ELECTRONIC RESEARCH ARCHIVE
Volume **29**, Number **6**, December **2021**

doi:10.3934/era.2021065
pp. **3853–3865**

A COMPUTABLE FORMULA FOR THE CLASS NUMBER OF THE IMAGINARY QUADRATIC FIELD $\mathbb{Q}(\sqrt{-p})$, $p = 4n - 1$

Jorge Garcia Villeda

One University Drive
Camarillo, CA 93012, USA

(Communicated by Zhi-Wei Sun)

Abstract. Using elementary methods, we count the quadratic residues of a prime number of the form $p = 4n - 1$ in a manner that has not been explored before. The simplicity of the pattern found leads to a novel formula for the class number h of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Such formula is computable and does not rely on the Dirichlet character or the Kronecker symbol at all. Examples are provided and formulas for the sum of the quadratic residues are also found.

1. **Introduction.** Given a prime number p and $0 < k < p$, we look at the residues of k^2 modulo p. When we add those residues we obtain the sum of quadratic residues relative to the prime number p. The question is, how does that sum behave? Is there a formula for such sum? What is that sum related to? Here are the answers to these simple questions. There is indeed a very simple formula for this sum when the number is of the form $p = 4n + 1$, in fact this sum is $\binom{p}{2}$. There is also a formula when the prime is of the form $4n - 1$, in fact this sum is $\binom{p}{2} - p \cdot h$ where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. When $p \equiv 3 \pmod 4$, $h(-p)$ is equal to the class number of primitive, positive-definite, integral binary quadratic forms of discriminant $-p$ and it can be calculated by counting the numbers of reduced, primitive, positive-definite, integral, binary quadratic forms of discriminant $-p$ (see [2] page 68.) Formulas for the class number when the prime is of the form $p = 4n - 1 > 3$ are

$$h(-p) = \frac{\sqrt{p}}{\pi} \sum_{r=1}^{\infty} \frac{\chi(r)}{r},$$

$$h(-p) = \frac{-1}{4p} \sum_{r=1}^{4p} r \cdot \left(\frac{p}{r}\right),$$

where χ is the Dirichlet character and $\left(\frac{p}{r}\right)$ is the Kronecker symbol (which is ultimately a Dirichlet character). The first formula is the Dirichlet class number formula and can be found in [3] and the second formula can be found in [5] (Corollary 1 p. 428).

A formula developed by Cohen [1] [Corollary 5.3.16] provides the class number.

2020 *Mathematics Subject Classification.* Primary: 11E41, 11R29; Secondary: 11E16.

Key words and phrases. Class number, quadratic residues, imaginary fields, quadratic field, sum of quadratic residues.

Theorem 1.1. *Let $D < -4$ be a fundamental discriminant. Then $h(-D)$ is the closest integer to the sum*

$$\sum_{n=1}^{N} \left(\frac{D}{n}\right) \cdot \left(\operatorname{erfc}\left(n\sqrt{\frac{\pi}{|D|}}\right) + \frac{\sqrt{|D|}}{\pi n} e^{-\pi n^2/|D|}\right)$$

where $\operatorname{erfc}(x) = \frac{2}{\pi}\int_x^\infty e^{-t^2}\,dt$, $N = \left\lfloor \sqrt{\frac{|D|\log|D|}{2\pi}} \right\rfloor$ *and* $\left(\frac{D}{n}\right)$ *is the Kronecker symbol.*

In Section 2 we will prove the basic lemmas as well as the definition of *residue* whereas in Section 3 we will establish the main result for the sum of quadratic residues. In Section 4 we establish several formulas for the class number when p is of the form $4n-1$ and finally in Section 5 we provide some examples and foresee some future work.

2. Sum of quadratic residues.

If we look at small primes of the form $p = 4n-1$ and we add the residues of k^2 and $(2n-k)^2$ mod p we observe some patterns as k ranges from 1 to $2n$. Unfortunately these patterns do not hold for larger primes, however, we need to make some adjustments to those patterns. The following lemmas will capture those patterns and these lemmas will be the building blocks of our main theorems.

Definition 2.1. Let q be a positive integer and $x \in \mathbb{Z}$. By $r_q(x)$ we denote the least non negative residue of x modulo q. Clearly

$$x = \lfloor x/q \rfloor \cdot q + r_q(x).$$

Lemma 2.2. *Let $n \in \mathbb{N}$, $p, h, r, k \in \mathbb{Z}$ such that p is prime, $p = 4n-1$, $k^2 = hp + r$, $0 \le r \le 4n-2$ and $0 \le k \le n$.*

(i) If $k \ge r - 3n + 2$ then

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2r - k + n.$$

(ii) If $k < r - 3n + 2$ then

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2r - k - 3n + 1.$$

Proof. Notice that

$$\begin{aligned}(2n-k)^2 &\equiv 4n^2 - 4nk + k^2 - (4n-1)(n-k) \pmod p \\ &= k^2 + n - k = hp + r + n - k \\ &\equiv r + n - k \pmod p.\end{aligned}$$

Clearly $0 \le r + n - k$. If $k \ge r - 3n + 2$, then $r + n - k \le 4n - 2$, hence

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2r - k + n.$$

This proves the first part. For the second part notice also that

$$\begin{aligned}(2n-k)^2 &\equiv r + n - k - 4n + 1 \pmod p \\ &= r - k - 3n + 1 \pmod p.\end{aligned}$$

Clearly $r-k-3n+1 \le 4n-2$. Since $k < r-3n+2$, $r-k-3n+1 = r+n-k-4n+1 > -1$, hence

