\ (p)$ if there is an integer x such that $x^2 \equiv a\ mod\ (p)$. If such integer x doesn't exist a is called a non-quadratic residue $mod\ (p)$. Also the Legendre's symbol $\left(\frac{a}{p}\right)$ involved in Gausse's Lemma for a prime number p and an integer a is simply defined to be $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue mod (p), $\left(\frac{a}{p}\right) = 0$ if $p|a$, and $\left(\frac{a}{p}\right) = -1$ if a a non-quadratic residue mod (p). I also recall Gausse's Lemma that asserts if $U_p = \{1, 2, 3, \dots, p-1\}$ and if $a \in U_p$ then $\left(\frac{a}{p}\right) = (-1)^{\mu}$, where $\mu = |aP \cap N|$ is the number of members of the set $aP \cap N$ with P being the set $P = \left\{1, 2, 3, \dots, \frac{p-1}{2}\right\}$, $N = -P$, and $aP = \left\{a, 2a, 3a, \dots, \frac{p-1}{2}a\right\}$. And finally Q_p denotes the subgroup of U_p consisting of quadratic residues $mod\ (p)$.

Lemma : Let $(6n-1, 6n+1)$ be any pair of twin primes. Then

$$\left(\frac{3}{6n-1}\right) = \left(\frac{3}{6n+1}\right) = (-1)^n$$

Note, that the Lemma implies that when n is odd 3 is a non-quadratic residue both $mod(6n-1)$ and $mod(6n+1)$, for example considering that $n = 3$ for the twine primes (17,19), $3 \notin Q_{17}$ and $3 \notin Q_{19}$. But for the twine primes (71,73), since $n = 12$, $3 \in Q_{71}$ and $3 \in Q_{73}$, as $28^2 \equiv 3 mod(71)$ and $21^2 \equiv 3 mod(73)$.

Proof: (a) Let $p = 6n+1$ first, then $\frac{p-1}{2} = \frac{6n+1-1}{2} = 3n$, so that $P = \{1, 2, 3, \dots, 3n\}$ and $3P = \{3, 6, 9, , \dots, , 9n\}$.
We now arrange members of $3P$ to look like a 3 by n matrix as follows

$$3P = \{ \quad 3, \quad 6, \quad 9, \quad \dots, \quad 3n-3, \quad 3n,$$

$3n+3, \quad 3n+6, \quad 3n+9, \quad \dots, \quad 6n-3, \quad 6n$
$6n+3, \quad 6n+6, \quad 6n+9, \quad \dots, \quad 9n-3, \quad 9n \quad \}$

Next, we represent the set $3P$ in such a way that all members in the new representation are congruent to above members of $3P \ mod\ (6n+1)$ in exact respective order. To this end, since members of the first row are already in the set P we leave the first row as it is, however we replace all members u of the second and third row by their congruent $u-(6n+1) \equiv u \ mod\ (6n+1)$, and get

$3P = \{ \quad 3, \quad 6, \quad 9, \quad \dots, \quad 3n-3, \quad 3n,$
$-3n+2, \quad -3n+6, \quad -3n+9, \quad \dots, \quad -4, \quad -1,$
$2, \quad 5 \quad 8, \quad \dots, \quad 3n-4, \quad 3n-1 \quad \}$

As it is observed, only the entire members of the second row in this representation of $3P$ are in the set of $N=-P$. Therefore of $\mu = |\, nP \cap N| = n$, and by Gausse's Lemma, $\left(\frac{3}{6n+1}\right) = (-1)^n$.

(b) In this case $\frac{p-1}{2} = \frac{6n-1-1}{2} = 3n-1$, so that $P = \{1, 2, 3, \dots, 3n-1\}$, and $3P = \{3, 6, 9, , \dots, \ , 9n-3\}$. To prove this case, we again arrange the set $3P$ in three different rows, but in contrast with the first case this time we would rather have the first $n-1$ members of $3P$ as the first row, and the next n members of $3P$ as the second row and finally the the last n members of $3P$ as the third row, so that the total number in the three rows will be $(n-1)+n+n = 3n-1$, as expected,

$3P = \{ \quad 3, \quad 6, \quad 9, \quad \dots, \quad 3n-3,$
$3n, \quad 3n+3, \quad 3n+6, \quad \dots, \quad 6n-6, \quad 6n-3$
$6n, \quad 6n+3, \quad 6n+6, \quad \dots, \quad 9n-6, \quad 9n-3 \quad \}$

Next, again we represent the set $3P$ in such a way that all members in the new representation are congruent to the above members $mod\ (6n-1)$ in the same respective order. To this end, again members of the first row are already in the set P so we leave the first row unchanged, but we replace all members u of the second and third row by their congruent $u-(6n-1) \equiv u \ mod\ (6n-1)$, and get

$3P = \{ \quad 3, \quad 6, \quad 9, \quad \dots, \quad 3n-3,$
$-3n+1, \quad -3n+4, \quad -3n+7, \quad \dots, \quad -5, \quad -2$
$1, \quad 4 \quad 7, \quad \dots, \quad 3n-5 \quad 3n-2, \quad \}$

Again we observe, only the entire n members of the second row in this representation of $3P$ are in the set $N=-P$. Therefore of $\mu = |\, nP \cap N| = n$, and by Gausses Lemma, $\left(\frac{3}{6n-1}\right) = (-1)^n$.

