Comparison of Algorithms to Calculate "Quadratic Irregularity" of Prime Numbers: Extended Abstract

Joshua Holden*

August 6, 2002

One common way of constructing public-key cryptographic systems is to utilize the problem of finding a discrete logarithm in some abelian group. Groups that have been utilized for this purpose include $\mathbf{F}_q^*$ in the Massey-Omura and ElGamal cryptosystems and the group of points on an elliptic curve in elliptic curve cryptosystems. (See [5] for background, for example.) Another possibility which has been proposed by Buchmann and Williams (see, e.g., [1]) is to use the group of ideal classes in a number field. In order to make sure that the discrete logarithm problem is computationally hard, one needs to know something about the structure of the group involved, e.g. that it is divisible by a large prime. One situation in which it is easy to show this is in the case of the class group of $\mathbf{Q}(\zeta_p)$; according to a well-known theorem of Kummer, p divides the order of the class group of $\mathbf{Q}(\zeta_p)$ if and only if p divides the numerator of a Bernoulli number B_m for some even m such that $2 \leq m \leq p-3$. Such primes are called irregular; the others are called regular.

We extend the concept of regular and irregular primes to the setting of arbitrary totally real number fields k_0, using the values of the zeta function ζ_{k_0} at negative integers as our "higher Bernoulli numbers". In this setting the author proved in his thesis ([4]), building on work of Greenberg and Kudo, that under a certain technical condition Kummer's criterion can be extended to give information about whether p divides the class group of $k_0(\zeta_p)$. Thus we are interested in the feasibility of finding these analogues of irregular primes, since their associated class groups may be especially suitable for cryptography.

In the case where k_0 is a real quadratic field, Siegel, in [6], presented two formulas for calculating these zeta-values: one using entirely elementary methods and one which is derived from the theory of modular forms. (See also [7] and [2] for a discussion of these formulas. The author would like to thank Henri Cohen for suggesting an analysis of the second formula.) We will briefly discuss several algorithms based on these formulas and compare the running time involved in using them to determine the index of k_0-irregularity of a prime number. (The author has already discussed one of these algorithms in [3].)

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

1 Definitions

Let k_0 be a totally real number field, and let p be an odd prime. Let $k_1 = k_0(\zeta_p)$, where ζ_{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 Let ζ_{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.

Then the extension of Kummer's criterion mentioned above is as follows: 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 1 (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.*

For the case we consider, 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 ζ_{k_0} be also denoted by ζ_D. In this case δ 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. For the condition in Theorem 1 that no prime of the field k_1^+ lying over p splits in k_1 to be satisfied it is sufficient that p should not divide D, and we should also note that since p does not divide the degree of $k_0 = \mathbf{Q}(\sqrt{D})$ over $\mathbf{Q}$, a theorem of Leopoldt shows that p divides $h(k_1)$ if and only if p divides $h^-(k_1)$.

We will assume throughout that all multiplication is done using a naive algorithm, unless otherwise noted.

2 First formula

Siegel's first formula to compute $\zeta_D(1-2m)$ for $m \geq 1$ an integer is analogous to the formula $\zeta(1-2m) = -B_{2m}/(2m)$. Using elementary methods, Siegel showed that similarly

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

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

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

We will assume throughout that B_j, $1 \le j \le M$, are precomputed over a common denominator. A first attempt at an algorithm based on (1) might compute $B_0(\alpha), \ldots, B_M(\alpha)$ naively from the formula. The time taken for this would be dominated by the powerings. For $\alpha = a/b$ some rational number, the total time would be

$$O(M^4(\lg M + \lg a + \lg b)(\lg a + \lg b)).$$

However we can do better than this, using a cross between Horner's method of evaluating polynomials and an algorithm used by Brent to calculate Bernoulli numbers, as discussed in [3]. This method gives a total time of

$$O(M^3(\lg M + \lg a + \lg b)^2).$$

Using either of these algorithms to compute $\zeta_D(1-2m)$, $2 \le 2m \le M$, is then relatively straightforward. The slower version has time

$$O(M^4 D(\lg M + \lg D) \lg D),$$

while the faster one runs in time

$$O(M^3 D(\lg D + \lg M)^2).$$

3 Second formula

Siegel's second formula is, as I said, derived from the theory of modular forms. It says that

$$\zeta_D(1-2m) = 4 \sum_{l=1}^{r} b_l(4m) s_l^{k_0}(2m), \qquad r = \lfloor m/3 \rfloor + 1 \tag{2}$$

where $s_l^{k_0}$ is a sum over norms of ideals in the ring of integers of k_0 which can also be expressed in terms of a purely arithmetic function $e_r(n)$, as follows:

$$s_l^{k_0}(2m) = \sum_{j|l} \chi_D(j) j^{2m-1} e_{2m-1}((l/j)^2 D)$$

and

$$e_r(n) = \sum_{\substack{x^2 \equiv n \pmod 4 \\ |x| \le \sqrt{n}}} \sigma_r\left(\frac{n-x^2}{4}\right)$$

