A Note on the Sequence \( \left( \frac{p-1}{2} \right)! \mod p \)

Michele Elia

Politecnico di Torino, I-10129 Torino, Italy
michele.elia@polito.it

Abstract

As a consequence of Wilson’s theorem, the factorial \( \frac{p-1}{2}! \mod p \) provides a square root of \( (-1)^{(p+1)/2} \). The main goal of the paper is to derive an alternative expression for these square roots that avoids the factorial computation. Further, several questions concerning the infinite sequences, formed with these square roots modulo primes \( p \) congruent to 1 or congruent to 3 modulo 4, are considered and heuristics for some explanations are proposed.

Mathematics Subject Classification: 11R29, 11A05, 11R11

Keywords: Wilson theorem, number theory, field class number

1 Introduction

Wilson’s identity holds only for prime numbers, and may be written, \([1, 10]\), as

\[
\left( \frac{p-1}{2}! \right)^2 = (-1)^{\frac{p+1}{2}} \mod p, \quad \forall \ p \ \text{prime}.
\]

This equation shows that \( \frac{p-1}{2}! \mod p \) provides a root of the quadratic polynomial \( Q_p(X) = X^2 - (-1)^{\frac{p+1}{2}} \mod p \). For a prime \( p \), define the reduced set of residues modulo \( p \) as \( S_p = \{ a : -\frac{p-1}{2} \leq a \leq \frac{p-1}{2} \} \). If \( p = 3 \mod 4 \), it is trivial to observe that \( Q_p(X) \) has roots \( \pm 1 \mod p \). If \( p = 1 \mod 4 \), the quadratic polynomial \( Q_p(X) \) has roots \( \pm a \mod p \), where \( a \) may be chosen to be positive in \( S_p \), and can be easily computed from the representation \( p = x^2 + y^2 \) with \( x \) and \( y \) coprime and \( x \leq y \).
It is thus worthwhile to consider and study two separate sequences \( W_1 \) and \( W_3 \), for primes congruent 1 or 3 modulo 4, respectively.

**Definition 1.** With the above assumptions and notations, the infinite sequences \( W_1 \) and \( W_3 \) are defined as follows

\[
W_1 = \{ w_1(p) = \frac{1}{\alpha} \left( \frac{p-1}{2} \right)! \mod p \}, \text{ if } p = 1 \mod 4.
\]

\[
W_3 = \{ w_3(p) = \left( \frac{p-3}{2} \right)! \mod p \}, \text{ if } p = 3 \mod 4.
\]

Since sequences \( W_1 \) and \( W_3 \) both consist only of 1s and \(-1\)s, we may consider the following problems:

a) Find the values of \( w_1(p) \) and \( w_3(p) \) for every \( p \) without computing the factorial, that is, express the value of \( \frac{p-1}{2}! \mod p \) by means of some other function of \( p \).

b) Determine whether both sequences \( W_1 \) and \( W_3 \) contain an infinite number of 1s and \(-1\)s.

c) Compute the relative densities of 1s and \(-1\)s in sequences \( W_1 \) and \( W_3 \).

The (somewhat limited) objective of this paper is to find several properties of the sequences \( W_1 \) and \( W_3 \), and to give a relatively satisfactory answer to question a). In this latter endeavor, it is found that the sequence \( W_3 \) has close connections with Gauss’ class number problem, that is for a given \( m \), determine a complete list of fundamental binary quadratic forms of discriminant \(-d\) such that the class number \( h(\sqrt{-d}) \) is \( m \), [6, 7, 14, 16]. This connection may be useful to tackle questions b) and c), for which only some heuristics are formulated.

To these aims, the paper is organized as follows. Section 2 collects definitions and ancillary results concerning sums of Legendre symbols. Sections 3 and 4 are devoted to the sequences \( W_1 \) and \( W_3 \), respectively, and alternative expressions for \( \frac{p-1}{2}! \mod p \) are derived. Section 5 collects numerical observations concerning the combinatorial behavior of the sequences \( W_1 \) and \( W_3 \), and reports the conclusions.