Excercise1: Use the same method of proof of the Lemma, and show that, assuming $(6n-1, 6n+1)$ are twins primes,

(a) If n is even then $\left(\frac{2}{6n-1}\right) = \left(\frac{2}{6n+1}\right) = (-1)^{\frac{3n}{2}}$.

(b) If n is odd then $\left(\frac{2}{6n-1}\right) = (-1)^{\frac{3n-1}{2}} = (-1)^{\frac{(3n+1)}{2}} = \left(\frac{2}{6n+1}\right)$.

(c) Use the above Lemma, parts **(a)** and **(b)** of the Exercise, and the formula $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and show that when n is even $\left(\frac{6}{6n-1}\right) = \left(\frac{6}{6n+1}\right) = (-1)^{\frac{5n}{2}}$,

but when n is odd then, $\left(\frac{6}{6n+1}\right) = (-1)^{\frac{5n+1}{2}}$.

Proposition 1: If n is an odd number and $(6n-1, 6n+1)$ are twin primes, then

$$\left(\frac{n}{6n-1}\right) = \left(\frac{n}{6n+1}\right) = (-1)^{\frac{3(n-1)}{2}}. \qquad (1)$$

Proof: We will show that both $\left(\frac{n}{6n+1}\right)$ and $\left(\frac{n}{6n-1}\right)$ are each equal to $(-1)^{\frac{3(n-1)}{2}}$, in two separate parts, and in that order.

(A) To prove the part $\left(\frac{n}{6n+1}\right) = (-1)^{\frac{3(n-1)}{2}}$, we consider $p = 6n + 1$.

Since $\frac{p-1}{2} = \frac{6n+1-1}{2} = 3n$, both sets $P = \{1, 2, 3, \dots, 3n\}$ and $nP = \{n, 2n, 3n, \dots, 3n^2\}$ have $3n$ members. Therefore display the set nP similar to an n by 3 matrix where the first row has the first 3 members of In order to prove (1) for this case, since P (and also nP) has $3n$ members of nP , the second row then next three members of nP, ..., and the last row the last three members of nP as ,

$$\begin{array}{lccc} nP = \{ & n, & 2n, & 3n \\ & 4n, & 5n, & 6n \\ & 7n, & 8n, & 9n \\ & 10n, & 11n, & 12n \\ & 13n, & 14n, & 15n \\ & & \dots & \\ & (3n-5)n, & (3n-4)n, & (3n-3)n \\ & (3n-2)n, & (3n-1)n, & 3n^2 \quad \} \end{array}$$

Next we are going to represent the set nP in such a way that in the new representations all members are in the precise respective order congruent to the above members $mod\ (6n + 1)$. Since the fiirst three numbers on the first row above are already members of P we leave the first row above unchanged. However, we replace all members u of the second and third rows by $u - (6n + 1) \equiv u\ mod(6n + 1)$. Then we replace all members v of the fourth and fifth rows by $v - 2(6n + 1) \equiv v\ mod\ (6n + 1)$, and like wise we replace all members w of the sixth and seventh rows by $w - 3(6n + 1) \equiv w\ mod(6n + 1)$, and ….., we continue in this way, until we finally replace the members z of the last two $(n-1)th$ and nth rows by $z - \frac{(n-1)}{2}(6n + 1) \equiv z\ mod(6n + 1)$. Having completed this task we see that the set nP will have the following form,

$$\begin{array}{lccc} nP = \{ & n, & 2n, & 3n, \\ & \text{- 2n-1}, & \text{- n-1 ,} & \text{- 1,} \\ & \text{n-1,} & \text{2n -1,} & \text{3n -1,} \\ & \text{2n -2,} & \text{n – 2,} & \text{- 2,} \\ & \text{n - 2,} & \text{2n -2 ,} & \text{3n -2} \\ & & \dots & \\ & \frac{-5n+1}{2}, & \frac{-3n+1}{2}, & \frac{-n+1}{2}, \\ & \frac{n+1}{2}, & \frac{3n+1}{2}, & \frac{5n+1}{2} \quad \} \end{array}$$

Note that, since n is odd, the fractions on the last two rows above are all integers. Next, as we observe from above congruent representation of nP that, starting from the second row down to the last, the entire numbers in each row belong to N and P alternatively, while the numbers in the last row entirely belonging to P. Since each row contains three number, and except for first row the set nP has $(n - 1)$ rows, the number of members in the set nP which are at the same time members of N is

exactly $3 \times \frac{(n-1)}{2} = \frac{3(n-1)}{2}$, as claimed. Therefore, by Gausse's Lemma we have $\left(\frac{n}{6n+1}\right) = (-1)^{\frac{3(n-1)}{2}}$, and the proof of this part is complete.

