# Irregularity of Prime Numbers over Real Quadratic Fields

Joshua Holden

Department of Mathematics and Statistics, University of Massachusetts at Amherst
Amherst, MA 01003, USA
holden@math.umass.edu

**Abstract.** The concept of regular and irregular primes has played an important role in number theory at least since the time of Kummer. We extend this concept to the setting of arbitrary totally real number fields $k_0$, using the values of the zeta function $\zeta_{k_0}$ at negative integers as our "higher Bernoulli numbers". Once we have defined $k_0$-regular primes and the index of $k_0$-irregularity, we discuss how to compute these indices when $k_0$ is a real quadratic field. Finally, we present the results of some preliminary computations, and show that the frequency of various indices seems to agree with those predicted by a heuristic argument.

## 1 Definitions and Basic Concepts

Let $k_0$ be a totally real number field, and let $p$ be an odd prime. Let $k_1 = k_0(\zeta_p)$, where $\zeta_{p^n}$ will denote a primitive $p^n$-th root of unity. Let $\Delta = \mathrm{Gal}(k_1/k_0)$, and let $\delta = |\Delta|$. Let $p^e$ be the largest power of $p$ such that $\zeta_{p^e} \in k_0(\zeta_p)$.

**Definition 1.** *Let $\zeta_{k_0}$ be the zeta function for $k_0$. We say that $p$ is* $k_0$-regular *if $p$ is relatively prime to $\zeta_{k_0}(1-2m)$ for all integers $m$ such that $2 \leq 2m \leq \delta - 2$ and also $p$ is relatively prime to $p^e\zeta_{k_0}(1-\delta)$. The number of such zeta-values that are divisible by $p$ will be the* index of $k_0$-irregularity *of $p$.*

It is well-known that the numbers $\zeta_{k_0}(1-2m)$ and $p^e\zeta_{k_0}(1-\delta)$ are rational; see, e.g., [16]. In fact we can show that they are $p$-integral. Deligne and Ribet [6] have shown that one can construct an $p$-adic $L$-function $L_p(s,\rho)$ for even characters $\rho$ over a totally real field $k_0$. Furthermore, there exists a power series $f_\chi \in \mathbf{Z}_p[[T]]$ such that

$$L_p(1-s,\omega\chi^{-1}) = f_\chi(u^s-1)/h_\chi(u^s-1)$$

for $s \in \mathbf{Z}_p$, where $h_\chi(T) = T$ if $\chi = \omega$ (the $p$-adic Teichmüller character) and $h_\chi(T) = 1$ otherwise, and $u$ is a certain element of the principal units of $\mathbf{Z}_p$. The $p$-adic $L$-function $L_p(1-n,\rho)$ is equal to $L(1-n,\rho\omega^{-n})$ at negative integers, up to some fudge factors which are units. If $s = 2m$ is a positive integer then $u^{2m}-1$ is in $\mathbf{Z}_p$ and so is $f_\chi(u^{2m}-1)$. The case $2m < \delta$ corresponds to $\chi \neq \omega$, so $L_p$ is $p$-integral and thus so is $L(1-2m,1) = \zeta_{k_0}(1-2m)$. The case of $2m = \delta$

J.P. Buhler (Ed.): ANTS-III, LNCS 1423, pp. 454–462, 1998.

is similar, with $h_\chi(u^\delta - 1) = u^\delta - 1$ being equal to $p^e$, up to a unit. (For more details, see [14].)

The definition of $p$ being $k_0$-regular is consistent with that of $p$ being regular, since if $k_0 = \mathbf{Q}$ we have $\delta = p - 1$, $L(1 - 2m, 1) = -B_{2m}/(2m)$ for $B_{2m}$ the $2m$-th Bernoulli number, $2 \leq 2m \leq p - 3$, and $p$ never divides $p^e L(2 - p, 1) = -pB_{p-1}/(p-1)$ by the Claussen-von Staudt Theorem (Theorem 5.10 of [20]) or by the argument given in Section 2 of [17]. Also, $k_0$-regularity seems to share at least some of the properties of regularity. For example, by a proof analogous to one for the case over $\mathbf{Q}$, there are infinitely many $k_0$-irregular primes for any given $k_0$.