## 2 Preliminaries and Legendre symbol sums

A partition of \( S_p \) into three disjoint subsets is defined as follows

\[
S_p^- = \{ a : a < 0, a \in S_p \} \quad S_p^0 = \{ 0 \} \quad \text{and} \quad S_p^+ = \{ a : a > 0, a \in S_p \},
\]
clearly \( S_p^- = -S_p^+ \). For a fixed prime \( p \), consider the following summations concerning Legendre symbols

\[
g_n = \frac{-1}{p} \sum_{k=1}^{p-1} \left( \frac{k}{p} \right) k^n \quad \forall \ n \in \{0, 1, 2, \ldots, p-2\} .
\]

This set of equations defines a linear transformation of a \((p-1)\)-dimensional vector of Legendre symbols into a \((p-1)\)-dimensional vector of rational numbers

\[
\left( \left( \frac{1}{p} \right), \left( \frac{2}{p} \right), \ldots, \left( \frac{p-1}{p} \right) \right) \rightarrow (g_0, g_1, \ldots, g_{p-2}) .
\]

The transformation is invertible because the square matrix \( K = (k^n), k = 1, \ldots, p-1 \) and \( n = 0, \ldots, p-2 \), is a Vandermonde matrix with distinct entries in the second row. The factor in front of the summations is chosen to make \( g_1 \) exactly equal to the class number of the imaginary quadratic field \( \mathbb{Q}(\sqrt{-p}) \) when \( p = 3 \mod 4 \), in view of Dirichlet’s formula \([4, 3]\)

\[
h(\sqrt{-p}) = \frac{-1}{p} \sum_{k=1}^{p-1} k \left( \frac{k}{p} \right) \quad \forall \ p = 3 \mod 4 .
\]

**Lemma 1.** Every entry in vector \((g_0, g_1, \ldots, g_{p-2})\), except \( g_{p-1} \), is an integer, further \( g_0 = 0 \), and the numerator of \( g_{p-1} \) is congruent \(-1\) modulo \( p \).

**Proof.** The value \( g_0 = 0 \) is trivially true because the number of quadratic residues is equal to the number of quadratic non-residues in \( S_p \). To prove the other properties, consider the sums \( S_j = \sum_{k=1}^{p-1} \left( \frac{k}{p} \right) k^j \), which are integers, and observe that the said properties follow by proving that \( S_j = 0 \mod p \) for every index \( j \neq \frac{p-1}{2} \), and \( S_{p-1} = -1 \mod p \).

Assume \( j \neq \frac{p-1}{2} \), and multiply \( S_j \) by \( \left( \frac{a}{p} \right) \), with \( a \) being a primitive element in \( \mathbb{Z}_p^* \), then

\[
\left( \frac{a}{p} \right) S_j = \left( \frac{a}{p} \right) \sum_{k=1}^{p-1} \left( \frac{k}{p} \right) k^j = \sum_{k=1}^{p-1} \left( \frac{ak}{p} \right) k^j .
\]

Performing the change of index \( ak = \mu p + h \) in the summation, and taking modulo \( p \), we have

\[
\left( \frac{a}{p} \right) S_j \mod p = \sum_{h=1}^{p-1} \left( \frac{h}{p} \right) (\mu p + h) \cdot \frac{1}{a^j} \mod p = \frac{1}{a^j} \sum_{h=1}^{p-1} \left( \frac{h}{p} \right) h^j \mod p = \frac{1}{a^j} S_j \mod p .
\]
The conclusion $S_j = 0 \mod p$ follows, because $\frac{1}{a^j} \neq \left(\frac{a}{p}\right)$ for every $j \neq 0, \frac{p-1}{2}$.

When $j = \frac{p-1}{2}$, we have

$$S_{\frac{p-1}{2}} \mod p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) k^{\frac{p-1}{2}} \mod p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)^2 \mod p = p-1 \mod p = -1.$$ 

\[ \square \]

Lemma 2. The entries in $g = (g_0, g_1, \cdots, g_{p-2})$ are connected by the following recurrence

$$\left[\left(-1\right)^{\frac{n}{2}}\right] g_n = \sum_{j=0}^{n-1} \left(\begin{array}{c} n \\ j \end{array}\right) (-1)^j p^{n-j} g_j. \quad (3)$$

In particular, $g_1 = \left\{ \begin{array}{ll} h(\sqrt{-p}) & \text{if } p = 3 \mod 4 \\ 0 & \text{if } p = 1 \mod 4 \end{array} \right.$

and $g_2 = \left\{ \begin{array}{ll} ph(\sqrt{-p}) & \text{if } p = 3 \mod 4 \\ \omega(p) & \text{if } p = 1 \mod 4 \end{array} \right.$,

where $\omega(p)$ is an integer for every $p > 5$ that can be directly evaluated from the summation.