(B) Now consider the case where the prime number is $p = 6n - 1$. Since $\frac{p-1}{2} = \frac{6n-1-1}{2} = 3n - 1$, this time the set P has $3n - 1$ members; that is $P = \{1, 2, 3, \dots, 3n - 1\}$. However, to conclude (1) for this case we rather arrange the set $nP = \{n, 2n, 3n, \dots, (3n-1)n\}$ such that the first row has only the first two original members $n, 2n$ of nP (which already belong to P) but the remaining rows having three consecutive members of the set nP, just as in the proof of part (**A**). Note that with this arrangement, except for the first row, the set nP has $3(n-1)$ members from the second row down to the last, as seen bellow,

$nP =$ { n, $2n$

3n, 4n, 5n,

6n, 7n, 8n

9n, 10n, 11n,

12n, 13n, 14n

…

(3n -6) n, (3n-5) n, (3n-4) n

(3n -3) n, (3n-2) n, (3n-1) n }

From here, the rest of the proof would be goes exactly similar to the proof of the previous part **(A)** [except for replacing $(6n+1)$ by $(6n-1)$ all along]; meaning that starting from the second row we replace all members u of the second and third rows by $u - (6n-1) \equiv u \, mod(6n-1)$, and replace all members v of the fourth and fifth rows by $v - 2(6n-1) \equiv v \, mod\,(6n-1)$. Then likewise replace all members w of the sixth and seventh rows by $w - 3(6n-1) \equiv w \, mod(6n-1)$, and, again we continue in this way until we finally replace all members z of the last two $(n-1)th$ and nth row by $z - \frac{(n-1)}{2}(6n-1) \equiv v \, mod(6n-1)$. Having completed this task, after simplifications of all members of nP from second row down to the last, we obtain a representation of the set nP as,

$nP =$ { n, $2n$

$-3n+1$, $-2n+1$, $-n+1$

1, , $n+1$, $2n+1$

$-3n+2$, $-2n+1$, $-n+1$

2, $n+2$, $2n+2$

…

$\frac{-5n-1}{2}$, $\frac{-3n-1}{2}$, $\frac{-n-1}{2}$,

$\frac{n-1}{2}$, $\frac{3n-1}{2}$, $\frac{5n-1}{2}$ }

Note that, since n is odd, the fractions on last two rows are indeed all integers. Again, as we observe from the above representation of the set nP, starting from the second row we have $3n-3$ members in, each row having three numbers, which means (except for the first row) we have $n-1$, and again starting from the second row (whose members belong to $N = -P$) members of each row entirely belong to N and P alternatively, while the entire numbers in the last row belong to P. Again It

follows that there are exactly $\frac{1}{2}(3n-3) = \frac{3(n-1)}{2}$ members in the set $aP \cap N$, and therefore by Gausse's Lemma

$$\left(\frac{n}{6n-1}\right) = \mu = |aP \cap N| \ = \ (-1)^{\frac{3(n-1)}{2}}.$$

Corollary 1 If n is an odd number and $(6n-1, 6n+1)$ are twin primes, then
(i) If $n \equiv 1 \ mod\ (4)$ then n is a quadratic residues both *mod* $(6n-1)$ and $mod(6n+1)$.
(ii) If $n \equiv 3 \ mod\ (4)$ then n is a non-quadratic residue neither *mod* $(6n-1)$ and nor $mod(6n+1)$.

proof: (i) If $n \equiv 1 \ mod\ (4)$, then $n = 4k+1$, for some integer k, then

$$\left(\frac{n}{6n-1}\right) = \left(\frac{n}{6n+1}\right) = (-1)^{6k} = 1.$$

(ii) If $n \equiv 3 \ mod\ (4)$, then $n = 4k+3$, for some integer k, then

$$\left(\frac{n}{6n-1}\right) = \left(\frac{n}{6n+1}\right) = (-1)^{3(2k+1)} = -1.$$

Example 1:

(i) For twin primes $(29, 31)$, $n = 5 \equiv 1 \ mod\ (4)$, $11^2 \equiv 29^2 \equiv 5 \ mod\ (29)$, and $6^2 \equiv 25^2 \equiv 5 \ mod\ (31)$.

(ii) For twin primes $(101,103)$, $n = 17 \equiv 1 \ mod\ (4)$, $44^2 \equiv 57^2 \equiv 17 \ mod\ (101)$, and $29^2 \equiv 74^2 \equiv 17 \ mod\ (103)$. Also for twin primes $(101,103)$, $n = 77 \equiv 1 \ mod\ (4)$, $186^2 \equiv 73 \ mod\ (437)$, and $103^2 \equiv 73 \ mod\ (439)$.

(ii) For twin primes $(437,439)$, since $n = 73 \ mod\ (4)$, the unit 3 is a non-quadratic residue neither $mod\ (17)$ nor $mod\ (19)$. Also, for twin primes $(41,43)$, since $n = 7 \equiv 3 \ mod\ (4)$, the unit 7 is a non-quadratic residue neither $mod\ (41)$ nor $mod\ (43)$.