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2r - k - 3n + 1.$$

□

Lemma 2.3. *Let $n \in \mathbb{N},\ p, k, m \in \mathbb{Z}$ such that p is prime, $p = 4n-1$ and $0 \le k \le n$.*

(i) If $mp - k < k^2 - k \le (m+1)p - n - 1$ then

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2k^2 - k + n - 2mp.$$

(ii) If $(m+1)p - n - 1 < k^2 - k < (m+1)p - k$ then

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2k^2 - k + n - (2m+1)p.$$

Proof. (i) Clearly $mp < k^2 \le (m+1)p + k - n - 1 \le (m+1)p - 1$. Hence there is $r \in \{1, 2, .., p-1\}$ such that $k^2 = mp + r$. Since

$$\begin{aligned} r - 3n + 2 &= k^2 - mp - 3n + 2 \\ &= k^2 - (m+1)p + n + 1 \le k. \end{aligned}$$

By Lemma 2.2,

$$\begin{aligned} r_p\left(k^2\right) + r_p\left((2n-k)^2\right) &= 2r + n - k = 2(k^2 - mp) + n - k \\ &= 2k^2 - k + n - 2mp. \end{aligned}$$

(ii) Clearly $mp < (m+1)p - n - 1 + k < k^2$. Since $k^2 < (m+1)p$, $mp < k^2 < (m+1)p$. Hence there is $r \in \{1, 2, .., p-1\}$ such that $k^2 = mp + r$. Since $r - 3n + 2 = k^2 - mp - 3n + 2 = k^2 - (m+1)p + n + 1 > k$, by Lemma 2.2,

$$\begin{aligned} r_p\left(k^2\right) + r_p\left((2n-k)^2\right) &= 2r - k - 3n + 1 \\ &= 2k^2 - 2mp - k - p + n \\ &= 2k^2 - k + n - (2m+1)p. \end{aligned}$$

□

Corollary 1. *Let $n \in \mathbb{N},\ p, k, \in \mathbb{Z}$ such that p is prime, $p = 4n-1$ and $0 \le k \le n$. Consider an integer $m \ge 0$.*

(i) If $\lceil \sqrt{mp} \rceil < k \le \frac{1}{2} + \frac{1}{2}\sqrt{1 + 4\left\lceil (m+1)p - n - 1 \right\rceil}$ then

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2k^2 - k + n - 2mp.$$

(ii) If $\frac{1}{2} + \frac{1}{2}\sqrt{1 + 4\left\lceil (m+1)p - n - 1 \right\rceil} < k < \lceil \sqrt{(m+1)p} \rceil$ then

$$r_p\left(k^2\right) + r_p\left((2n-k)^2\right) = 2k^2 - k + n - (2m+1)p.$$

Proof. Notice that $\sqrt{m} < k$ implies $mp - k < k^2 - k$, also the inequality $k \le \frac{1}{2} + \frac{1}{2}\sqrt{1 + 4\left\lceil (m+1)p - n - 1 \right\rceil}$ implies $4k^2 - 4k \le 4\left[(m+1)p - n - 1\right]$. Hence

$$mp - k < k^2 - k \le (m+1)p - n - 1,$$

and by Lemma 2.3 we have the result. The second part is done similarly. □

The following notation will be very useful for our future theorems and identities.

Notation. For $n \in \mathbb{N},\ m, \in \mathbb{Z}$ with p is prime, $p = 4n - 1$ and $m \ge 0$ we denote

$$\begin{aligned} Q_m &= \frac{1}{2} + \frac{1}{2}\sqrt{1 + 4\left\lceil (m+1)p - n - 1 \right\rceil} = \frac{1}{2} + \frac{1}{2}\sqrt{4mp + 3p - 4} \\ R_m &= \lceil \sqrt{mp} \rceil \\ M &= \left\lfloor \frac{n^2}{p} \right\rfloor. \end{aligned}$$

The following lemma will allow us to estimate the quadratic residues.

Lemma 2.4. *Using the previous notation, consider* $n \in \mathbb{N}$, $p = 4n-1$ *a prime number and* $r \in \{0, 1, ..., p-1\}$ *such that*

$$n^2 = Mp + r.$$

Assume that $M > 0$. *Then* $r \geq 1$. *If* $n = 11$ *then* $r = 4n - 9$ *and if* $n \neq 11$ *then* $r \leq 4n - 10$.

Proof. Clearly $r \geq 1$ otherwise p divides n which is impossible. If $n = 11$, then $p = 43$ and hence $n^2 = 121 = 2 \cdot 43 + 35$, therefore $r = 35 = 4 \cdot n - 9$. Assume now that $n \neq 11$. Let $y = M + 1$. Consider $u = 4n - r$, $u \geq 2$ and $f(y) = 4y^2 - (y + u - 1)$.

Case $u = 3$. Then $n^2 = Mp + 4n - 3$. Hence $(n-3)(n-1) = n^2 - 4n - 3 = Mp$, therefore p divides $(n-3)$ or p divides $(n-1)$. This forces $n = 3, p = 11, M = \left\lfloor \frac{9}{11} \right\rfloor = 0$ or $n = 1, p = 3, M = 0$, which is impossible.

Case $u = 4$. Then $(n-2)^2 = Mp$. This forces $n = 2, p = 7, M = \left\lfloor \frac{4}{7} \right\rfloor = 0$, which is also impossible.

