Canad. Math. Bull. Vol. **34** (2), 1991 pp. 196–201

# THE PARITY DISTRIBUTION OF TRACES IN IMAGINARY QUADRATIC FIELDS

D. S. DUMMIT

ABSTRACT. Computations of the Iwasawa $\lambda$-invariant for imaginary quadratic fields showed a discrepancy in the proportion of even and odd traces of certain integers from these imaginary quadratic fields. This paper shows that such a discrepancy is in some sense to be expected and that the proportion of even and odd traces of principal generators of powers of prime ideals in imaginary quadratic fields is related to the 3-primary component of the class group.

Let $D > 0$ be a squarefree positive integer with $k = \mathbf{Q}(\sqrt{-D})$ and let $O_k$ denote the ring of integers of $k$, so that $O_k = \mathbf{Z} + \mathbf{Z}\omega$ where

$$\omega = \begin{cases} \sqrt{-D} & \text{if } D \equiv 1,\ 2 \bmod 4 \\ \dfrac{1+\sqrt{-D}}{2} & \text{if } D \equiv 3 \bmod 4. \end{cases}$$

In the first case, the trace to $\mathbf{Q}$ of every element of $O_k$ is an even integer and in the second case there are integers of $k$ with odd trace.

Let $\mathcal{P}$ be a prime ideal of $O_k$ lying above the rational prime $p$ and let $f$ be the order of $\mathcal{P}$ in the class group of $k$, so that $\mathcal{P}^f = (\pi)$ is the smallest power of $\mathcal{P}$ which is a principal ideal. For $D \neq 1, 3$, the element $\pi$ is uniquely defined up to sign. For $D = 1$ we may determine $\pi$ uniquely by choosing $\pi = 1 + i$ if $\mathcal{P}$ is the prime above 2 and requiring $\pi \equiv 1 \bmod (1+i)^3$ for all other primes $\mathcal{P}$. For $D = 3$ we choose $\pi = \sqrt{3}$ for the prime $\mathcal{P}$ above 3 and otherwise require $\pi \equiv 1 \bmod (3)$.

Let $t_p =$ Trace $\pi \in \mathbf{Z}$ be the trace from $k$ to $\mathbf{Q}$ of a generator $\pi$ of the ideal $\mathcal{P}^f$ chosen above. Note that the parity of $t_p$ is well-defined and that $t_p$ depends only on the prime $p$ and not on the choice of prime ideal $\mathcal{P}$ lying over $p$ in $k$.

If $D \equiv 1, 2 \bmod 4$ then $t_p$ is even since all integers in such fields have even trace.

If $p$ does not split in $k$ then again $t_p$ is even since such primes are principal with $p$ as a generator which of course has even trace (if $D = 3$ the element $\pi$ is $-p$).

If $D \equiv 7 \bmod 8$ and $p$ splits in $k$ then $t_2$ is odd and $t_p$ is even for all odd $p$. This is elementary since $t_2 = \pi + \bar{\pi}$ (where $\bar{\pi} \neq \pi$ is the complex conjugate of $\pi$) would imply $\bar{\pi} \in \mathcal{P}$ if $t_2$ were even, a contradiction; for $p$ odd writing $\pi = (t + b\sqrt{-D})/2$ gives $4p^f = 4\pi\bar{\pi} = t^2 + b^2D$, which is impossible mod 8 for $t$ (and hence $b$) odd.