In the following Exercise, parts **(a)** can be concluded as a direct application of Legendre's Criterion,

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

However part **(b)** can concluded by the method used in the proof of the above Proposition.

Exercise 2: Show that, if $(6n-1, 6n+1)$ are twin primes, then

(a) $\left(\frac{-1}{6n-1}\right) = (-1)^{3n-1} = 1, \quad \left(\frac{-1}{6n+1}\right) = (-1)^{3n}$.
Therefore $-1 \in Q_{6n-1}$, but -1 isn't a member of Q_{6n+1}.
(b) $\left(\frac{6n}{6n-1}\right) = (-1)^{3n}$, but $\left(\frac{6n}{6n-1}\right) = 1$, which means $6n \in Q_{6n-1}$.

Remark 1: Since quadratic residues are also defined for composite numbers in textbooks, just in case a reader wonders whether the converse of part (i) of the above Corollary; which means whether conditions $n \in Q_{6n-1}$ and $n \in Q_{6n+1}$ imply $(6n-1, 6n+1)$ are twin primes, here are two an examples to the contrary:

(i) $73 \in Q_{437}$ as $103^2 \equiv 73 \ mod(437)$ and $73 \in Q_{439}$ as $186^2 \equiv 73 \ mod(439)$, but 437 isn't a prime number.

(ii) $9 \in Q_{53}$ as $3^2 \equiv 9 \ mod(53)$, and $9 \in Q_{55}$ as $8^2 \equiv 9 \ mod(55)$, , but 55 isn't a prime number.

Proposition 2: If n is an odd number and $(12n-1,\ 12n+1)$ are twin primes, then $n \in Q_{2n-1}$ and $n \in Q_{2n+1}$. That is $\left(\frac{n}{12n-1}\right) = \left(\frac{n}{12n+1}\right) = 1$ (2)

Proof: The proof is very similar to that of Proposition 1, so I will be briefer about it. Again we use Gausse's Lemma to prove (2). As in proof of Proposition 1 we first show that $\left(\frac{n}{12n+1}\right) = 1$.

(A) Consider $p = 12n+1$ first, then since $\frac{p-1}{2} = \frac{12n+1-1}{2} = 6n$ we have $P = \{1, 2, 3, \dots, 6n\}$ and $nP = \{n, 2n,\ 3n, \dots,\ , 6n^2\}$. In order to prove (2) for this case, since P (and also nP) has $6n$ members we first arrange members of nP in n rows, each having 6 members as follows ,

$nP = \{$ n, 2n, 3n, 4n, 5n, 6n,
7n, 8n, 9n, 10n, 11n, 12n,
13n, 14n, 15n, 16n, 17n, 18n
19n, 20n, 21n, 22n, 23n, 24n
…
(6n -11) n, (6n-10) n, (6n-9) n, (6n -8) n, (6n-7) n, (6n-6) n
(6n -5) n, (6n-4) n, (6n-3) n, (6n -2) n, (6n-1) n, (6n) n }

The six numbers on the first row of the above set already belong to P, so it is enough to show that from the second row down to the last one there are $3(n-1)$ members belonging to $N = -P$, because, $3(n-1)$ being an even number, by Gausse's Lemma we will have $\left(\frac{n}{12n+1}\right) = (-1)^{3(n-1)} = 1$ .To this end, just as in the proof of Proposition1, starting from the second row we replace all members u of the second and third rows by $u - (12n+1) \equiv u\ mod(12n+1)$, then we replace all members v of the fourth and fifth rows by $v - 2(12n+1) \equiv v\ mod\ (12n+1)$, and likewise all members w of the sixth and seventh rows by $w - 3(12n+1) \equiv w\ mod(12n+1)$, and ….., we continue in this way, until we finally replace the members z of the last two $(n-1)th$ and nth rows by $z - \frac{(n-1)}{2}(12n+1) \equiv v\ mod(12n+1)$. Having completed this task we see that the set nP above, after simplifications of its members, starting from second row down to the last, we will get the following set, as a representation of nP, having the same class of numbers $mod(12n+1)$ expressed in the same order of its members,

nP
$= \{$ n, $2n$, $3n$, $4n$, $5n$, $6n$
5n-1, - 4n-1 ,- 3n - 1,- 2n-1, -n-1, -1,
n-1, 2n-1, 3n-1, 4n-1, 5n-1, 6n -1,
-5n-2, -4n -2, - - 3n-2, -2n-2, -n-2, -2
n-2, 2n-2, 3n-2, 4n-2, 5n-2, 6n-2
…
$\frac{-11n+1}{2}$, $\frac{-9n+1}{2}$, $\frac{-7n+1}{2}$, $\frac{-5n+1}{2}$, $\frac{-3n+1}{2}$, $\frac{-n+1}{2}$
$\frac{n+1}{2}$, $\frac{3n+1}{2}$, $\frac{5n+1}{2}$, $\frac{7n+1}{2}$, $\frac{9n+1}{2}$, $\frac{11n+1}{2}$ $\}$

Note that since n is odd, the fractions in the last two rows are indeed integers. Now as we observe from above arrangement, starting from the second row down to the last, the entire numbers in each row alternatively belong to N and P respectively, while the numbers in the last row entirely belonging to P. Since each row contains six numbers and except for first row the set nP has $(n-1)$ other rows, the number

of members in the set nP that are at the same time members of N is exactly $3(n-1)$, as claimed. So the proof of this part is complete.