Assume now that $u \neq 3, 4$. Now

$$n^2 = Mp + 4n - u = (M+1)p + 1 - u = y(4n-1) + 1 - u, \tag{1}$$

hence n satisfies $n^2 - n \cdot 4y + (y + u - 1) = 0$, therefore

$$n = 2y \pm \sqrt{4y^2 - (y + u - 1)},$$

hence there is a non-negative integer x such that $f(y) = x^2$. If $x = 0$ then $n = 2y$ and $0 = 4y^2 - (y + u - 1)$. From Equation 1, we have $4y^2 = y(4n-1) + 1 - u$, hence $y(4n-1) = y$. This forces $y = 0$ and $n = 0$ contradicting $n \geq 1$.. Hence necessarily $x > 0$. Therefore $4y^2 - x^2 = y + u - 1 \geq 1$ and then $y + x \leq u - 1$. Hence $y \in \{0, 1, 2, ..., u-2\}$. We know, $y \neq 0$. If $y = 1$ then $M = 0$ contrary to our assumption. Therefore $y \in \{2, ..., u-2\}$. We now continue analyzing the cases $u = 2, 5, 6, 7, ...$

Case $u = 2$. Then $y + x \leq 1$, this is impossible as $x \geq 1$ and $y \geq 2$.

Case $u = 5$. Then $y \in \{2, 3\}$. Clearly $f(2) = 10 \neq x^2$ and $f(3) = 29 \neq x^2$.

Case $u = 6$. Then $y \in \{2, 3, 4\}$. If $y = 2$, then $f(2) = 9 = x^2$, this forces $x = 3, n = 1, p = 3, M = 0$ which is impossible. Clearly $f(3) = 28 \neq x^2$ and $f(4) = 55 \neq x^2$.

Case $u = 7$. Then $y \in \{2, 3, 4, 5\}$. Clearly $f(2) = 8, f(3) = 27, f(4) = 54$ and $f(5) = 89$ none of which is a perfect square.

Case $u = 8$. Then $y \in \{2, 3, 4, 5, 6\}$. Clearly $f(2) = 7, f(3) = 26, f(4) = 53, f(5) = 88$ and $f(6) = 131$ none of which is a perfect square.

Case $u = 9$. Then $y \in \{2, 3, 4, 5, 6, 7\}$. Clearly $f(2) = 6, f(4) = 52, f(5) = 87, f(6) = 120$ and $f(7) = 181$ none of which is a perfect square. This leaves us with the case $y = 3$, which forces $f(3) = 25, x = 5, n \in \{11, 1\}$. But we know $n \neq 11$, hence $n = 1, M = 0$, which is impossible.

Therefore $u \geq 10$ and hence $r \leq 4n - 10$. □

The following lemma provides the computation of quadratic residues when n is congruent to 0,1,2 and 3 modulo 4 and $p = 4n - 1$. Such lemma will be useful when we provide some formulas regarding quadratic residues.

Lemma 2.5. *Let* $Q_m = \frac{1}{2} + \frac{1}{2}\sqrt{4mp + 3p - 4}\rfloor, R_m = \sqrt{mp}\rfloor$ *and* $M = \left\lfloor \frac{n^2}{p} \right\rfloor$. *If* $p = 4n - 1$ *is prime and* $r = r_p\left(n^2\right)$ *then* $M = \left\lfloor \frac{n}{4} \right\rfloor$ *and* r *is given in Table 1 for each possible* n *of the form* $4k, 4k+1, 4k+2$ *and* $4k+3$.

n	M	p	r
$4k$	k	$16k - 1$	M
$4k+1$	k	$16k + 3$	$5M + 1$
$4k+2$	k	$16k + 7$	$9M + 4$
$4k+3$	k	$16k + 11$	$13M + 9$

TABLE 1. The quadratic residues $r = r_p\left(n^2\right)$ for each of the four different cases of n.

Proof. We will verify that $M = \left\lfloor \dfrac{n^2}{4n-1} \right\rfloor = k$ in one case, the other cases are done similarly. Let $n = 4k,\ k \geq 1$. Clearly

$$k \cdot \big(4(4k) - 1\big) \leq 16k^2 < 16k^2 + 15k - 1 = (k+1) \cdot \big(4(4k) - 1\big),$$

hence $k \leq \dfrac{n^2}{4n-1} < k + 1$, therefore $M = \left\lfloor \dfrac{n^2}{4n-1} \right\rfloor = k$. Now, observe that

$$\begin{aligned}
(4k)^2 &= k \cdot \big(4(4k) - 1\big) + k, \\
(4k+1)^2 &= k \cdot \big(4(4k+1) - 1\big) + 5k + 1, \\
(4k+2)^2 &= k \cdot \big(4(4k+2) - 1\big) + 9k + 4, \\
(4k+3)^2 &= k \cdot \big(4(4k+3) - 1\big) + 13k + 9.
\end{aligned}$$

We can see that each of the numbers r in Table 1 satisfies $n^2 = Mp + r$ in each of the four different cases. □

The following lemma will allow us to place $n-1, n, n+1$ in the right interval as established in Corollary 1. This lemma and the following one will be useful to the proof of our main theorem which will come right after.