Proof. Multiplying both sides of (1) by $\left(-1\right)^{\frac{n}{2}}$, and using properties of Legendre symbols, we have

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

where $p-k$ has been substituted for $k$ in the last summation. Now, expanding the binomial $(p-k)^{n}$, exchanging the summations, and using the definition of $g_j$ we obtain

$$\left(-1\right)^{\frac{n}{2}} g_n = \sum_{j=0}^{n} \left(\begin{array}{c} n \\ j \end{array}\right) (-1)^j p^{n-j} g_j.$$

Finally, moving the term corresponding to $j = n$ in the summation to the left side, we get the asserted recurrence. If $p = 1 \mod 4$, the initial entries in vector $g$ are $g_0 = 0, g_1 = 0$ obtained by specializing (3), and $g_2$, which should be evaluated by its definition; obviously $g_2 = \frac{4}{5}$ when $p = 5$. If $p = 3 \mod 4$, the initial entries in vector $g$ are $g_0 = 0$, and $g_1 = h(\sqrt{-p})$, see (2). \[ \square \]

Proposition 1. $g_2$ is a multiple of 4, if $p = 1 \mod 4$. 

Proof. The proposition is equivalent to saying that \( g_2 = 0 \mod 4 \). Then, considering \( g_2 \) modulo 4, and noting that \( k^2 \) taken modulo 4 is zero when \( k \) is even, and is 1 when \( k \) is odd, we have

\[
g_2 = \sum_{k=1}^{(p-1)/2} \left( \frac{2k - 1}{p} \right) \mod 4 .
\]

Considering \( S = \sum_{j=1}^{(p-1)/2} \left( \frac{2j - 1}{p} \right) \) and \( T = \sum_{j=1}^{(p-1)/2} \left( \frac{2j}{p} \right) \), clearly \( S + T = 0 \); further, \( T = 0 \), because, introducing \( t = \sum_{j=1}^{(p-1)/2} \left( \frac{j}{p} \right) \) by manipulating the expression for \( T \) as

\[
T = \left( \frac{2}{p} \right)^{(p-1)/2} \sum_{j=1}^{(p-1)/2} \left( \frac{j}{p} \right) = \left( \frac{2}{p} \right) t ,
\]

we have \( t = \left( \frac{-1}{p} \right) t = \sum_{j=1}^{(p-1)/2} \left( \frac{-j}{p} \right) \), thus \( 2t = t + \left( \frac{-1}{p} \right) t = \sum_{j=-(p-1)/2}^{(p-1)/2} \left( \frac{-j}{p} \right) = 0 \), because the sum is over a full set of residues; the additional term for \( j = 0 \) is zero and does not alter the sum. In conclusion, \( g_2 = 0 \mod 4 \) since \( t = 0 \) implies \( T = S = 0 \).

It should be interesting to find arithmetical or algebraic significances for \( g_2 \) for primes congruent 1 modulo 4, as is the case of \( g_1 \) for primes congruent 3 modulo 4.

3 Case \( p = 1 \mod 4 \)

Since a prime \( p = 1 \mod 4 \) can be uniquely represented as the sum of two squares \( p = x^2 + y^2 \), with both \( x \) and \( y \) being positive integers of different parities, then \( x \) will be taken odd, and \( y \) even.

Proposition 2. In the representation of a prime as the sum of two squares, the odd component \( x \) is a quadratic residue modulo \( p \).

Proof. The property of \( x \) is a consequence of the following chain of equalities, where the first equality is due to the quadratic reciprocity law, and the remaining equalities are evident

\[
\left( \frac{x}{p} \right) = \left( \frac{p}{x} \right) = \left( \frac{x^2 + y^2}{x} \right) = \left( \frac{y^2}{x} \right) = 1 .
\]
It is remarked that $x$ and $y$ can be computed in polynomial complexity by counting the number of points on the elliptic curves $Y^2 = X^3 - X$ and $Y^2 = X^3 - bX$, with $b$ being a quadratic non-residue modulo $p$, [13]. For the numerical computations, $b$ is not actually necessary, because $y$ may be easily computed as $\sqrt{p - x^2}$.

To establish the quadratic character of the even component $y$, some further results are required.