(B) Now consider the case where the prime number is $p = 12n-1$. Since $\frac{p-1}{2} = \frac{12n-1-1}{2} = 6n-1$, this time the set P has $6n-1$ members; that is $P = \{1, 2, 3, \dots, 6n-1\}$. To conclude (2) for this case we rather arrange the set $nP = \{n, 2n, 3n, \dots, (6n-1)n\}$ such that the first row has only the first five original members $n, 2n, 3n, 4n, 5n$ of nP (which happen to belong to P) but the remaining $n-1$ rows, each having the next six consecutive members of nP, as in the proof of the first part (**A**). Note that with this arrangement, except for the first row, the set nP has $6n-1-5 = 6(n-1)$ members from the second row down to the last, as seen bellow,

nP = { n, $2n$, 3n, 4n, 5n,
6n, 7n, 8n, 9n, 10n, 11n,
12n, 13n, 14n, 15n, 16n, 17n,
18 n, 19n, 20n, 21n, 22n, 23n
…,
(6n -12) n, (6n-11) n, (6n-10) n, (6n -9) n, (6n-8) n, (6n-7) n
(6n -6) n, (6n-5) n, (6n-4) n, (6n -3) n, (6n-2) n, (6n-1) n }

From here, the rest of the proof would be goes exactly similar to the proof of the first case **(A)** except for replacing $(12n+1)$ by $(12n-1)$ all along.

It will then follow that the set nP has the following representation whose respective members will eventually simplify as $nP =$

{ n, $2n$, $3n$, $4n$, $5n$,
- 6n+1, - 5n+1, - 4n+1, - 3n+1, -2n+1, -n+1,
1, n+1, 2n+1, 3n+1, 4n+1, 5n +1,
-6n+2, -5n +2, -4n+2, -3n+2, - 2n+2 ,-n+2
2, n+2, 2n+2, 3n+2 , 4n+2, 5n+2
…
$\frac{-11n-1}{2}$, $\frac{-9n-1}{2}$, $\frac{-7n-1}{2}$, $\frac{-5n-1}{2}$, $\frac{-3n-1}{2}$, $\frac{-n-1}{2}$
$\frac{n-1}{2}$, $\frac{3n-1}{2}$, $\frac{5n-1}{2}$, $\frac{7n-1}{2}$, $\frac{9n-1}{2}$, $\frac{11n-1}{2}$ }

Note that, since n is odd, the fractions above are indeed all integers.

Again, as observe from the above representation of the set nP, starting from the second row we have $6n$— $1-5 = 6(n-1)$ members in the set, each row having six numbers, each row alternatively belong to N and P, while numbers in the last row belong to P. It follows that there are exactly $\frac{1}{2} \times 6(n-1) = 3(n-1)$ members in the set $aP \cap N$, and therefore by Gausse's Lemma

$$\left(\frac{n}{12n-1}\right) = \mu = |aP \cap N| = (-1)^{3(n-1)} = 1,$$

as $3(n-1)$ is an even number. This completes the proof of the Proposition 2.

Example 2:

For twin primes $(59, 61) = (12 \times 5 - 1, 12 \times 5 + 1)$, where $n = 5$, we have

$$8^2 \equiv 51^2 \equiv 5 \ mod\ (59), \text{ and } 26^2 \equiv 35^2 \equiv 5 \ mod\ (61).$$

So, $\left(\frac{5}{59}\right) = \left(\frac{5}{61}\right) = 1$.

And now I bring the main Theorem of the article,

Theorem (Astaneh)**:** Let $k = 1, 2, 3, \dots$, and $(6kn - 1,\ 6kn + 1)$ a twin prime .

(I) If n a odd, then

$$\left(\frac{n}{6kn-1}\right) = \left(\frac{n}{6kn+1}\right) = (-1)^{\frac{3k(n-1)}{2}}. \qquad (3)$$

(II) If n is an even number of the form $n = 2^l$ n', where n' is odd, then

$$\left(\frac{n}{6kn-1}\right) = \left(\frac{2}{6kn-1}\right)^l. \qquad (4)$$

$$\left(\frac{n}{6kn+1}\right) = \left(\frac{2}{6kn+1}\right)^l \qquad (5)$$

Proof: In the light of the proofs delivered for Propositions 1&2, the plan of the proof should be pretty clear, so her we go,

(I) Let n be odd. We will prove (3), by showing $\left(\frac{n}{6kn+1}\right) = (-1)^{\frac{3k(n-1)}{2}}$ and $\left(\frac{n}{6kn-1}\right) = (-1)^{\frac{3k(n-1)}{2}}$, separately and in that order.