As applications of this concept, we have the following two theorems (see [14]). The first is a special case of the Fontaine-Mazur Conjecture for number fields. Let $k_n = k_0(\zeta_{p^n})$ for $n > 1$ be a non-trivial extension of $k_1$. Let $K = \bigcup k_n$.

**Theorem 1 (Holden).** *Suppose $p$ is $k_0$-regular. Then there are no unramified infinite powerful pro-$p$ extensions $M$ of $k_n$, Galois over $k_0$, such that $K \cap M = k_n$ and $\mathrm{Gal}(M_{el}/k_n) = \mathrm{Gal}(M_{el}/k_n)^-$ according to the action of $\Delta$, where $M_{el}$ is the maximal elementary abelian subextension of $M/k_n$.*

The second theorem is an improvement of a theorem of Greenberg. A more limited version of the concept of $k_0$-regularity, though not the definition itself, appeared in Greenberg's paper [11], which presents a generalization of Kummer's criterion for the class number of $k_1$ to be divisible by $\ell$.

Let $k_1^+$ denote the maximal real subfield of $k_1$, which is equal to $k_0(\zeta_p + \zeta_p^{-1})$. Let $h(k_1)$ denote the class number of $k_1$ and $h^+(k_1)$ denote the class number of $k_1^+$. It is known that $h^+(k_1) \mid h(k_1)$; we let the relative class number $h^-(k_1)$ be the quotient.

**Theorem 2 (Greenberg, Holden).** *Assume that no prime of the field $k_1^+$ lying over $p$ splits in $k_1$. Then $p$ divides $h^-(k_1)$ if and only if $p$ is not $k_0$-regular.*

Ernvall, in [7,8,9], has defined a notion of "generalized irregular primes" which is closely related to mine for abelian $k_0$. Also, Hao and Parry, in [12], defined $m$-regular primes for any integer $m$ and showed they are equivalent to what I have called $D$-regular primes when $m$ is a positive discriminant. In both cases, results stronger than Theorem 2 are proved, but only for abelian $k_0$.

## 2 Computation

For the rest of this paper, $k_0$ will be a real quadratic field $\mathbf{Q}(\sqrt{D})$, with $D$ a positive fundamental discriminant. For such a $k_0$, we will say that primes are $D$-regular or have given index of $D$-irregularity, and we will let the zeta function $\zeta_{k_0}$ be also denoted by $\zeta_D$. In this case $\delta$ will be equal to $p - 1$ unless $D = p$, in which case $\delta = (p-1)/2$. Also, $e$ is always equal to 1 when $p$ does not divide the order of $k_0$ over $\mathbf{Q}$, which is true in this case since $p$ is odd. (The case of $p = 2$ is quite similar, but we will not go into it here.)

The first order of business is clearly to compute $\zeta_D(1-2m)$ for $m \geq 1$ an integer. We know that $\zeta(1-2m) = -B_{2m}/(2m)$, and using similar methods Siegel showed that

$$\zeta_D(1-2m) = \frac{B_{2m}}{4m^2} D^{2m-1} \sum_{j=1}^{D} \chi(j) B_{2m}(j/D) \ .$$

(See [18] and [21].) Here $\chi(j) = \left(\frac{D}{j}\right)$, the Kronecker symbol, and $B_{2m}(j/D)$ indicates the $2m$-th Bernoulli polynomial evaluated at the fraction $j/D$. The Bernoulli polynomial $B_r(x)$ can be computed from the Bernoulli numbers as

$$B_r(x) = \sum_{s=0}^{r} \binom{r}{s} B_{r-s} x^s \ .$$

(This is not the most profound formula Siegel found for such zeta functions, and it is probably also not the fastest. It is, however, the easiest to understand and to program, and so it seems reasonable to start with a thorough analysis of this formula before going on to others. For more on these other expressions, see [19], [21], and [4]. Also, there is a formula called the "continued fraction formula" for these zeta-values, which is likely to be faster but uses more computer storage space. For more on this, see [13].)