**Proposition 3.** The set $\mathbb{S}_p^+$ of positive residues less than $p/2$ is partitioned into the subsets $\mathbb{S}_Q^+$ and $\mathbb{S}_{NQ}^+$ of quadratic residues and quadratic non-residues, respectively. Defining $n_Q = |\mathbb{S}_Q^+|$ and $n_{QN} = |\mathbb{S}_{NQ}^+|$, we have

$$n_Q = n_{QN} = \frac{p - 1}{4} .$$

**Proof.** Since $-1$ is a quadratic residue modulo $p$, and $\mathbb{S}_p^- = -\mathbb{S}_p^+$, the number of quadratic residues in $\mathbb{S}_p^-$ is also $n_Q$, then $2n_Q = \frac{p - 1}{2}$, which implies $n_Q = \frac{p - 1}{4} = n_{QN}$. The equality $n_Q = n_{QN}$ is a consequence of the equation $n_Q + n_{QN} = \frac{p - 1}{2}$, which holds by definition. \hfill $\square$

In proving the following theorems we apply a trick that can be traced back to Gauss in one of his proofs of the quadratic reciprocity law.

Consider $p = u^2 + v^2$ with $u$ and $v$ chosen in such a way that $\frac{p - 1}{2}! = \frac{u}{v} \mod p$, and define the products $A = \prod_{t \in \mathbb{S}_Q^+} t$ and $B = \prod_{t \in \mathbb{S}_{NQ}^+} t$, then $A \cdot B = \frac{u}{v} \mod p$ holds by definition. Further, consider the partition of $\mathbb{S}_p^-$ of negative residues greater than $\frac{-p}{2}$ into the subsets $\mathbb{S}_Q^-$ and $\mathbb{S}_{NQ}$ of quadratic residues and quadratic non-residues. Since $-1$ is a quadratic residue modulo $p$, we have

$$\prod_{t \in \mathbb{S}_Q^+} t \cdot \prod_{t' \in \mathbb{S}_Q^-} t' = (-1)^{\frac{p - 1}{4}} A^2 \mod p, \quad \prod_{t \in \mathbb{S}_{NQ}^+} t \cdot \prod_{t' \in \mathbb{S}_{NQ}^-} t' = (-1)^{\frac{p - 1}{4}} B^2 \mod p .$$

Multiplying these two equations, member by member, we have $A^2 B^2 (-1)^{\frac{p - 1}{2}} = (p - 1)! = -1 \mod p$. Further, let $b$ be a quadratic non-residue, then we have

$$b^{\frac{p - 1}{2}} (-1)^{\frac{p - 1}{4}} A^2 = \prod_{t \in \mathbb{S}_Q^+} (bt) \cdot \prod_{t' \in \mathbb{S}_Q^-} (bt') = (-1)^{\frac{p - 1}{4}} B^2 \mod p ,$$

it follows that $-A^2 = B^2 \mod p$ because $b^{\frac{p - 1}{2}} = -1 \mod p$. From the equations $A^2 B^2 = -1 \mod p$ and $A^2 = -B^2 \mod p$ we obtain the equation $A^4 = B^4 = 1 \mod p$, which implies $B^2 = \pm 1 \mod p$ and $A^2 = \mp 1 \mod p$: it emerges that all the following eight possibilities modulo $p$ may occur

$$\begin{cases} A = \pm 1 \\ B = \pm \frac{u}{v} \end{cases} \quad \begin{cases} A = \pm \frac{u}{v} \\ B = \pm 1 \end{cases}$$
Theorem 1. Let $A$ and $B$ be defined as above, assume $p = x^2 + y^2$ with $x$ odd, and $\alpha$ to be the smallest root of $X^2 + 1 \mod p$ between $\frac{x}{y} \mod p$ and $\frac{y}{x} \mod p$. The quadratic character of even $y$ depends on the residue of $p \mod 8$, that is

1. If $p = 5 \mod 8$, then $\left( \frac{y}{p} \right) = -1$, and $|A| = 1, |B| = \alpha \mod p$.

2. If $p = 1 \mod 8$, then $\left( \frac{y}{p} \right) = 1$, and $|B| = 1, |A| = \alpha \mod p$.

Proof. If $p = 5 \mod 8$, then $B$ is the product of an odd number of quadratic non-residues, which implies that $\left( \frac{B}{p} \right) = -1$. It follows that $|B| = \alpha \mod p$ with $y$ being a quadratic non-residue, consequently $A = \pm 1 \mod p$.