(A) Consider the prime number $p = 6kn + 1$ first. Since $\frac{p-1}{2} = \frac{6kn+1-1}{2} = 3kn$ we have $P = \{1, 2, 3, \dots, 3kn\}$ and $nP = \{n, 2n, 3n, \dots, , 3kn^2\}$. In order to prove (3) for this case, since P (and thus nP) has $3kn$ members we first arrange members of nP in n rows, each row having $3k$ members as ,

$$\begin{array}{llll}
nP = \{ & n, & 2n, \dots, & (3k-1)n, \quad 3kn, \\
& (3k+1)n, & (3k+2)n, \dots, & (6k-1)n, \quad 6kn, \\
& (6k+1)n, & (6k+2)n, \dots, & (9k-1)n, \quad 9kn, \\
& (9k+1)n, & (9k+2)n, \dots, & (12k-1)n, \quad 12kn, \\
& (12k+1)n, & (12k+2)n, \dots, & (12k-1)n, \quad 15kn, \\
& & \dots, & \\
& [3(n-2)k+1]n, & [3(n-2)k+2]n, \dots, & 3kn^2 - 3kn - n, \quad 3kn^2 - 3kn \\
& [3(n-1)k+1]n, & [3(n-1)k+2]n, \dots, & 3kn^2 - n, \quad 3kn^2 \quad \}
\end{array}$$

The $3k$ numbers on the first row of the above set already belong to P, so it is enough to show that starting from the second row down to the last there are $\frac{3k(n-1)}{2}$ members belonging to $N = -P$ .To this end, just as in the proof of Proposition1&2, starting from the second row we replace all members u of the second and third rows by $u - (6kn + 1) \equiv u\ mod(6kn + 1)$, then we replace all members v of the fourth and fifth rows by $v - 2(6kn + 1) \equiv v\ mod\ (6kn + 1)$, and likewise all members w of the sixth and seventh rows by $w - 3(6kn + 1) \equiv w\ mod(6kn + 1)$, and ….., we continue in this way, until we finally replace the members z of the last two $(n-1)th$ and nth rows by $z - \frac{(n-1)}{2}(6kn + 1) \equiv z\ mod(6kn + 1)$. Having completed this task we see that the set nP above, after simplifications of its members, starting from second row down to the last, will have the following representation of nP, having the same class of numbers $mod(6kn + 1)$ expressed in the same order of its members,

$$\begin{array}{llll}
nP = \{ & n, & 2n, \dots, & (3k-1)n, \quad 3kn, \\
& -3kn + n - 1, & -3kn + 2n - 1, \dots, & -n - 1, \quad -1, \\
& n - 1, & 2n - 1, \dots, & 3kn - n + 1, \quad 3kn - 1, \\
& -3kn + n - 2, & -3kn + 2n - 2, \dots, & -n - 2, \quad -2,
\end{array}$$

$$n-2, \quad 2n-2, \quad \ldots, \quad 3kn-n-2, \quad 3kn-2,$$

$$\ldots,$$

$$, \quad \frac{1-(6k+1)n}{2}, \frac{1-(6k-1)n}{2} \quad \ldots, \quad \frac{-3n+1}{2}, \quad \frac{-n+1}{2}$$

$$\frac{n+1}{2}, \quad \frac{3n+1}{2}, \quad \ldots, \quad \frac{(6k-1)n-1}{2}, \quad \frac{(6k+1)n-1}{2} \quad \}$$

Note that, since n is odd, the fractions above are indeed all integers.
Also, as we observe from above arrangement, starting from the second row down to the last, the entire numbers in each row alternatively belong to N and P respectively, while the numbers in the last row entirely belonging to P. Since each row contains 3k numbers and except for first row the set nP has $(n-1)$ other rows, the number of members in the set nP which are at the same time members of N is exactly $\frac{3k(n-1)}{2}$, as claimed. So by Gausse's Lemma $\left(\frac{n}{6kn+1}\right) = (-1)^{\frac{3k(n-1)}{2}}$, and the proof of this part is complete.