Lemma 2.6. *Let* $p = 4n-1$ *prime,* $Q_m = \frac{1}{2} + \frac{1}{2}\sqrt{4mp + 3p - 4}\rfloor, R_m = \sqrt{mp}\rfloor$, $M = \left\lfloor \frac{n^2}{p} \right\rfloor$ *and* $r = r_p\left(n^2\right)$. *Then*

(i) *For* $m \leq M - 1$, $R_m < Q_m < R_{m+1}$.
(ii) *If* $M \geq 1$ *then* $R_{M-1} < n - 1 < Q_M$.
(iii) *If* $M \geq 1$ *then* $R_{M-1} < n - 2 < Q_{M-1}$.
(iv) $R_M < n < Q_M$.
(v) $R_M < n + 1 < Q_{M+1}$.
(vi) $r \neq 2n - 3$, *and* $r \neq 2n - 2$. *If* $n > 1$ *then* $r \neq 2n - 1$.
(vii) *If* $M \geq 1$ *then* $n - 1 \notin (Q_{M-1}, R_M)$.
(viii) *If* $M \geq 1$ *then* $n - 1 < Q_{M-1} \implies n + 1 < Q_M \implies n + 1 \notin (Q_M, R_{M+1})$. *Also* $n - 1 < Q_{M-1} \iff r < 2n - 3$.
(ix) $R_M < n - 1 \implies R_{M+1} < n + 1 \implies n + 1 \notin (Q_M, R_{M+1})$.
(x) $Q_M < R_{M+1} \iff 2n - 2 < r$.
(xi) $Q_M < n + 2,\ R_{M+1} < n + 2$.

Proof. (i) Notice that $R_m < Q_m \iff 2 < 3n$ which is true for all n. Notice also that $Q_m < R_{m+1} \iff (m+1)(4n-1) < n^2 + 2n + 1$. Since $m \leq M - 1$, we have that $(m+1)(4n-1) \leq Mp = n^2 - r < n^2 + 2n + 1$.

(ii) Notice that $R_{M-1} < n-1 \iff (M-1)p < n^2-2n+1$. We certainly have $Mp-p = n^2-r-p < n^2-2n+1$. Also $n-1 < Q_M \iff n^2-3n+4 < (M+1)p-n-1 \iff n^2+4 < n^2-r+p+2n-5$, and certainly by Lemma 2.4, $r < 6n-10$.

(iii) We observe that $R_{M-1} < n-2 \iff (M-1)p < n^2-4n+4$. We do have $Mp-p < n^2-r-4n+1 < n^2-4n+4$. Likewise, $n-2 < Q_{M-1} \iff n^2-5n+6 < Mp-n-1$, we certainly have, by Lemma 2.4, $n^2-5n+6 < n^2-r-n-1$.

(iv) Observe that $R_M < n$ is equivalent to $Mp < n^2$ which is definitely true. Also $n < Q_M$ is equivalent to $n^2-n < Mp+p-n-1 = n^2-r+p-n-1$ which is true as $r < p-1$.

(v) Note that $R_M < n+1$ is equivalent to $Mp < n^2+2n+1$ which is true because $n^2-r < n^2+2n+1$. Also $n+1 < Q_M$ is equivalent to $n^2+n < (M+2)p-n-1 = n^2-r+2p-n-1$, this last inequality is true by Lemma 2.4.

(vi) If $r = 2n-2$ then

$$n^2+n(-4M-2)+M+2 = 0, \tag{2}$$

hence there is a non-negative integer x such that $(2M+1)^2-(M+2) = x^2$. Thus $2M+1+x \leq (2M+1)^2-x^2 = M+2$, therefore $M+x \leq 1$. This gives us three possibilities $M = 0, x = 0$ or $M = 0, x = 1$ or $M = 1, x = 0$. From $n = 2M+1 \pm x$ and Equation 2, each of the previous possibilities leads us to a contradiction.

If $r = 2n-3$ then $Mp = n^2-2n+3$ hence p divides $4n^2-8n+12$. Since p divides $4n^2-n$ and $8n-2$, we conclude that p divides $n+10$, which is not possible. Now let $n > 1$, and assume $r = 2n-1$. Then $Mp = (n-1)^2$ which forces $M = 0, n = 1$, contradicting our assumption.

(vii) If $n \in (Q_{M-1}, R_M)$, then $Mp-n-1 < n^2-3n+2$ and $n^2-2n+1 < Mp = n^2-r$, this forces $2n-3 < r < 2n-1$, i.e. $r = 2n-2$, which was proven impossible in case vi. Hence $n \in (Q_{M-1}, R_M)$ is impossible.

(viii) Clearly $n-1 < Q_{M-1} \iff r < 2n-3$. Now, $n+1 < Q_M$ iff $r \leq 2n-3$ iff $r < 2n-3$ as by case vi, $r \neq 2n-3$.

(ix) Observe that $R_M < n-1 \implies r > 2n-1$ and $R_{M+1} < n+1 \iff Mp+p < n^2+2n+1 \iff 2n-2 < r$. The results follows.

(x) Note that $Q_M < R_{M+1} \iff (M+1)p < n^2+2n+1 \iff 2n-2 < r$.

(xi) Observe that $R_{M+1} < n+2$ is equivalent to $Mp < n^2+4n+5$ which is the same as $0 < r+4n+5$, of course this last inequality is true. Finally, $Q_M < n+2$ is equivalent to $Mp < n^2+4$ which is the same as the true inequality $0 < r+4$.

□

Remark 1. Let x, y two real numbers. Then

$$\left|\{k \in \mathbb{Z} \ : \ x < k \leq y\}\right| = \lfloor y \rfloor - \lfloor x \rfloor .$$

Remark 2. Let $x \in \mathbb{R}$, $y \in \mathbb{R}-\mathbb{Z}$. Then

$$\left|\{k \in \mathbb{Z} \ : \ x < k < y\}\right| = \lfloor y \rfloor - \lfloor x \rfloor .$$

Lemma 2.7. *Let $p = 4n-1$ prime, $Q_m = \frac{1}{2}+\frac{1}{2}\sqrt{4mp+3p-4}$, $R_m = \sqrt{mp}$ and $M = \left\lfloor \frac{n^2}{p} \right\rfloor$. If $M \geq 1$, and $r = r_p\left(n^2\right)$. Then*

(i) Either $n-1 = \lfloor Q_{M-1} \rfloor = \lfloor R_M \rfloor$ or $n-2 = \lfloor Q_{M-1} \rfloor = \lfloor R_M \rfloor$.