If $p = 1 \mod 8$, then $B$ is the product of an even number of quadratic non-residues, so that the product in pairs is either 1 or $-1$; consequently, $B = \pm 1 \mod p$, then necessarily $|A| = \alpha \mod p$ with $y$ being a quadratic residue. Note that, in this case, $A$ is the product of an even number of quadratic residues, including 1, which stands alone, thus the product $A$ cannot be $\pm 1$ modulo $p$. \hfill \square

The quadratic character of $y$, obtained in Proposition 3, is explicitly expressed as a corollary.

Corollary 1. In the representation of a prime as the sum of two squares, the even component $y$ is a quadratic residue if and only if $\frac{p-1}{4}$ is even, that is

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

We conclude this section with a second characterization of the sequence $W_1$.

Theorem 2. The sequence $W_1 = \{ w_1(p) : p = 1 \mod 4, p \in \mathbb{P} \}$ admits of the description

$$w_1(p) = (-1)^{\frac{p-5-2s_o}{8}} ,$$

where $s_o \in \mathbb{S}_p$ is an even value obtained from $t_o = \frac{1}{2} \sum_{u=1}^{\frac{p-1}{2}} (u + \bar{u})^2 \mod p$ as

$$s_o = \begin{cases} t_o & \text{if } t_o \text{ is even} \\ t_o - p & \text{if } t_o \text{ is odd} \end{cases} ,$$

and $\bar{u}$ is the absolute value of the inverse of $u \mod p$, thus it is an element of $\mathbb{S}_p^+$.
Proof. The factorial, except for a reordering of the factors, can be written as
\[
\frac{p-1}{2}! = 1 \cdot \alpha \cdot (x_1x_2) \cdots (x_{p-1}x_{p-2}) \mod p
\] (4)

where the \(\frac{p-5}{4}\) products \((x_ix_{i+1})\) are +1 or −1 modulo \(p\). Let \(n^+\) and \(n^-\) denote the number of +1s and −1s in the sequence, then by definition \(n^+ + n^- = \frac{p-5}{4}\), and clearly we have \(w_1(p) = (-1)^{n^-}\).

To compute \(n^-\) we consider the sum \(t_o = \frac{1}{2} \sum_{u=1}^{\frac{p-1}{2}}(u + \bar{u})^2 \mod p\) where \(\bar{u}\) is the absolute value of the inverse of \(u\) lying in \(S^+_p\). Expanding the square in the summation defining \(t_o\), we have
\[
t_o = \frac{1}{2} \sum_{u=1}^{\frac{p-1}{2}} (u + \bar{u})^2 \mod p = \frac{1}{2} \left( \sum_{u=1}^{\frac{p-1}{2}} u^2 + \sum_{u=1}^{\frac{p-1}{2}} \bar{u}^2 + 2 \sum_{u=1}^{\frac{p-1}{2}} (u\bar{u}) \mod p \right) .
\]

Now, \(\sum_{u=1}^{\frac{p-1}{2}} u^2 = \sum_{\bar{u}=1}^{\frac{p-1}{2}} \bar{u}^2 = 0 \mod p\), because the sums of squares are equal, since they are computed on the same set \(S^+_p\), and their value is \(\frac{p-1}{6}(\frac{p-1}{2} + 1)(2\frac{p-1}{2}+1) = \frac{p^2-1}{2}p\), which is 0 modulo \(p\). Then, in the sum \(t_o = \sum_{u=1}^{\frac{p-1}{2}} (u\bar{u}) \mod p\), every product \((u\bar{u}) \mod p\), which is either 1 or −1, appears twice as many times as in the product (4), and the summation value is \(2(n^+ - n^-) \mod p\). Since the sum is considered modulo \(p\), if \(t_o\) is even, it is the true value of \(2(n^+ - n^-)\) because the absolute value of this number is less than \(\frac{p-1}{2}\). Conversely, if \(t_o\) is odd, this means that \(2(n^+ - n^-)\) was negative, then \(p\) must be subtracted in order to have an even number in the right interval, that is, we have just defined \(s_o\). In conclusion, solving the system of equations \(n^+ + n^- = \frac{p-5}{4}\) and \(2(n^+ - n^-) = s_o\), \(n^-\) is obtained as
\[
n^- = \frac{1}{4} \left( \frac{p-5}{2} - s_o \right) = \frac{p-5-2s_o}{8} .
\]

This concludes the proof. \(\square\)

It would be desirable to have a fast way of computing \(s_o\), or better, to have some closed-form expression for it in terms of \(p\).