(B) Now consider the case where the prime number is $p = 6kn-1$. Since $\frac{p-1}{2} = \frac{6kn-1-1}{2} = 3kn-1$, this time the set P has $3kn-1$ members; that is $P = \{1, 2, 3, \ldots, 3kn-1\}$, and therefore so has $nP = \{n, 2n, 3n, \ldots, (3kn-1)n\}$. To conclude (3) for this case we rather arrange the set nPsuch that the first row has only the first $(3k-1)$ members of nP, and the remaining $(n-1)$ rows have $3k$ respective members of nP as follows

$$nP = \{ \quad n, \quad 2n, \quad \ldots, \quad (3k-1)n,$$
$$3kn, \quad (3k+1)n, \quad \ldots, \quad (6k-2)n, \quad (6k-1)n,$$
$$6kn, \quad (6k+1)n, \quad \ldots, \quad (9k-2)n, \quad (9k-1)n,$$
$$9kn, \quad (9k+1)n, \quad \ldots, \quad (12k-2)n, \quad (12k-1)n,$$
$$12kn, \quad (12k+1)n, \quad \ldots, \quad (15k-2)n, \quad (15k-1)n,$$
$$\ldots,$$
$$3k(n-2)n, \ [3(n-2)k+1]n, \ldots, \quad [3k(n-1)-2]n, \ [3k(n-1)-1]n$$
$$3k(n-1)n, \ [3k(n-1)+1]n, \ldots, \quad [3kn-1]n, \quad 3kn^2 \quad \}$$

Again, the first $(3k-1)$ numbers in the first row of the above set already belong to P, so it is enough to show that starting from the second row down to the last there are $\frac{3k(n-1)}{2}$ members belonging to $N = -P$ .To this end, just as in the case **(A)** , starting from the second row we replace all members u of the second and third rows by $u-(6kn-1) \equiv u \ mod(6kn-1)$, then we replace all members v of the fourth and fifth rows by $v-2(6kn-1) \equiv v \ mod\ (6kn-1)$, and likewise all members w of the sixth and seventh rows by $w-3(6kn-1) \equiv w \ mod(6kn-1)$, and ….., we continue in this way, until we finally replace the members z of the last two $(n-1)th$ and nth rows by $z-\frac{(n-1)}{2}(6kn-1) \equiv v \ mod(6kn-1)$. Having completed this task the set nP above, after simplifications of its members, starting from second row down to the last, will have the following representation , having the same class of numbers $mod(6kn-1)$,expressed in the same order of its members,

$$nP = \{ \quad n, \quad 2n, \quad \ldots, \quad (3k-1)n,$$
$$-6kn+1, \quad -6kn+n+1, \ldots, \quad -2n+1, \quad -n+1,$$
$$1, \quad n+1, \quad \ldots, \quad 3kn-2n+1, \quad 3kn-n+1,$$
$$-3kn+2, \quad -3kn+n+2, \ldots, \quad -2n+2, \quad -n+2,$$

$$2, \quad n+2 \quad \ldots, \quad 3kn-2n+1, \quad 3kn-n+2,$$
$$\ldots,$$
$$\frac{(-6k+1)n-1}{2}, \frac{(-6k+3)n-1}{2}, \ldots, \frac{(-3n-1)}{2}, \quad \frac{(-n-1)}{2},$$
$$\frac{n-1}{2}, \quad \frac{3n-1}{2}, \quad \ldots, \quad \frac{(6k-1)n-1}{2}, \quad \frac{(6k+1)n-1}{2} \quad \}$$

Again note that, since n is odd, the fractions above are indeed all integers. Also, as we observe from above arrangement, starting from the second row down to the last, the entire numbers in each row alternatively belong to N and P respectively, while the numbers in the last row entirely belonging to P. Since each row contains 3k numbers and except for first row the set nP has $(n-1)$ rows, the number of members in the set nP which are at the same time members of N is exactly $\frac{3k(n-1)}{2}$, as claimed. So by Gausse's Lemma $\left(\frac{n}{6kn+1}\right) = (-1)^{\frac{3k(n-1)}{2}}$. Hence proof of part **(I)** is complete.

(II) Since $n = 2^l n'$, for some $l = 1, 2, 3, \ldots$ and some odd integer n', we can look at the original twin prime as $(6Kn'-1, 6Kn'+1)$, with $K = 2^l k$. Now, since n' is odd, we can apply (3) to the pair $(6Kn'-1, 6Kn'+1)$ and get $\left(\frac{n'}{6Kn'-1}\right) = \left(\frac{n'}{6Kn'+1}\right) = (-1)^{\frac{3k(n'-1)}{2}} = (-1)^{\frac{3\times 2^l k(n'-1)}{2}} = 1$. Therefore,
$\left(\frac{n'}{6kn-1}\right) = \left(\frac{n'}{6kn+1}\right) = 1$, and,
$\left(\frac{n}{6kn-1}\right) = \left(\frac{2^l n'}{6kn-1}\right) = \left(\frac{n'}{6kn-1}\right)\left(\frac{2^l}{6kn-1}\right) = \left(\frac{2^l}{6kn-1}\right) = (\frac{2}{6kn-1})^l$
which means equality (4) holds. Similarly
$\left(\frac{n}{6kn+1}\right) = \left(\frac{2^l n'}{6kn+1}\right) = \left(\frac{n'}{6kn+1}\right)\left(\frac{2^l}{6kn+1}\right) = \left(\frac{2^l}{6kn+1}\right) = (\frac{2}{6kn+1})^l$,
and equality (5) also holds as well. Hence the proof the Theorem is complete.