(ii) Either $n+1=\lfloor Q_M\rfloor=\lfloor R_{M+1}\rfloor$ *or* $n=\lfloor Q_M\rfloor=\lfloor R_{M+1}\rfloor$.

Proof. From Lemma 2.6, $n-1\in(R_{M-1},Q_M)-(Q_{M-1},R_M)=(R_{M-1},Q_{M-1}]\cup[R_M,Q_M)$.

- Assume now $n-1\in(R_{M-1},Q_{M-1}]$. If $n-1=Q_{M-1}$ then $r=2n-3$ which is not possible, hence $n-1<Q_M$. By Lemma 2.6, $n+1<Q_M$ and $R_M<n$. Therefore $n-1=\lfloor Q_{M-1}\rfloor=\lfloor R_M\rfloor$. The situation looks like the one on Figure 1.

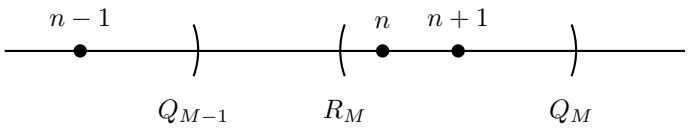

FIGURE 1. The resulting case when $n-1\in(R_{M-1},Q_{M-1}]$.

If $2n-2<r$, by Lemma 2.6 (x),(xi), $Q_M<R_{M+1}<n+2$. If $2n-2>r$, by Lemma 2.6 (x),(xi), $R_{M+1}\le Q_M<n+2$. In either case, $n+1<R_{M+1},Q_M<n+2$ and hence $n+1=\lfloor Q_M\rfloor=\lfloor R_{M+1}\rfloor$.

- Assume now $n-1\in[R_M,Q_M)$. If $n-1=R_M$ then $r=2n-1$ which, by Lemma 2.6, is not possible as $M\ge 1$. Hence $R_M<n-1$. By Lemma 2.6 (ix), $n<Q_M$. Therefore $n-2=\lfloor Q_{M-1}\rfloor=\lfloor R_M\rfloor$. The situation looks like the one on Figure 2

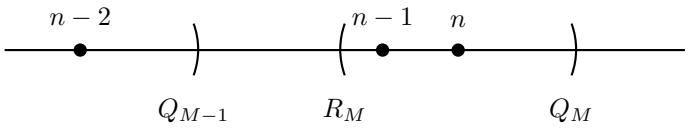

FIGURE 2. The resulting case when $n-1\in[R_M,Q_M)$.

Since $Q_{M-1}<n-1$, by Lemma 2.6 (viii),(x) $r>2n-3$, $Q_M<R_{M+1}$. Since $R_M<n-1$, by Lemma 2.6 (ix), $R_{M+1}<n+1$. Hence, $n<Q_M<R_{M+1}<n+1$ and hence $n=\lfloor Q_M\rfloor=\lfloor R_{M+1}\rfloor$.

□

3. **Main result.** The following theorem provides a formula to compute the sum of the quadratic residues modulo $p=4n-1$. Such a formula did not exist at the moment.

Theorem 3.1. *Let* $n\in\mathbb{N},n>1$ *such that* $p=4n-1$ *is prime. If* $Q_m=\frac{1}{2}+\frac{1}{2}\sqrt{4mp+3p-4}\rfloor, R_m=\sqrt{mp}\rfloor$ *and* $M=\left\lfloor\frac{n^2}{p}\right\rfloor$ *then*

$$\frac{1}{2}\sum_{k=1}^{p-1}r_p\left(k^2\right)=-p\sum_{m=0}^{M-1}(2m+1)\big(\lfloor R_{m+1}\rfloor-\lfloor R_m\rfloor\big)-2p\sum_{m=0}^{M-1}m\big(\lfloor Q_m\rfloor-\lfloor R_m\rfloor\big)+\frac{4n^3+3n^2-n}{6}-Mp\Big(2n-1-2\lfloor Q_{M-1}\rfloor\Big). \tag{3}$$

Proof. We observe that the sum of quadratic residues from 1 to $p-1$ is twice the sum of the quadratic residues from 1 to $2n-1$ as they repeat. Hence it is enough to look at the sum from 1 to $2n-1$. Let $a_k = r_p\left(k^2\right)+r_p\left((2n-k)^2\right)$, $b_k = 2k^2-k+n$ and $c_k = a_k - b_k$. In the sum of the quadratic residues from 1 to $2n-1$, if we add the first one and the last one, the second and the second to the last and so on, we obtain that

$$\sum_{k=1}^{2n-1} r_p\left(k^2\right) = a_n + \sum_{k=1}^{n-1} a_k = a_n + \sum_{k=1}^{n-1} b_k + \sum_{k=1}^{n-1} c_k.$$

From Corollary 1 we know that

$$c_k = \begin{cases} -2mp & k \in (R_m, Q_m] \\ \\ -(2m+1)p & k \in (Q_m, R_{m+1}). \end{cases}$$

From Lemma 2.6, $n-1 \in (R_{M-1}, Q_M) - (Q_{M-1}, R_M) = (R_{M-1}, Q_{M-1}] \cup [R_M, Q_M)$. From the proof of Lemma 2.7, we know that $n-1 \neq Q_{M-1}$ and $n-1 \neq R_M$, hence $n-1 \in (R_{M-1}, Q_{M-1}) \cup (R_M, Q_M)$. Let $I = \{1, 2, ..., n-1\}$.