Research partially sponsored by NSERC and NSF EPSCoR grants.
Received by the editors July 12, 1989 and, in revised form, October 5, 1990.

https://doi.org/10.4153/CMB-1991-031-2 Published online by Cambridge University Press

It remains to consider the situation of $D \equiv 3 \bmod 8$ and $p$ a split prime in $k$, which is more interesting. Let $F$ denote the Hilbert class field of $k$ and let $F_{(2)}$ denote the ray class field of $k$ of conductor (2). Let $G = \mathrm{Gal}\,(F_{(2)}/k)$ be the Galois group of $F_{(2)}$ over $k$ (the ray class group to conductor (2)). Since $D \equiv 3 \bmod 8$ the ideal (2) is inert in $k$ so that $F_{(2)}$ is an abelian extension of $F$ of degree 3 with Galois group $H = \mathrm{Gal}\,(F_{(2)}/F)$ canonically isomorphic by the Artin isomorphism to the group $(O/(2)O)^x \simeq \mathbf{Z}/3\mathbf{Z}$, with representatives $1, \omega, 1+\omega \bmod (2)$. The quotient $G/H$ is the class group $C_k$ of $k$ so we have the exact sequence of abelian groups

$$1 \longrightarrow H \longrightarrow G \longrightarrow C_k \longrightarrow 1. \tag{1}$$

If $\mathcal{P}$ is a prime ideal of $k$ then the order $f$ of $\mathcal{P}$ in the class group $C_k$ is the smallest power of the Artin symbol

$$\left(\frac{F_{(2)}/k}{\mathcal{P}}\right)$$

which is an element of the subgroup $H$ of $G$. Since $H \simeq (O/(2)O)^x \simeq \mathbf{Z}/3\mathbf{Z}$ has representatives $1, \omega, 1+\omega \bmod (2)$ it follows that $\pi \equiv 1 \bmod (2)$ precisely when this element of $H$ is the identity of $H$, and $\pi \equiv \omega$ or $1+\omega \bmod (2)$ otherwise. Since the trace of $\omega$ is 1, we see that $\pi$ has even trace if and only if the smallest power of the Artin symbol for $\mathcal{P}$ in $F_{(2)}/k$ to lie in the subgroup $H$ is the identity element of $H$. By the Tchebotarov Density Theorem the primes in $k$ with given Artin symbol in $F_{(2)}/k$ have density $1/3h$ (the order of $G$), which proves the following

THEOREM.

(1) *If* $D \equiv 1, 2 \bmod 4$ *or if $p$ does not split in $k$ then $t_p$ is even.*

(2) *Suppose* $D \equiv 7 \bmod 8$ *and $p$ splits in $k$. Then $t_2$ is odd and $t_p$ is even for all odd $p$.*

(3) *Suppose* $D \equiv 3 \bmod 8$. *Let $h$ denote the class number of $k$ and let $n$ denote the number of elements in the ray class group of conductor 2 which are the identity when raised to their order in the quotient group $C_k$, the class group of $k$. Then $t_p$ is even with density $n/3h$ as $p$ ranges over the split primes of $k$.*

The integer $n$ in the Theorem depends on the structure of the 3-primary component of $G$ and in particular on the 3-primary component of the class group of $k$. For example, if $h$ is prime to 3 then $t_p$ is even with density 1/3 since in this case the group extension (1) splits: $G \simeq H \times C_k$ and $h$ of the $3h$ classes (the identity coset of $C_k$) have even trace.

More generally, if the 3-primary component of $G$ is cyclic of order $3^N$ with $G$ of order $3^N h'$, $h'$ prime to 3, then it is easy to see that $n = h'$ so that only $1/3^N$ of the traces will be even. For example, the field $\mathbf{Q}(\sqrt{-59})$ has class number 3 with the ideal $\mathcal{P}_3$ lying above 3 as generator. Since $\mathcal{P}_3^3 = (7 + \sqrt{-59})/2 \not\equiv 1 \bmod (2)$ the extension (1) does not split so that $G \simeq \mathbf{Z}/9\mathbf{Z}$ and we should expect even traces 1/9 ($\sim 0.1111$) of the time. Computing[2] the traces for split primes up to $10^6$ for this field

[2] On a PC with the infinite precision number theoretic language PC-ALGEB using algorithms developed in [2]

https://doi.org/10.4153/CMB-1991-031-2 Published online by Cambridge University Press

we find that there are 4,327 even traces and 34,890 odd traces ($\sim 0.1103$ and $\sim 0.8897$, respectively).