In order to determine whether a prime $p$ is $D$-irregular, we will need to know the values of $\zeta_D(1-2m)$ for all $2 \leq 2m \leq \delta$, which in most cases will be $2 \leq 2m \leq p-1$. Thus it is most efficient to first compute all $\zeta_D(1-2m)$ for a range $2 \leq 2m \leq M$ and then use them to test all primes $p$ such that $3 \leq p \leq M+1$. The time to check whether $p$ divides $\zeta_D(1-2m)$ or $p\zeta_D(1-\delta)$, and even to what order, is then much smaller than the time to compute $\zeta_D(1-2m)$ in the first place. Therefore it is interesting, and sometimes useful, to find the order of the running time (in $m$ and $D$) of the computation of $\zeta_D(1-2m)$.

Since the Bernoulli numbers are ubiquitous in this computation, we will assume that they have been precomputed. For more on the computation of Bernoulli numbers, see e.g. [1] and [10]. Our cost model will assume "naive" arithmetic: if the arguments are integers with bit length $t$ and $t'$, we assign a cost of $O(t+t')$ to addition and subtraction and $O(tt')$ to multiplication and division. For rational numbers, there is the phenomenon of "coefficient explosion" when we put fractions over a common denominator to add them. We will deal with this by computing a common denominator of the Bernoulli polynomials in the zeta function beforehand and assuming that all of our values are expressed over it, thus reducing the problem to precomputation and integer arithmetic. For more on the time-complexity of arithmetic, see e.g. Section 1.1.2 of [5].

First we will need to calculate

$$\begin{aligned} B_{2m}(j/D) &= \sum_{s=0}^{2m} \binom{2m}{s} B_{2m-s}(j/D)^s \\ &= \sum_{s=0}^{2m} \frac{(2m)!}{s!(2m-s)!} B_{2m-s}(j/D)^s \ . \end{aligned}$$

All of the fractions in this expression have a common denominator equal to the product of the denominators of $B_0, \ldots, B_{2m}$ times $D^{2m}$, and this is the same for each $j$. Thus we will assume that the Bernoulli numbers are precomputed over this denominator. (We will discuss the cost of this precomputation later.) The way to compute the Bernoulli polynomial which is asymptotically fastest seems to be to start with $B_0$ and repeatedly perform the operation of multiplying by

$$\frac{s}{2m-s+1}(j/D)$$

and then adding $B_s$, as $s$ goes from 1 to $2m$. (This idea, which is used by PARI to compute Bernoulli numbers, may go back to Lehmer. The papers [10] and [1] investigate some fast methods of computing Bernoulli numbers using "inexact" arithmetic due to Wilf, Buhler, et al., which may also be useful for Bernoulli polynomials. However, they require a faster multiplication algorithm to be worthwhile.) In order to figure out how long this will take, we first need to know the bit length of $B_s$, stored as a rational number. Using a standard estimate of the size of Bernoulli numbers, we see that

$$|B_s| = O\left(\left(\frac{s}{2\pi e}\right)^s\right) \ .$$

(See Chapter 15 of [15], or Section 3 of [1], for example.) Since we need to keep the Bernoulli numbers over a common denominator, our denominator will be $D^{2m}$ times the product of the denominators of $B_0, \ldots, B_{2m}$, and the Claussen-von Staudt Theorem shows that this second factor is

$$\prod_{\substack{1 \le 2k \le m \\ (p-1) | 2k}} p \ .$$

Bach shows in [1] that the bit size of this is $O(m \lg m)$, so the bit size of our denominator as a whole is $O(m(\lg m + \lg D))$. Thus the bit length of $B_s$, which is the bit length of the numerator plus the bit length of the denominator, is

$$O\left(\lg\left(\frac{s}{2\pi e}\right)^s + 2m(\lg m + \lg D)\right) \ ,$$

or $O(m(\lg m + \lg D))$. The order of running time is controlled by $2m$ multiplications of $(s/(2m-s+1))(j/D)$ by the result of the previous step. The first factor has bit length of order $O(\lg m + \lg D)$, while the second factor has a bit length of the same order as the final result, $B_{2m}(j/D)$, which from its definition can be seen to have bit length of order $O(m + m(\lg m + \lg D) + m \lg D) + O(\lg D) = O(m(\lg m + \lg D))$. (Note that the binomial coefficient is less than $2^{2m}$.) Thus the total time to compute $B_{2m}(j/D)$ is $O(m)O(\lg m + \lg D)O(m(\lg m + \lg D)) = O(m^2(\lg^2 D + \lg^2 m + \lg D \lg m))$.