- Case $n-1 < Q_{M-1}$.
  By Lemma 2.7, $n-1 = \lfloor Q_{M-1} \rfloor = \lfloor R_M \rfloor$ and also $R_{M-1} < n-2 < n-1 < Q_{M-1}$. Since all the c_k's, for k that are in certain intervals, have the same value, we have

$$\begin{aligned}
\sum_{k=1}^{n-1} c_k &= \sum\nolimits_{k \in I \cap \left(\bigcup_{m=0}^{M-1} (R_m, Q_m] \cap (Q_m, R_{m+1})\right)} c_k \\
&= \sum_{m=0}^{M-1} \left(\sum_{k \in I \cap (R_m, Q_m]} c_k + \sum_{k \in I \cap (Q_m, R_{m+1})} c_k \right) \\
&= \sum_{m=0}^{M-1} \sum_{k \in I \cap (R_m, Q_m]} c_k + \sum_{m=0}^{M-1} \sum_{k \in I \cap (Q_m, R_{m+1})} c_k \\
&= \sum_{m=0}^{M-1} (-2mp) \sum_{k \in I \cap (R_m, Q_m]} 1 + \sum_{m=0}^{M-1} (-(2m+1)p) \sum_{k \in I \cap (Q_m, R_{m+1})} 1 \\
&= -p \sum_{m=0}^{M-1} 2m\big(\lfloor Q_m \rfloor - \lfloor R_m \rfloor\big) - p \sum_{m=0}^{M-1} (2m+1)\big(\lfloor R_{m+1} \rfloor - \lfloor R_m \rfloor\big) \\
&= -p \sum_{m=0}^{M-1} 2m\big(\lfloor Q_m \rfloor - \lfloor R_m \rfloor\big) - p \sum_{m=0}^{M-1} (2m+1)\big(\lfloor R_{m+1} \rfloor - \lfloor R_m \rfloor\big) \\
&\qquad - 2Mp\Big(n-1-\lfloor Q_{M-1} \rfloor\Big).
\end{aligned}$$

- Case $R_M < n-1$. From the proof of Lemma 2.7, $\lfloor Q_{M-1} \rfloor = \lfloor R_M \rfloor = n-2$ $\lfloor Q_M \rfloor = \lfloor R_{M+1} \rfloor = n$ and also $R_{M-1} < n-2 < Q_{M-1} < R_M < n-1 < n < Q_M$. Since $n-1 \in (R_M, Q_M)$ then $a_{n-1} = 2(n-1)^2-(n-1)+n-2Mp$, hence $c_{n-1} = -2Mp$. As in the previous case, to compute the sum of the c_k's, we

have the same terms plus this additional one. Note that $n-1-\lfloor Q_{M-1}\rfloor = 1$.

$$\begin{aligned}
\sum_{k=1}^{n-1} c_k &= \sum_{k=1}^{n-2} c_k + c_{n-1} \\
&= \sum_{m=0}^{M-1} (-(2m+1)p)\Big(\lfloor R_{m+1}\rfloor - \lfloor Q_m\rfloor \Big) - 2Mp \\
&\qquad + \sum_{m=0}^{M-1} (-2mp)\Big(\lfloor Q_m\rfloor - \lfloor R_m\rfloor \Big) \\
&= -p \sum_{m=0}^{M-1} (2m+1)\Big(\lfloor R_{m+1}\rfloor - \lfloor Q_m\rfloor \Big) - 2Mp \\
&\qquad - p \sum_{m=0}^{M-1} 2m\Big(\lfloor Q_m\rfloor - \lfloor R_m\rfloor \Big) \\
&= -p \sum_{m=0}^{M-1} 2m\Big(\lfloor Q_m\rfloor - \lfloor R_m\rfloor \Big) - 2Mp\Big(n-1-\lfloor Q_{M-1}\rfloor \Big) \\
&\qquad - p \sum_{m=0}^{M-1} (2m+1)\Big(\lfloor R_{m+1}\rfloor - \lfloor Q_m\rfloor \Big).
\end{aligned}$$

Notice that $a_n = \frac{1}{2}(r_p\left(n^2\right) + r_p\left((2n-n)^2\right) = \frac{1}{2}(2n^2 - 2Mp) = n^2 - Mp$. Since

$$\sum_{k=1}^{n-1} b_k + n^2 = \sum_{k=1}^{n-1} (2k^2 - k + n) + n^2 = \frac{4n^3 + 3n^2 - n}{6},$$

we can now put all the pieces together to obtain,

$$\begin{aligned}
\frac{1}{2}\sum_{k=1}^{p-1} r_p\left(k^2\right) &= \sum_{k=1}^{2n-1} r_p\left(k^2\right) = a_n + \sum_{k=1}^{n-1} b_k + \sum_{k=1}^{n-1} c_k \\
&= \frac{4n^3 + 3n^2 - n}{6} - Mp + \sum_{k=1}^{n-1} c_k \\
&= -p \sum_{m=0}^{M-1} 2m\big(\lfloor Q_m\rfloor - \lfloor R_m\rfloor\big) - p \sum_{m=0}^{M-1} (2m+1)\big(\lfloor R_{m+1}\rfloor - \lfloor R_m\rfloor\big) \\
&\qquad + \frac{4n^3 + 3n^2 - n}{6} - Mp - 2Mp\Big(n-1-\lfloor Q_{M-1}\rfloor \Big) \\
&= -p \sum_{m=0}^{M-1} (2m+1)\big(\lfloor R_{m+1}\rfloor - \lfloor R_m\rfloor\big) - 2p \sum_{m=0}^{M-1} m\big(\lfloor Q_m\rfloor - \lfloor R_m\rfloor\big) \\
&\qquad + \frac{4n^3 + 3n^2 - n}{6} - Mp\Big(2n-1-2\lfloor Q_{M-1}\rfloor \Big).
\end{aligned}$$