If the 3-primary component of $G$ is elementary abelian of order $3^N$ then a quick calculation shows $n = (3^N - 2)h'$ ($h'$ again the order of $G$ prime to 3) so that in this case the majority $(3^N - 2)/\, 3^N$ of traces are even. For example, the field $\mathbf{Q}(\sqrt{-307})$ has class number 3 with the ideal $\mathcal{P}_7$ above 7 as generator. Since $\mathcal{P}_7^3 = 6 + \sqrt{-307} \equiv 1 \bmod (2)$ in this case the extension (1) splits so that $G \simeq \mathbf{Z}/\,3\mathbf{Z} \times \mathbf{Z}/\,3\mathbf{Z}$ and we should expect even traces 7/9 ($\sim 0.7778$) of the time. Here the traces for split primes up to $10^6$ give 32,972 even traces and 9,452 odd traces ($\sim 0.7772$ and $\sim 0.2228$, respectively).

As the 3-primary component of $G$ (or of $C_k$) becomes more interesting the proportion of even and odd traces becomes more interesting. We give the following two examples[3]:

(1) The field $\mathbf{Q}(\sqrt{-4027})$ has class number 9 with class group $C_k \simeq \mathbf{Z}/\,3\mathbf{Z} \times \mathbf{Z}/\,3\mathbf{Z}$ (generators are $\mathcal{P}_{13}$ and $\mathcal{P}_{17}$). Since

$$\mathcal{P}_{13}^3 = \frac{69 + \sqrt{-4027}}{2} \not\equiv 1 \mod 2$$

the ideal $\mathcal{P}_{13}$ has order 9 in the ray class group, so that $G \simeq \mathbf{Z}/\,9\mathbf{Z} \times \mathbf{Z}/\,3\mathbf{Z}$. A simple calculation then shows that $n = 7$ here so that even traces occur with density 7/27 (= .2593). Computations give 10,063 even and 29,013 odd traces for the split primes less than $10^6$($\sim 0.2575$ and $\sim 0.7425$, respectively).

(2) The field $\mathbf{Q}(\sqrt{-3299})$ has class number 27 with class group $C_k \simeq \mathbf{Z}/\,9\mathbf{Z} \times \mathbf{Z}/\,3\mathbf{Z}$ (generators are $\mathcal{P}_3$ (of order 9) and $\mathcal{P}_{11}$ (of order 3)). Since

$$\mathcal{P}_{11}^3 = \frac{45 + \sqrt{-3299}}{2} \not\equiv 1 \mod 2$$

the ideal $\mathcal{P}_{11}$ has order 9 in the ray class group, so that $G \simeq \mathbf{Z}/\,9\mathbf{Z} \times \mathbf{Z}/\,9\mathbf{Z}$. Here $n = 61$ so that even traces occur with density $61/\,81$(=.7531). Computations give 29,542 even and 9,613 odd traces ($\sim 0.7545$ and $\sim 0.2455$, respectively).

REMARK 1. Computations of the Iwasawa $\lambda$-invariants for imaginary quadratic fields $k$ for various primes $p$ utilizing a test due to Gold, Sinnott *et al* showed that the integer solutions $t \in \mathbf{Z}$ of the congruence

$$t^{p-1} + pt^{p-3} - 1 \equiv 0 \mod p^2 \tag{2a}$$

satisfying the further Archimedean constraint

$$0 < t < 2\sqrt{p} \tag{2b}$$

were disproportionately odd: for $p < 6{,}580{,}633$ the proportions are $748/1145 = .6533\ldots$ and $397/1145 = .3466\ldots$ [If the prime $p$ splits in $k$ into principal primes, $p = \pi\bar{\pi}$ then

[3] The famous examples of nontrivial 3-ranks of Scholz and Taussky [4]

https://doi.org/10.4153/CMB-1991-031-2 Published online by Cambridge University Press