Now we need to compute

$$\zeta_D(1-2m) = \frac{B_{2m}}{4m^2} D^{2m-1} \sum_{j=1}^{D} \chi(j) B_{2m}(j/D) \ .$$

Computing the Kronecker symbol $\chi(j) = \left(\frac{D}{j}\right)$ takes time $O(\lg^2 D)$ which is not significant compared to computing $B_{2m}(j/D)$. (See, for example, Section 1.4.2 of [5].) The product $\chi(j)B_{2m}(j/D)$ needs to be calculated $D$ times, which takes $O(Dm^3 \lg D(\lg m + \lg D))$, and then added up, which is not significant. The rest of the calculations are of about the same running time as one calculation of $B_{2m}(j/D)$, and thus do not contribute. The bit lengths are also of the same order as those we have already calculated, giving us a total computation time of

$$O(Dm^2(\lg^2 D + \lg^2 m + \lg D \lg m))$$

and a total bit length of $O(m(\lg m + \lg D))$.

We should add to this the time to put the Bernoulli numbers over a common denominator. Since we are planning to compute all $\zeta_D(1-2m)$ for a range $2 \leq 2m \leq M$, we can start with a small common denominator and update it as we increase $m$. In fact, since we need a precomputed table of Bernoulli numbers up to $B_M$, it seems to make more sense to precompute them initially over a common denominator for all of them. Then we need only to update the factor of $D^{2m}$, which involves a multiplication by $D^2$ of each of $O(m)$ numbers of bit size $O(m \lg m)$, for a total time of $O(m^2 \lg D \lg m)$, which is of the same order as the above computations. (If we also updated the common denominator of the Bernoulli numbers at each step, we would have a similar time-complexity.) Finally, we conclude that if the time necessary to compute $\zeta_D(1-2m)$ is $O(Dm^2(\lg^2 D + \lg^2 m + \lg D \lg m))$, then the time necessary to compute all $\zeta_D(1-2m)$ for a range $2 \leq 2m \leq M$ and then use them to test all primes $p$ such that $3 \leq p \leq M+1$ is $O(DM^3(\lg^2 D + \lg^2 M + \lg D \lg M))$.

Implementing the algorithm using the PARI-GP program (see [2] for more information) and a Sun SPARCstation-10 computer, we have in Table 1 a few examples of actual processor times in hours, minutes, and seconds. These times include an estimated 14.5 seconds used in starting up PARI-GP and loading the programs and Bernoulli numbers from disk.

**Table 1.** Examples of processor times

| $D$ | $M$ | running time |
|---|---|---|
| 5 | 1000 | 55:01.9 |
| 8 | 1000 | 1:28:47.7 |
| 12 | 1000 | 2:17:34.5 |
| 13 | 1000 | 2:43:22.6 |

We may compare these time estimates to those of others working with generalized notions of irregularity. Ernvall does not seem to have a general algorithm, and his algorithms for special cases do not overlap ours, although they are similar to those of Hao and Parry. Hao and Parry have an algorithm for testing $D$-irregularity which does not compute zeta-values explicitly. It checks

whether $p$ divides $\zeta_D(1-2m)$ (or $p\zeta_D(1-\delta)$) in time $O(Dp\lg^3 p + D\lg^2 D)$. Thus the index of $D$-irregularity for $p$ is calculated in time $O(Dp^2\lg^3 p + Dp\lg^2 D)$. To then check all primes $p$ such that $3 \le p \le M+1$ takes $O(DM^2\lg^3 M + DM\lg^2 D)O(M/\lg M) = O(DM^3\lg^2 M + DM^2\lg^2 D/\lg M)$ by the Prime Number Theorem. This is comparable to our running time in both $D$ and $M$. Since Hao and Parry's algorithm does not use Bernoulli numbers, and in fact fundamentally uses only integers, it requires no precomputation and is likely always to be faster in practice. On the other hand, since it does not compute zeta-values it cannot provide any extra information. In particular, it cannot tell whether a higher power of $p$ divides $\zeta_D(1-2m)$, an issue we will address in the next section.