4 Case \(p = 3 \mod 4\)

The class number \(h(\sqrt{-p})\) of the imaginary quadratic field \(K = \mathbb{Q}(\sqrt{-p})\) is odd [5, Corollary 2, p.182]. Setting \(d = \frac{p+1}{4}\), an integral basis \(\{1, \theta\}\) of the order \(\mathcal{O}_K\) is obtained, taking \(\theta\) to be a root of \(x^2 - x + d\). The following proposition, reported for easy reference without proof, is Theorem 70 in [5, p.307].
A note on the sequence \( \left( \frac{p-1}{2} \right)! \mod p \)

**Proposition 4.** The set \( \mathbb{S}_p^+ \) of positive residues less than \( p/2 \) is partitioned into the subsets \( \mathbb{S}_Q^+ \) and \( \mathbb{S}_{NQ}^+ \) of quadratic residues and quadratic non-residues, respectively. The cardinalities of these subsets, \( n_Q = |\mathbb{S}_Q^+| \) and \( n_{QN} = |\mathbb{S}_{NQ}^+| \), satisfy the equations

\[
\begin{align*}
n_Q + n_{QN} &= \frac{p-1}{2} \quad \text{an odd number} \\
n_Q - n_{QN} &= \Delta \quad \text{a positive odd number},
\end{align*}
\]

with

\[
\Delta = \begin{cases} 
  h(\sqrt{-p}) & \text{if } p = -1 \mod 8 \\
  3h(\sqrt{-p}) & \text{if } p = 3 \mod 8 \quad \text{and } p \neq 3.
\end{cases}
\]

Therefore, the value of \( n_{QN} \), which will be useful in the next theorem, is immediately obtained

\[
n_{QN} = \frac{p - 1 - 2\Delta}{4}.
\]

**Theorem 3.** For every prime \( p > 3 \) and congruent \( 3 \mod 4 \), we have

\[
w_3(p) = \left( \frac{p - 1}{2} \right)! \mod p = (-1)^{\frac{1 + h(\sqrt{-p})}{2}}.
\]

(5)

The case \( p = 3 \) is not included in (5), and we have \( w_3(3) = 1 \).

**Proof.** The case \( p = 3 \) is trivial. Assume \( p > 3 \), since we know that \( \left( \frac{p-1}{2} \right)! \mod p = \pm 1 \), considering the Legendre symbol of \( \left( \frac{p-1}{2} \right)! \mod p \), we have

\[
\left( \frac{p - 1}{2} \right)! \mod p = \left( \frac{p - 1}{p} \right) = (-1)^{n_{QN}} = (-1)^{\frac{p - 1 - 2\Delta}{4}}.
\]

The conclusion, i.e. equation (5), is obtained by distinguishing two cases:

1) \( p = 8k - 1 \), then

\[
(-1)^{\frac{p - 1 - 2\Delta}{4}} = (-1)^{\frac{8k - 2 - 2h(\sqrt{-p})}{4}} = (-1)^{\frac{-1 - h(\sqrt{-p})}{2}} = (-1)^{\frac{1 + h(\sqrt{-p})}{2}}.
\]

2) \( p = 8k + 3 \), then

\[
(-1)^{\frac{p - 1 - 2\Delta}{4}} = (-1)^{\frac{8k + 2 - 6h(\sqrt{-p})}{4}} = (-1)^{\frac{1 - 3h(\sqrt{-p})}{2}} = -(-1)^{\frac{1 + h(\sqrt{-p}) + 4h(\sqrt{-p})}{2}} = (-1)^{\frac{1 + h(\sqrt{-p})}{2}}.
\]

\[
\Box
\]

5 **Heuristics and Conclusions**

Sequences defined over the ordered set of primes, by means of the factorials \( \left( \frac{p-1}{2} \right)! \mod p \), have many interesting and intriguing properties. Theorems 2
and 3 show alternative characterizations of the sequences $W_1$ and $W_3$, concerning primes congruent 1 and 3 modulo 4, by means of functions of $p$ that avoid the factorial. Unfortunately, these functions are of computational complexity comparable to the evaluation of factorials. Furthermore, in search of patterns within these sequences, it was found that the initial parts of $W_1$ and $W_3$ show an apparently unpredictable alternation of 1s and $-1$s; some statistics [9] could thus be useful to describe their overall trend. Numerical experiments, reported in the following table, show that in both sequences, $W_1$ and $W_3$, the number of 1s is approximately equal to the number of $-1$s.