Gold's test for $\lambda_p > 1$ is to check whether $\log_p \pi \equiv 0 \bmod \bar{\pi}^2$ where the equation is considered in the $\bar{\pi}$-adic embedding of $k$ into $\mathbf{Q}_p$ and $\log_p$ is the associated $p$-adic logarithm. Writing $\pi = (t + b\sqrt{-D})/2$, where $t \in \mathbf{Z}$ is the trace of $\pi$, it is easy to see that Gold's test is precisely equation (2a). Turning this around, fixing $p$ and solving for all solutions $t$ of (2a) subject to (2b) gives all $D$ for which $p$ splits into principal primes in $\mathbf{Q}(\sqrt{-D})$ and $\lambda_p > 1$ (the Archimedean constraint (2b) is required so that $4p - t^2$ $(= b^2D)$ is positive), so in particular determines all $p$ with $\lambda_p > 1$ for the imaginary quadratic fields of class number 1.] Trying to explain this distribution led to the question of the general distribution of traces in imaginary quadratic fields considered here.

If $t$ is a solution to (2a) and (2b) then $s = 2p-t^2$ is a solution to the equation $s^{(p-1)/2} \equiv 1 \bmod p^2$, satisfying $-2p < s < 2p$. The value $s = 1$ is always a solution to this latter equation and, conversely, if $2p - 1$ is a square, we have a solution to (2a) (with $s = 1$ and $t$ odd). Examining the tables shows that the parity of the values remaining when the primes $p$ with $2p - 1$ a square are removed are approximately evenly distributed.

If we assume that the values of $p$ with $2p - 1$ a square account for the abundance of odd solutions to (2a), then A. Granville has supplied the following heuristic for the distribution of these values. The probability that $t$ satisfies (2a) is $1/p$, so the suggested number of even solutions in our range is approximately $\sqrt{p}/p$. Hence the number of even solutions up to $x$ is approximately

$$\sum_{p \leqq x} 1/\sqrt{p} \approx \int_1^x \frac{1}{\sqrt{t}\log t}\, dt \approx 2x^{1/2}/\log x.$$

Similarly, the expected number of odd solutions of (2a) in our range is $2x^{1/2}/\log x$ plus the number of primes $p \leqq x$ for which $2p - 1$ is a square. If $2p - 1 = d^2$, then $d \leqq \sqrt{2x}$ and $d = 2n+1$ is odd. Hence we wish to count the number of integers $n \leqq \sqrt{x/2}$ such that $2n^2 + 2n + 1$ is a prime. A classical conjecture of Hardy-Littlewood, Schinzel-Sierpinski predicts that

$$\#\{\, n \leqq x \mid 2n^2 + 2n + 1 \text{ is prime } \} \approx Cx/\log x$$

with

$$C = \prod_{p=\text{odd prime}} \frac{1 - \omega(p)/p}{1 - 1/p}$$

where $\omega(p)$ is the number of residue classes $n \bmod p$ for which $2n^2 + 2n + 1 \equiv 0 \bmod p$. Since $2n^2 + 2n + 1 \doteq n^2 + (n+1)^2$, this is equivalent to the assertion that $-1$ is a square, hence

$$\omega(p) = \begin{cases} 0 & \text{if } p \equiv 3 \bmod 4 \\ 2 & \text{if } p \equiv 1 \bmod 4 \end{cases},$$

which gives $C \approx 1.372$ (computing the product for the first million primes). It follows that the expected number of odd solutions to (2a) would be approximately (2 +

https://doi.org/10.4153/CMB-1991-031-2 Published online by Cambridge University Press

$C\sqrt{2})x^{1/2}/\log x$, hence that the proportion of odd to even solutions would be $1+(C/\sqrt{2})$ $\approx 1.97$.

