MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 194
APRIL 1991, PAGES 851-858

CYCLOTOMIC INVARIANTS FOR PRIMES BETWEEN 125000 AND 150000

R. ERNVALL AND T. METSÄNKYLÄ

ABSTRACT. Computations by Iwasawa and Sims, by Johnson, and by Wagstaff have determined certain important cyclotomic invariants for all primes up to 125000. We extended their results to 150000, basing our work on a recently computed list of irregular primes and using a new method.

1. INTRODUCTION

Since 1978, when Wagstaff [10] published the results of his extensive computations, one knows the values of certain important cyclotomic invariants, notably the Iwasawa invariants λ_p and ν_p, for all primes $p < 125000$. The first, and hardest, step in these computations is the determination of irregular primes. Recently Tanner and Wagstaff [9], returning to this theme, extended the list of irregular primes to 150000 and obtained partial results about the cyclotomic invariants.

The present note is a report on our computations completing the determination of these invariants up to $p < 150000$. Since at the primes of this size the earlier methods of computation no longer are efficient, it was necessary to develop new techniques. A description of our method, based on a suitable combination of congruences for Bernoulli numbers, is included.

2. THE RESULTS

Let p be an odd prime. For $n \geq 0$, let K_n denote the cyclotomic field of p^{n+1}th roots of 1, and let h_n and A_n be the class number and p-class group, respectively, of K_n. As usual, write

$$h_n = h_n^+ h_n^- , \qquad A_n = A_n^+ \oplus A_n^- ,$$

where h_n^+ and A_n^+ are the class number and p-class group, respectively, of the field $K_n \cap \mathbb{R}$.

It is well known that the triviality of A_n, for all $n \geq 0$, is equivalent to the triviality of A_0. If these groups are nontrivial, p is called *irregular*. This is the

Received March 23, 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R18, 11B68, 11R23, 11R29, 11Y40.

Key words and phrases. Cyclotomic fields, Bernoulli numbers, irregular primes, Iwasawa invariants, class numbers, computation.

case if and only if p divides $B_2B_4\cdots B_{p-3}$, where B_t are Bernoulli numbers (in the even suffix notation).

If p divides B_t with $t\in\{2, 4, \dots, p-3\}$, then (p, t) is called an *irregular pair.* We let r_p denote the number of such pairs, *the index of irregularity* of p.

Expressed in a brief form, the results of our computations read as follows: for every p between 125000 and 150000,

$$A_n^- \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^{r_p} \qquad (n=0, 1, \dots), \tag{1}$$

$$\operatorname{ord}_p(h_0^-) = \operatorname{ord}_p(B_2B_4\cdots B_{p-3}), \tag{2}$$

where $\operatorname{ord}_p(a)$ stands for the exponent of p in the canonical decomposition of a.

Actually, we know that A_n^+ is trivial for these p, so that (1) and (2) remain true if A_n^- and h_0^- are replaced by A_n and h_0, respectively. The triviality of A_n^+ was proved by Tanner and Wagstaff [9] in conjunction with the verification of Fermat's Last Theorem for prime exponents $p < 150000$; see, e.g., Corollary 8.19 in Washington's book [11].

The formulas (1) and (2), together with the result $A_n^+ = 1$, had been verified by Wagstaff [10] for $p < 125000$, and earlier by Johnson [2], [3], [4] in shorter ranges. Computations for verifying (1) were initiated by Iwasawa and Sims [1].

By Iwasawa's general result,

$$\operatorname{ord}_p(h_n) = \lambda_p n + \nu_p, \quad \operatorname{ord}_p(h_n^-) = \lambda_p^- n + \nu_p^-$$

for all n large enough, say $n \ge n_p$, where λ_p, λ_p^-, ν_p, ν_p^- are integers (λ_p, λ_p^- nonnegative) independent of n. Notice that the μ-invariant vanishes by the theorem of Ferrero and Washington. Given that the groups A_n^+ are trivial, (1) is equivalent to

$$\lambda_p = \lambda_p^- = \nu_p = \nu_p^- = r_p, \quad \text{minimal } n_p = 0$$

(for this and the following facts, we refer to [11], especially §10.3).

We may decompose $\lambda_p^- = \lambda^{(2)} + \lambda^{(4)} + \cdots + \lambda^{(p-3)}$, where each $\lambda^{(t)}$ is the λ-invariant associated with the p-adic L-function $L_p(s, \omega^t)$, ω being the Teichmüller character mod p. Since $\lambda^{(t)}$ is positive if and only if (p, t) is an irregular pair, the equation $\lambda_p^- = r_p$ is equivalent to

$$\lambda^{(t)} = 1 \quad \text{for each irregular pair } (p, t).$$

To establish the results (1) and (2), it is enough to verify—and this is what we did—that none of the following three congruences hold for any irregular pair (p, t):

$$\frac{B_t}{t} \equiv \frac{B_{t+p-1}}{t+p-1} \pmod{p^2}, \tag{i}$$

$$B_1(\omega^{t-1}) \equiv 0 \pmod{p^2}, \tag{ii}$$

(iii) $$B_t \equiv 0 \pmod{p^2}.$$

Here, $B_1(\omega^{t-1}) = (1/p)\sum_{a=1}^{p-1}\omega^{t-1}(a)a$ is the first generalized Bernoulli number attached to ω^{t-1}, in fact, $B_1(\omega^{t-1}) = -L_p(0, \omega^t)$. We point out that (ii) can be converted into a simple congruence mod p^2 between B_t and B_{t+p-1}; see Propositions 6 and 2 in §4.