Example 3: (I) For twin primes $(347,349) = (6\times 2\times 29-1, 6\times 2\times 29+1)$, where $k=2$ and $n=29$, since n is odd equality (3) in part **(I)** of Theorem implies
$$\left(\frac{29}{6\times 2\times 29-1}\right) = \left(\frac{29}{6\times 2\times 29+1}\right) = (-1)^{\frac{3k(n-1)}{2}} = (-1)^{\frac{3\times 2(29-1)}{2}} = 1.$$
So $29 \in Q_{347}$ and $29 \in Q_{349}$. Indeed $42^2 \equiv 29\ mod\ (347)$ and $99^2 \equiv 29\ mod\ (349)$.

(II) Consider the twin prime $(239,241) = (6\times 2\times 20-1, 6\times 2\times 20+1)$. Then $k=2$ and $n = 20 = 2^2\times 5$, which means $l=1$, $n'=5$. Then equality (4) in the Theorem implies $\left(\frac{20}{239}\right) = \left(\frac{2}{239}\right)^2$. Now since $99^2 \equiv 2\ mod\ (239)$, it follows that $\left(\frac{20}{347}\right) = 1$ which means $20 \in Q_{239}$. Also the equality (5) in the Theorem implies $\left(\frac{20}{241}\right) = \left(\frac{2}{241}\right)^2$, and since $23^2 \equiv 2\ mod\ (241)$, it also follows that $20 \in Q_{241}$.

Corollary 2: Let n be an odd number and let $(6kn-1, 6kn+1)$ be twin primes. If k is even and/or if $n \equiv 1\ mod\ (4)$, then n is a quadratic residue both $mod(6kn-1)$ and $mod(6kn+1)$.

Proof: Is left to the reader to conclude from the Theorem

Remark 2: When dealing with twin prime numbers, it would be relevant to mention as we consider positive integers along the number line, we may encounter very large but finite intervals consisting of consecutive composite integers. Indeed, if k is as large as you like, the set of k consecutive numbers,

$C_k = \{\ \ (k+1)!+2, (k+1)!+3,\ (k+1)!+4, \dots, (k+1)!+(k+1)\ \ \ \}$,

consists of composite number only, as the first integer in C_k is divisible by 2,the second by 3, the third by 4, … , and the last one by $(k+1)$ .However, in spite of this (and as to support the twin prime conjecture), if you subtract the last number in C_k from the first number in C_{k+1}, you get

$(k+2)!+2-[(k+1)!+(k+1)] = (k+1)\times(k+1)!+1-k$,

and it shows a much larger interval between C_k and C_{k+1} in which prime numbers (and so also perhaps twin primes) might show up.

On the other note, if $\{p_n\}$ represents the sequence of all prime number, it is known the series $\sum_1^\infty \frac{1}{p_n}$ diverges. In spite of this fact, in 1919 Viggo Brunt proved if the conjecture of the existence of infinite primes twins is a fact, then the series $\sum_1^\infty \frac{1}{q_n}$, where $\{q_n\}$ represents all members of twin prime, converges to what is known as Brunt's constant.

It may be relevant also to mention that the divergent series $\sum_1^\infty \frac{1}{p_n}$ of prime reciprocals (like any other divergent series $\sum_1^\infty a_n$for which $\lim_{n\to\bowtie} a_n = 0$) has infinitely many infinite subseries that converge. Indeed, given any small number $\epsilon > 0$ one can find a subseries of $\sum_1^\infty \frac{1}{p_n}$ that converges to a number lass than $\epsilon > 0$. To observe this, let $\epsilon > 0$ be arbitrary, and choose a number to satisfy $N > \frac{1}{\epsilon}+1$. Then for each positive integer $k = 1,2,3,\dots$ find a prime number p_k with $N^k < p_k$, then

$\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}+\cdots < \sum_1^\infty \frac{1}{N^k} = \frac{\frac{1}{N}}{1-\frac{1}{N}} = \frac{1}{N-1} < \epsilon$.

I Close the article by a Remark unrelated to quadratic residues, but about inverses modulus consecutive odd numbers, including twin primes. $(6n-1,\ 6n+1)$.

Remark 3: Let $6n-1,\ 6n+1$ be any two consecutive odd numbers, then $3n$ is the inverse of $(6n-1)\ mod\ (6n+1)$ and, at the same time, $3n$ is the inverse of $(6n+1)\ mod\ (6n-1)$.

Note that, since $(6n+1) \equiv 2 \bmod (6n-1)$ it also follows that $3n$ is also the inverse of $2 \bmod (6n-1)$, and likewise $(6n-1) \equiv -2 \bmod (6n+1)$

$-2 \bmod (6n+1)$ implies $3n$ is also the inverse of $-2 \bmod (6n+1)$.

Proofs: Simply follows from the two respective identities,

$$3n(6n-1) = 18n^2-3n = 18n^2-3n-1+1 = (6n+1)(3n-1)+1 \equiv 1 mod(6n+1)$$

and

$$3n(6n+1) = 18n^2+3n = 18n^2+3n-1+1 = (6n-1)(3n+1)+1\ .$$