REMARK 2. Let now $E$ be an elliptic curve defined over the Hilbert class field $F$ of $k$ which has complex multiplication by $O_k$. Let $\psi_{F/k}$ be the associated Grössencharacter of $E$. For $v$ a prime of $F$ of good reduction for $E$, $\psi_{F/k}(v) = \pi_v \in k^x$ where $\pi_v$ is the element of $O_k$ such that multiplication by $\pi_v$ is the Frobenius morphism $(x,y) \longmapsto (x^{q_v}, y^{q_v})$ on the (affine part of the) reduced curve $\tilde{E}/\mathbf{F}_{q_v}$ over the residue field $\mathbf{F}_{q_v}$ for $v$.

If $\mathcal{P}$ is the prime of $k$ lying below $v$, then the element $\pi_v$ is a generator for $\mathcal{P}^f$ where $f$ is the order of $\mathcal{P}$ in the class group of $k$ (and $q_v = p^f$ above), so that the traces $a_p$ considered above are the traces of Frobenius in the sense of elliptic curves, i.e. are coefficients of the $L$-series for $E$ (or of the associated modular form). The results above can then be interpreted as giving the distribution of the parity of the coefficients $a_p$ of the associated modular forms.

This can also be seen directly from the elliptic curves by considering the Galois action on the 2-division points of the curve (which is the Galois action on the quotient $T_2/2T_2$ of the 2-adic Tate module $T_2$ and so determines the mod 2 behavior of the traces of Frobenius for most primes). The equivalence of this with the field-theoretic approach above is just the classical complex multiplication theory for elliptic curves which relates the ray class field to conductor (2) to the field obtained by adjoining the 2-division points of an elliptic curve having complex multiplication by $O_k$.

Finally we note that this latter approach also applies for example to elliptic curves defined over $\mathbf{Q}$ which are not complex multiplication curves and shows that the parity distribution of the coefficients $a_p$ of their $L$-series is determined by the splitting of primes in the field obtained by adjoining the 2-division points of the curve (*cf*. Serre [5], [6] where these and other modular forms are considered). For example, the tables [1] provide examples of parity distributions similar to those considered above, determined by the rationality of the 2-division points (note also that if the curve has good reduction at 2 then it is possible to have $a_2$ odd and all other traces even — analogous to the case $D \equiv 7 \bmod 8$ considered above). For example, the modular form $\eta(z)^2\eta(11z)^2$ (whose coefficients were previously computed in connection with [3])) arises from the curve $E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$ and the coefficients $a_p$ are odd with density 1/3 (the 2-division points generate an $S_3$ extension of $\mathbf{Q}$ and 2 of the 6 invertible $2 \times 2$ matrices with coefficients in $\mathbf{F}_2$ have even trace).

## REFERENCES

**1.** B. J. Birch and W. Kuyk, ed., *Modular Functions of One Variable, IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, New York, 1975.

**2.** D. S. Dummit, D. Ford, H. Kisilevsky and J. Sands, *Computation of Iwasawa $\lambda$-invariants for imaginary quadratic fields*, in preparation.

**3.** D. S. Dummit, H. Kisilevsky and J. McKay, *Multiplicative products of $\eta$-functions*, Contemporary Mathematics, Vol. **45** (1985), Amer. Math. Soc., 89–98.

https://doi.org/10.4153/CMB-1991-031-2 Published online by Cambridge University Press

**4.** A. Scholz and O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginär-quadratischen Zahlkörper: ihre rechnerishe Bestimmung und ihr Einfluß auf der Klassenkörperturm, J. Reine Angew. Math., **171** (1934), 19–41.

**5.** J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Ens. Math., **22** (1976), 227–260.

**6.** J.-P. Serre, *Quelques applications du Théoreme de Densité de Chebotarev*, Publ. Math. I.H.E.S., no. **54** (1981), 123–201.

*Department of Mathematics*
*Concordia University—Loyola Campus*
*Montreal, Quebec, H4B 1R6.*

https://doi.org/10.4153/CMB-1991-031-2 Published online by Cambridge University Press