<table>
<thead>
<tr>
<th># p</th>
<th># $p = 1 \bmod 4$</th>
<th># $-1$</th>
<th># 1</th>
<th># $p = 3 \bmod 4$</th>
<th># $-1$</th>
<th># 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>23</td>
<td>8</td>
<td>15</td>
<td>27</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>100</td>
<td>47</td>
<td>22</td>
<td>25</td>
<td>53</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>500</td>
<td>246</td>
<td>114</td>
<td>132</td>
<td>254</td>
<td>123</td>
<td>131</td>
</tr>
<tr>
<td>1000</td>
<td>495</td>
<td>229</td>
<td>266</td>
<td>505</td>
<td>249</td>
<td>256</td>
</tr>
<tr>
<td>2000</td>
<td>987</td>
<td>496</td>
<td>491</td>
<td>1013</td>
<td>499</td>
<td>514</td>
</tr>
<tr>
<td>4000</td>
<td>1988</td>
<td>991</td>
<td>997</td>
<td>2012</td>
<td>1019</td>
<td>993</td>
</tr>
</tbody>
</table>

Since the partitions remain stable as the sequence length increases, a reasonable guess is that the density of 1s equals the density of $-1$s in each of the two sequences $W_1$ and $W_3$. However, on a purely theoretical footing, it would be quite an achievement to prove that 1 and $-1$ appear infinitely many times. In the same vein, observing the initial parts of the partition of the prime sequence into four different sequences depending upon whether the primes are congruent 1 or 3 modulo 4, or $(\frac{p-1}{2})! \bmod p$ is either 1 or $-1$,

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$-1$</td>
<td>17</td>
<td>37</td>
<td>101</td>
<td>157</td>
<td>181</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>13</td>
<td>29</td>
<td>41</td>
<td>53</td>
<td>61</td>
</tr>
<tr>
<td>3</td>
<td>$-1$</td>
<td>7</td>
<td>11</td>
<td>19</td>
<td>43</td>
<td>47</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>23</td>
<td>31</td>
<td>59</td>
<td>71</td>
<td>83</td>
</tr>
</tbody>
</table>

it is natural to ask whether there is some hidden relation among the primes in the same set (line).

Notably, in view of Theorem 3, the sequence $W_3$ may be defined using the class numbers of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-p})$, therefore, the question of whether $W_3$ contains an infinite number of 1s and $-1$s, is equivalent to the question of whether the class numbers $h(\sqrt{-p})$ assume infinitely many values congruent 1 or 3 modulo 4, respectively, [8, 2]. This property would follow easily from the complete solution of Gauss’ class number problem, mentioned in the introduction. Regarding this problem, let $N(m)$ denote the number of imaginary quadratic fields with class number $m$; the Gauss conjecture, that $N(m)$ is finite for every positive $m$, has been proved [7, 12]. However, it seems that no formal proof that $N(m) > 0$ for every $m$ has been given. If this is true,
A note on the sequence \( \left( \frac{p-1}{2} \right)! \mod p \)

as is commonly believed, the sequence \( W_3 \) contains infinite 1s and \(-1\)s. The assumption that \( N(m) > 0 \), at least for every odd \( m \), is supported by Table 1, taken from Watkins' paper [16]; the same table also supports the guess that the density of 1s is equal to the density of \(-1\)s.

For the sequence \( W_1 \), an equally elegant connection with some arithmetical function (of some algebraic number field) has not been found, and it remains to ascertain whether the sum \( \frac{1}{2} \sum_{u=1}^{p-1} (u + \bar{u})^2 \mod p \) has some intuitive arithmetical significance.