□

Corollary 2. *Under the hypothesis of Theorem 3.1,*

$$\frac{1}{2}\sum_{k=1}^{p-1} r_p\left(k^2\right) = p\left(\sum_{m=0}^{M} \lfloor R_m\rfloor + \sum_{m=0}^{M-1} \lfloor Q_m\rfloor\right) - Mp(2n-1) + \frac{p\cdot(n^2+n)}{6}$$

Proof. From Theorem 3.1,

$$\begin{aligned}\frac{1}{2}\sum_{k=1}^{p-1} r_p\left(k^2\right) &= -p\sum_{m=0}^{M-1}(2m+1)\big(\lfloor R_{m+1}\rfloor - \lfloor R_m\rfloor\big) - 2p\sum_{m=0}^{M-1} m\big(\lfloor Q_m\rfloor - \lfloor R_m\rfloor\big)\\ &\qquad + \frac{4n^3+3n^2-n}{6} - Mp\big(2n-1-2\lfloor Q_{M-1}\rfloor\big)\\ &= -2p\sum_{m=0}^{M-1} m\Big(\lfloor R_{m+1}\rfloor - \lfloor R_m\rfloor\Big) - Mp\big(2n-1-2\lfloor Q_{M-1}\rfloor\big)\\ &\qquad + \frac{4n^3+3n^2-n}{6} - p\sum_{m=0}^{M-2}\Big(\lfloor R_{m+1}\rfloor - \lfloor Q_m\rfloor\Big)\\ &= p\left(\sum_{m=0}^{M}\lfloor R_m\rfloor + \sum_{m=0}^{M-1}\lfloor Q_m\rfloor\right) - Mp\Big(2n-1-2\lfloor Q_{M-1}\rfloor\Big)\\ &\qquad + \frac{4n^3+3n^2-n}{6} - 2Mp\lfloor R_M\rfloor.\end{aligned}$$

By Lemma 2.7, $\lfloor Q_{M-1}\rfloor = \lfloor R_M\rfloor$, the result follows. □

4. **A computable class number formula.** We now establish our formula that allows us to compute the class number for the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ when $p = 4n-1$ is prime.

Theorem 4.1. *Let $n \in \mathbb{N}, n > 1$ such that $p = 4n-1$ is prime. If $Q_m = \frac{1}{2} + \frac{1}{2}\sqrt{4mp+3p-4}\rceil, R_m = \sqrt{mp}\rceil$ and $M = \left\lfloor \frac{n^2}{p}\right\rfloor$ then*

$$h(-p) = (2M+1)(2n-1) - 2\left(\sum_{m=0}^{M}\lfloor R_m\rfloor + \sum_{m=0}^{M-1}\lfloor Q_m\rfloor\right) - \frac{(n^2+n)}{3}.$$

Proof. According to the formula

$$\sum_{k=1}^{p-1} r_p(k^2) = \binom{p}{2} - p\cdot h(-p),$$

and Corollary 2, we obtain that

$$\binom{p}{2} - p\cdot h(-p) = 2p\left(\sum_{m=0}^{M}\lfloor R_m\rfloor + \sum_{m=0}^{M-1}\lfloor Q_m\rfloor\right) - 2Mp(2n-1) + \frac{p\cdot(n^2+n)}{3},$$

the formula follows. □

Corollary 3. *Let $n \in \mathbb{N}, n > 1$ such that $p = 4n-1$ is prime. If $Q_m = \frac{1}{2} + \frac{1}{2}\sqrt{4mp+3p-4}\rceil, R_m = \sqrt{mp}\rceil$, $M = \left\lfloor \frac{n^2}{p}\right\rfloor$ and*

$$\gamma_k = \sum_{m=0}^{k}\lfloor R_m\rfloor + \sum_{m=0}^{k-1}\lfloor Q_m\rfloor$$

then

$$h(-p)=\begin{cases}\dfrac{1}{3}(32k^2+14k-3)-2\gamma_k, & p=16k-1\\ \dfrac{1}{3}(32k^2+18k+1)-2\gamma_k, & p=16k+3\\ \dfrac{1}{3}(32k^2+22k+3)-2\gamma_k, & p=16k+7\\ \dfrac{1}{3}(32k^2+26k+3)-2\gamma_k, & p=16k+11.\end{cases}$$