## 3 Predictions and Data

There is a heuristic argument which has been used to predict the fraction of primes with a given index of **Q**-irregularity. If one assumes that for any prime $p$ the Bernoulli numbers are distributed randomly modulo $p$ (i.e. $B_{2m}$ is divisible by $p$ with probability $1/p$), then the probability that the index of irregularity $i(p)$ is equal to $k$ should be

$$\binom{\frac{p-3}{2}}{k}\left(1-\frac{1}{p}\right)^{\frac{1}{2}(p-3)-k}\left(\frac{1}{p}\right)^k \ ,$$

which approaches

$$f(k) = \frac{1}{k!}\left(\frac{1}{2}\right)^k e^{-1/2}$$

as $p$ goes to infinity. (See, e.g., section 5.3 of [20].) The resulting predicted fractions appear to agree well with computer calculations of actual percentages of irregular primes, for example the work of Buhler, Crandall, Ernvall, and Metsänkylä in [3] for the primes less than 4000000.

A similar argument can be given for $D$-irregular primes. In this case it is well-known that $\zeta_D(s) = \zeta(s)L(s,\chi)$, where $\chi(j) = \left(\frac{D}{j}\right)$, the Kronecker symbol. Thus each $\zeta_D(1-2m)$ and each $p\zeta_D(1-\delta)$ breaks up into two pieces. The first piece behaves essentially like $B_{2m}$ in terms of distribution modulo $p$. We will assume that the second piece is independent of the first modulo $p$, and is also evenly distributed. We would then predict that the probability that $p$ divides the second piece is

$$\binom{\frac{p-1}{2}}{k}\left(1-\frac{1}{p}\right)^{\frac{1}{2}(p-1)-k}\left(\frac{1}{p}\right)^k \ ,$$

which also goes to $f(k)$. Then the expected probability of $p$ having index of $d$-irregularity $i_D(p)$ equal to $k$ would be

$$\sum_{i+j=k} f(i)f(j) \ ,$$

where $i, j \ge 0$.

Since the behavior of the first piece is well-studied for primes up to 4000000, we concentrate on the second piece. We let $i_D^{(2)}(p)$ be the number of zeta-values for which the second piece is divisible by $p$. The PARI-GP program was used to compute the index of $D$-irregularity for various ranges of primes and various values of $D$. For $D = 5$, 8, 12, and 13, the actual numbers and fractions of the 167 primes less than 1000 with $i_D^{(2)}(p) = k$ are shown in Table 2. For comparison, Table 3 gives values of $f(k)$ for small $k$.

**Table 2.** Results for $D = 5, 8, 12, 13$ and $p < 1000$

| $k$ | $D=5$ Number | $D=5$ Fraction | $D=8$ Number | $D=8$ Fraction | $D=12$ Number | $D=12$ Fraction | $D=13$ Number | $D=13$ Fraction |
|---|---|---|---|---|---|---|---|---|
| 0 | 112 | .670659 | 108 | .646707 | 102 | .610778 | 103 | .616766 |
| 1 | 43 | .257485 | 47 | .281437 | 53 | .317365 | 44 | .263473 |
| 2 | 11 | .065868 | 11 | .065868 | 11 | .065868 | 17 | .101796 |
| 3 | 1 | .005988 | 1 | .005988 | 0 | 0 | 3 | .017964 |
| 4 | 0 | 0 | 0 | 0 | 1 | .005988 | 0 | 0 |

**Table 3.** Values of $f(k)$

| $k$ | $f(k)$ |
|---|---|
| 0 | .606531 |
| 1 | .303265 |
| 2 | .075816 |
| 3 | .012636 |
| 4 | .001580 |

The average number and fraction of the 24 primes less than 100 with $i_D^{(2)}(p) = k$ was also calculated, for all $D$ less than 100. Table 4 gives the results.

**Table 4.** Results for $D < 100$ and $p < 100$

| $k$ | Average Number | Average Fraction |
|---|---|---|
| 0 | 15.3 | .637500 |
| 1 | 7.16667 | .298611 |
| 2 | 1.23333 | .051389 |
| 3 | 0.26667 | .011111 |
| 4 | 0.03333 | .001389 |

While these samples are far too small to be conclusive, they seem to indicate some merit to the heuristic argument.