<table>
<thead>
<tr>
<th>m</th>
<th>( N(m) )</th>
<th>smaller</th>
<th>large</th>
<th>m</th>
<th>( N(m) )</th>
<th>smaller</th>
<th>large</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9</td>
<td>3</td>
<td>163</td>
<td>3</td>
<td>16</td>
<td>23</td>
<td>907</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>47</td>
<td>2683</td>
<td>7</td>
<td>31</td>
<td>71</td>
<td>5923</td>
</tr>
<tr>
<td>9</td>
<td>34</td>
<td>199</td>
<td>10627</td>
<td>11</td>
<td>41</td>
<td>167</td>
<td>15667</td>
</tr>
<tr>
<td>13</td>
<td>37</td>
<td>191</td>
<td>20563</td>
<td>15</td>
<td>68</td>
<td>239</td>
<td>34483</td>
</tr>
<tr>
<td>17</td>
<td>45</td>
<td>383</td>
<td>37123</td>
<td>19</td>
<td>47</td>
<td>311</td>
<td>38707</td>
</tr>
<tr>
<td>21</td>
<td>85</td>
<td>431</td>
<td>61483</td>
<td>23</td>
<td>68</td>
<td>647</td>
<td>90787</td>
</tr>
<tr>
<td>25</td>
<td>95</td>
<td>599</td>
<td>93307</td>
<td>27</td>
<td>93</td>
<td>983</td>
<td>103387</td>
</tr>
<tr>
<td>29</td>
<td>83</td>
<td>887</td>
<td>166147</td>
<td>31</td>
<td>73</td>
<td>719</td>
<td>133387</td>
</tr>
<tr>
<td>33</td>
<td>101</td>
<td>839</td>
<td>222643</td>
<td>35</td>
<td>103</td>
<td>1223</td>
<td>210907</td>
</tr>
<tr>
<td>37</td>
<td>85</td>
<td>1487</td>
<td>158923</td>
<td>39</td>
<td>115</td>
<td>1439</td>
<td>253507</td>
</tr>
<tr>
<td>41</td>
<td>109</td>
<td>2551</td>
<td>296587</td>
<td>43</td>
<td>106</td>
<td>1847</td>
<td>300787</td>
</tr>
<tr>
<td>45</td>
<td>154</td>
<td>1319</td>
<td>308323</td>
<td>47</td>
<td>107</td>
<td>3023</td>
<td>375523</td>
</tr>
<tr>
<td>49</td>
<td>132</td>
<td>1511</td>
<td>393187</td>
<td>51</td>
<td>159</td>
<td>1559</td>
<td>546067</td>
</tr>
<tr>
<td>53</td>
<td>114</td>
<td>2711</td>
<td>425107</td>
<td>55</td>
<td>163</td>
<td>4463</td>
<td>452083</td>
</tr>
<tr>
<td>57</td>
<td>179</td>
<td>2591</td>
<td>615883</td>
<td>59</td>
<td>128</td>
<td>2399</td>
<td>474307</td>
</tr>
<tr>
<td>61</td>
<td>132</td>
<td>3863</td>
<td>606643</td>
<td>63</td>
<td>216</td>
<td>2351</td>
<td>991027</td>
</tr>
<tr>
<td>65</td>
<td>164</td>
<td>3527</td>
<td>703123</td>
<td>67</td>
<td>120</td>
<td>3719</td>
<td>652723</td>
</tr>
<tr>
<td>69</td>
<td>209</td>
<td>3119</td>
<td>888427</td>
<td>71</td>
<td>150</td>
<td>5471</td>
<td>909547</td>
</tr>
<tr>
<td>73</td>
<td>119</td>
<td>2999</td>
<td>886867</td>
<td>75</td>
<td>237</td>
<td>4703</td>
<td>916507</td>
</tr>
<tr>
<td>77</td>
<td>216</td>
<td>6263</td>
<td>1242763</td>
<td>79</td>
<td>175</td>
<td>4391</td>
<td>1333963</td>
</tr>
<tr>
<td>81</td>
<td>228</td>
<td>3671</td>
<td>1030723</td>
<td>83</td>
<td>150</td>
<td>3911</td>
<td>1074907</td>
</tr>
<tr>
<td>85</td>
<td>221</td>
<td>4079</td>
<td>1285747</td>
<td>87</td>
<td>222</td>
<td>5279</td>
<td>1261747</td>
</tr>
<tr>
<td>89</td>
<td>192</td>
<td>6311</td>
<td>1429387</td>
<td>91</td>
<td>214</td>
<td>4679</td>
<td>1391083</td>
</tr>
<tr>
<td>93</td>
<td>262</td>
<td>5351</td>
<td>1475203</td>
<td>95</td>
<td>241</td>
<td>6959</td>
<td>1659067</td>
</tr>
<tr>
<td>97</td>
<td>185</td>
<td>5519</td>
<td>1842523</td>
<td>99</td>
<td>289</td>
<td>5591</td>
<td>1480627</td>
</tr>
</tbody>
</table>

Table 1: Watkins' Table of odd class field numbers of imaginary quadratic fields, [16]
References


A note on the sequence \( \left( \frac{p-1}{2} \right)! \mod p \)


Received: September 15, 2013