where σ_r is the usual sum-of-powers function. The coefficients b_l are most easily expressed as the coefficients of a certain power series, and can be computed as needed, over a common denominator, without adding to the asymptotic running time. It is not hard to prove that in this form $b_i(4m)$ is of size $O(m)$. The running time for calculating the function $e_r(n)$ is complicated by the need for factoring; we use an estimate based on the elliptic curve factoring

method to get an expected running time involving the function $L(x) = e^{\sqrt{\log x \log\log x}}$. Given this, we get an expected running time of

$$O(\sqrt{n}\, L(n)^{1+o(1)} + r^2\sqrt{n}\lg^2 n).$$

If we now applied (2) as written to compute all $\zeta_D(1-2m)$, $2 \le 2m \le M$, we would get a running time of

$$O(M^3\sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)} \lg M + M^5\sqrt{D}\lg M(\lg M + \lg D)^2).$$

However, it is more efficient to rearrange the terms of the formula as follows:

$$\begin{aligned}
\zeta_D(1-2m) &= 4\sum_{l=1}^{r} b_l(4m) s_l^{k_0}(2m) \\
&= 4\sum_{l=1}^{r} b_l(4m) \sum_{j|l} \chi_D(j) j^{2m-1} e_{2m-1}((l/j)^2 D) \\
&= 4\sum_{k=1}^{r} \left(\sum_{j=1}^{\lfloor r/k \rfloor} \chi_D(j) j^{2m-1} b_{jk}(4m) \right) e_{2m-1}(k^2 D) \qquad (3)
\end{aligned}$$

This rearrangement of the formula requires fewer calls to compute e_r by a factor of $\lg m$. Using this version of the formula, the time necessary to compute all $\zeta_D(1-2m)$, $2 \le 2m \le M$, is

$$O(M^3\sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)} + M^5\sqrt{D}(\lg M + \lg D)^2).$$

This is much worse than the best algorithm based on (1) in terms of M, but it is better in terms of D.

It should be noted that the asymptotic running time of this algorithm is greatly improved by using Schönhage-Strassen fast multiplication, in which case the second term becomes smaller than the first and the running time becomes

$$O(M^3\sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)})$$

This is still worse than using (1) in terms of M, but only by a subexponential factor.

It should also be noted that (2) and (3) also present opportunities for time savings when computing zeta-values for multiple D in the same range of M. The author has not yet had a chance to analyze these savings precisely.

4 Summary

Here is a table of the various algorithms, for comparison. We present the asymptotic order of the running time using naive multiplication and Schönhage-Strassen fast multiplication. We also show a model where multiplication takes constant time regardless of the size of the factors; evidence indicates that this may be more realistic in practice for the numbers that we can currently deal with.

The factor of $\lg M$ in the times for algorithms based on (2) has been included to emphasize that these algorithms are slower than those based on (3), even though the factor of $\lg M$ could be absorbed into that of $L(M)^{\sqrt{2}+o(1)}$.

Equation used	Multiplication	Time order
(1)	naive	$M^4 D(\lg M + \lg D) \lg D$
(1)	fast	$M^3 D(\lg D \lg(M \lg D) \lg \lg(M \lg D) + \lg^2 M \lg \lg M)$
(1)	constant	$M^2 D \lg M + M D \lg^2 D$
(1) from [3]	naive	$M^3 D(\lg D + \lg M)^2$
(1) from [3]	fast	$M^3 D(\lg D + \lg M) \lg(\lg M + \lg D) \lg \lg(\lg M + \lg D)$
(1) from [3]	constant	$M^2 D + M D \lg^2 D$
(2)	naive	$M^3 \sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)} \lg M + M^5 \sqrt{D} \lg M (\lg M + \lg D)^2$
(2)	fast	$M^3 \sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)} \lg M$
(2)	constant	$M^3 \sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)} \lg M$
(3)	naive	$M^3 \sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)} + M^5 \sqrt{D} (\lg M + \lg D)^2$
(3)	fast	$M^3 \sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)}$
(3)	constant	$M^3 \sqrt{D}\, L(M)^{\sqrt{2}+o(1)}\, L(D)^{1+o(1)}$

References

[1] Johannes Buchmann and H. C. Williams. Quadratic fields and cryptography. In *Number Theory and Cryptography (Sydney, 1989)*, pages 9–25. Cambridge University Press, 1990.

[2] Henri Cohen. Variations sur un thème de Siegel et Hecke. *Acta Arithmetica*, 30:63–93, 1976.

[3] Joshua Holden. Irregularity of prime numbers over real quadratic fields. In *Algorithmic number theory: third international symposium; proceedings*, number 1423 in Springer Lecture Notes in Computer Science, pages 464–462. Springer-Verlag, 1998.

[4] Joshua Holden. *On the Fontaine-Mazur Conjecture for Number Fields and an Analogue for Function Fields*. PhD thesis, Brown University, 1998.

[5] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag, second edition, 1994.

[6] Carl Ludwig Siegel. Bernoullische Polynome und quadratische Zahlkörper. *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-physikalische Klasse*, 2:7–38, 1968.

[7] 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.