One other notable observation is that $p^2$ sometimes divides $\zeta_D(1-2m)$ or $p\zeta_D(1-\delta)$. This is something which has not yet been observed over $\mathbf{Q}$, and a similar heuristic to the one above predicts that the probability of it drops to 0 as $p$ goes to infinity. However, for discriminants less than 100 we observe 12 total occurrences for primes less than 50, including 2 where $p^3$ divides. In the case of $\zeta_{77}(1-32)$, $p=37$, we have $p$ dividing both the first piece and the second piece; in the other cases $p^2$ divides the only second piece. For the same discriminants there are only 4 occurrences for primes between 50 and 100; in each of them $p^2$ exactly divides the second piece and $p$ does not divide the first. For $D=5$ this phenomenon happens once more in the primes less than 1000, at $\zeta_5(1-216)$, $p=443$, where $p^2$ exactly divides the second piece. For $D=8$, at $\zeta_8(1-92)$, $p=587$, and for $D=12$, at $\zeta_{12}(1-520)$, $p=929$, $p$ divides the first and second pieces once each. For $D=13$, $p^2$ does not divide any of the zeta-values we have calculated. Once again, the evidence so far seems to agree with the heuristic prediction.

## Acknowledgments

The author would like to thank David Hayes, for his comments on a draft of this paper; Michael Rosen, for supervising the thesis which was the starting point from which this work diverged; and the Brown Mathematics Department and especially Joseph Silverman for the use of the department's computing facilities in the preliminary stages of this research. I would also like to thank Masanobu Kaneko for the e-mail exchange which led me to start thinking about faster ways to compute Bernoulli polynomials.

## References

1. Eric Bach. The complexity of number-theoretic constants. *Information Processing Letters*, 62:145–152, 1997.
2. C. Batut, D. Bernardi, H. Cohen, and M. Olivier. *User's Guide to PARI-GP*. Laboratoire A2X, Université Bordeaux I, version 1.39 edition, January 14, 1995. `ftp://megrez.math.u-bordeaux.fr`.
3. J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä. Irregular primes and cyclotomic invariants up to four million. *Mathematics of Computation*, 59:717–722, 1992.
4. Henri Cohen. Variations sur un thème de Siegel et Hecke. *Acta Arithmetica*, 30:63–93, 1976.
5. Henri Cohen. *A Course in Computational Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.
6. Pierre Deligne and Kenneth Ribet. Values of abelian $L$-functions at negative integers over totally real fields. *Inventiones Mathematicae*, 59:227–286, 1980.
7. Reijo Ernvall. Generalized Bernoulli numbers, generalized irregular primes, and class number. *Annales Universitatis Turkuensis. Series A. I.*, 178, 1979. 72 pp.

8. Reijo Ernvall. Generalized irregular primes. *Mathematika*, 30:67–73, 1983.
9. Reijo Ernvall. A generalization of Herbrand's theorem. *Annales Universitatis Turkuensis. Series A. I.*, 193, 1989. 15 pp.
10. Sandra Fillebrown. Faster computation of Bernoulli numbers. *Journal of Algorithms*, 13:431–445, 1992.
11. Ralph Greenberg. A generalization of Kummer's criterion. *Inventiones Mathematicae*, 21:247–254, 1973.
12. Fred H. Hao and Charles J. Parry. Generalized Bernoulli numbers and $m$-regular primes. *Mathematics of Computation*, 43:273–288, 1984.
13. David Hayes. Brumer elements over a real quadratic field. *Expositiones Mathematicae*, 8:137–184, 1990.
14. Joshua Holden. *On the Fontaine-Mazur Conjecture for Number Fields and an Analogue for Function Fields.* PhD thesis, Brown University, 1998.
15. Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics.* Springer-Verlag, second edition, 1990. Second Corrected Printing.
16. Kenneth Ribet. Report on $p$-adic $L$-functions over totally real fields. *Asterisque*, 61:177–192, 1979.
17. Michael Rosen. Remarks on the history of Fermat's last theorem 1844 to 1984. In Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 505–525. Springer-Verlag, 1997.
18. Carl Ludwig Siegel. Bernoullische Polynome und quadratische Zahlkörper. *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-physikalische Klasse*, 2:7–38, 1968.
19. Carl Ludwig Siegel. Berechnung von Zetafunktionen an ganzzahligen Stellen. *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-physikalische Klasse*, 10:87–102, 1969.
20. Lawrence C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, second edition, 1997.
21. Don Zagier. On the values at negative integers of the zeta-function of a real quadratic field. *L'Enseignement Mathématique II Série*, 22:55–95, 1976.