Proof. The proof is immediate by applying Theorem 4.1 and Lemma 2.5. □

A concise way to compute the class number is

Corollary 4. *Let $n\in\mathbb{N}, n>1$ such that $p=4n-1$ is prime. If $Q_m=\frac{1}{2}+\frac{1}{2}\sqrt{4mp+3p-4}\rceil, R_m=\sqrt{mp}\rceil$, $M=\left\lfloor\frac{n^2}{p}\right\rfloor$ and*

$$\beta_0=2\left\lfloor\frac{1}{2}+\frac{1}{2}\sqrt{3p-4}\right\rfloor$$

then

$$h(-p)=\begin{cases}\dfrac{1}{3}\displaystyle\sum_{m=1}^{k}\Big(64m+6-6\lfloor R_m\rfloor-6\lfloor Q_m\rfloor\Big)-\beta_0+1, & p=16k-1\\ \dfrac{1}{3}\displaystyle\sum_{m=1}^{k}\Big(64m+10-6\lfloor R_m\rfloor-6\lfloor Q_m\rfloor\Big)-\beta_0+\dfrac{13}{3}, & p=16k+3\\ \dfrac{1}{3}\displaystyle\sum_{m=1}^{k}\Big(64m+14-6\lfloor R_m\rfloor-6\lfloor Q_m\rfloor\Big)-\beta_0+5, & p=16k+7\\ \dfrac{1}{3}\displaystyle\sum_{m=1}^{k}\Big(64m+18-6\lfloor R_m\rfloor-6\lfloor Q_m\rfloor\Big)-\beta_0+7, & p=16k+11.\end{cases}$$

Proof. Observe that from Lemma 2.6 and Lemma 2.7, $r<2n-3$ implies $\lfloor Q_M\rfloor=n+1$ and $r>2n-3$ implies $\lfloor Q_M\rfloor=n$. Now, Table 1 in Lemma 2.5 provides the different values for r in each of the four cases and we notice that when $n=4k$ or $n=4k+1$, we have $r<2n-3$ and hence $\lfloor Q_M\rfloor=n+1$. In the other two cases $r>2n-3$ and $\lfloor Q_M\rfloor=n$. Consequently, if we look closely at Corollary 3 and we write γ_k and $\lfloor Q_M\rfloor$ as well as the term containing $32k^2$ as a sum from 1 to k, in we obtain desired result. □

5. **Examples, conjectures and future work.**

Example. As a simple example, consider $p=103=4\cdot 26-1$ a prime number, here $n=26=4\cdot 6+2$. We compute

$\lfloor Q_0\rfloor=9$	$\lfloor Q_1\rfloor=13$	$\lfloor Q_2\rfloor=17$	$\lfloor Q_3\rfloor=20$	$\lfloor Q_4\rfloor=22$	$\lfloor Q_5\rfloor=24$
$\lfloor R_1\rfloor=10$	$\lfloor R_2\rfloor=14$	$\lfloor R_3\rfloor=17$	$\lfloor R_4\rfloor=20$	$\lfloor R_5\rfloor=22$	$\lfloor R_6\rfloor=24$

Hence by using Corollary 3, case $n = 4k + 2$, we obtain $k = 6, \gamma_6 = 107 + 105 = 212$, and hence

$$h(-103) = \frac{1}{3}(32k^2 + 22k + 3) - 2\gamma_k = 429 - 424 = 5.$$

Example. As a more complicated example, consider $k = 50,000$, $n = 4 * k, p = 4n - 1 = 799,999$ a prime number. We compute

$$\begin{aligned} \beta_0 &= 1550, \\ \sum_{m=1}^{50,000} \Big(64m + 6 - 6\lfloor R_m \rfloor - 6\lfloor Q_m \rfloor\Big) &= 6216, \end{aligned}$$

and hence by using Corollary 4, case $n = 4k$, we obtain

$$h(-799,999) = \frac{1}{3}(6216) - 1550 + 1 = 523.$$

(We used Maple 2019 to compute the sum)

The author has been able to check the formula for the class number for all the primes $p = 4n - 1, p \leq 10^4$.

As opposed to the Shanks' Baby-Step–Giant-Step method introduced by Shanks in 1969 [6], which is an algorithm, we obtained a specific formula that does not rely on the Dirichlet character χ or the Kronecker symbol $\left(\frac{p}{r}\right)$. The algorithm implementation of this formula is straight forward. Further questions may arise such as *Does the formula provide some insight about the structure of the class group? What do the different* $\lfloor Q_m \rfloor, \lfloor R_m \rfloor$ *tell us about the class group? What do they represent?*

Whereas there does not exists a formula yet for $\sum_{n=1}^{M} \lfloor R_m \rfloor$ or $\sum_{n=0}^{M} \lfloor Q_m \rfloor$, in a coming paper [4], we found several identities involving these terms and others. This will allow us to simplify a bit more the new formula for the class number as well as relate it to an oscillating term that we called *jumps*.

The author does not have an extension of this class number formula to other discriminants $d < 0$ where $-d$ is not a prime of the form $4n - 1$; however, this is an interesting area of research and it must be pursued. Perhaps where one may start is with Lemma 2.2 and replace p with d and see if patterns emerge.

Acknowledgments. The author wishes to thank two anonymous reviewers for their insightful suggestions and careful reading of the manuscript. The author also wishes to extend a special thanks to his mom Petra Villeda and Ivette R. for being his source of inspiration.

REFERENCES

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Volume **138** of Graduate Text in Mathematics, Springer-Verlag, New York, 1993.
[2] L. E. Dickson, *Introduction to the Theory of Numbers*, Dover Publ. Inc., New York, 1957.
[3] P. G. L. Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, Volume **1**, Cambridge University Press, (2012), 313–342.
[4] J. Garcia, Sum of quadratic-type residues modulus a prime $p = 4n - 1$, work in progress.
[5] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 2004.

[6] D. Shanks, Class number, a theory of factorization, and genera, *1969 Number Theory Institute (Proc. Sympos. Pure Math., Volume **XX**, State Univ. New York, Stony Brook, N.Y., 1969)*, Amer. Math. Soc., (1971), 415–440.

Received May 2021; revised July 2021; early access September 2021.

E-mail address: jorge.garcia@csuci.edu