More precisely, the failures of (i) and (ii), for all t such that the pair (p, t) is irregular, imply that $\lambda_p^- = r_p$ and $\nu_p^- = r_p$, respectively [11, p. 201], and the failure of (iii) then yields the equation (2). Observe that the congruences in (i)–(iii) hold modulo p.

By Washington's heuristic arguments [6, p. 20] one expects that (1) and (2) remain true for all primes up to a very high limit. They should not be generally true, however.

3. The computations

If p is not too big, one can disprove (i)–(iii) by a fairly straightforward method involving basically the calculation of B_t and B_{t+p-1} mod p^2. In fact, such a method was employed by Johnson and Wagstaff for $p < 125000$. There is also another method presented in [1]; it is more sophisticated but still relies quite heavily on computations mod p^2.

For p close to 150000 we have to find a method which keeps computations mod p^2 to a minimum. We point out that in order that c^2 fit in a computer word, c should be below 2^{16}, which for c around $p/2$ leads to the bound $p < 1.3 \cdot 10^5$.

Write $p = 2m + 1$. For an integer a prime to p, let q_a denote the Fermat quotient of a, i.e.,

$$q_a \equiv \frac{a^{p-1} - 1}{p} \pmod{p}, \qquad 0 \le q_a < p.$$

Putting

$$S_1 = \sum_{a=1}^{m} a^{t-1} q_a, \qquad S_2 = \sum_{a=1}^{m} a^t q_a^2,$$

$$S_3 = \sum_{a=1}^{m} a^{t-1}, \qquad S_4 = \sum_{0<a<p/3} a^{t-1}, \qquad S_5 = \sum_{p/3<a<p/2} a^{t-2},$$

we formulate the following criteria, where (p, t) is assumed to be an irregular pair. The proofs will be presented in §4.

Criterion 1. *If* $S_1 \not\equiv 0 \pmod{p}$, *then* (i) *does not hold. If* $S_1 \equiv 0 \pmod{p}$, *then either* $2^t \equiv 1 \pmod{p}$ *or* (i) *holds.*

Criterion 2. *If* $S_2 \not\equiv 0 \pmod{p}$, *then* (i) *does not hold. If* $S_2 \equiv 0 \pmod{p}$, *then either* $2^{t-1} \equiv 1 \pmod{p}$ *or* (i) *holds.*

Criterion 3. *If* $2^t \not\equiv 1 \pmod{p}$, *then* (ii) *is equivalent to*

$$S_3 \equiv (1-t)pS_1 \pmod{p^2}$$

and (iii) *is equivalent to*

$$S_3 \equiv 0 \pmod{p^2}.$$

Criterion 4. *If* $2^{t-1} \not\equiv 1$ *and* $3^t \not\equiv 1 \pmod{p}$, *then* (ii) *is equivalent to*

$$3S_4 - (1-t)pS_5 \equiv -\left(\frac{2}{3}\right)^{t-2} \frac{3^t-1}{2^{t-1}-1}(1-t)pS_2 \pmod{p^2}.$$

If $3^t \not\equiv 1 \pmod{p}$, *then* (iii) *is equivalent to*

$$3S_4 - (1-t)pS_5 \equiv 0 \pmod{p^2}.$$

Criteria 1 and 2 always suffice to decide about the validity of (i), because the congruences $2^t \equiv 1$ and $2^{t-1} \equiv 1 \pmod{p}$ never hold simultaneously. Similarly, Criteria 3 and 4 are sufficient for (ii) and (iii) except when $2^t \equiv 3^t \equiv 1 \pmod{p}$. For the case of the last instance one can derive analogous criteria that work under the assumption $b^t \not\equiv 1 \pmod{p}$ for some other b prime to p (see §4).

There are 1079 irregular pairs with $125000 < p < 150000$. It turned out that all these pairs satisfy $2^{t-1} \not\equiv 1$ and $3^t \not\equiv 1 \pmod{p}$, so that one can disprove (i)–(iii) merely by using Criteria 2 and 4. The incongruence $2^t \not\equiv 1 \pmod{p}$ holds everywhere except at the pair $(130811, 52324)$. Thus, excluding this single pair, Criteria 1 and 3 apply to check the results.

In reality, we started with Criterion 1 without knowing of the above exception, and then went on with 2, 4, and 3 in this order.

We now describe the calculation of the sums $S_1, \dots, S_5$.

To obtain S_1 and S_2 (mod p, as they are needed), one has to find q_a which actually involves a computation mod p^2. We calculated the values of q_a $(1 \le a \le m)$ in cycles, passing from q_a to q_{2a} or, if $2a > m$, to q_{p-2a}. These are related to q_a by a simple congruence mod p. Hence, only the first q_a in each cycle actually requires computation mod p^2. In many cases (e.g., if 2 is a primitive root mod p or if m is a prime) there is but one cycle, and in our range, less than every hundreth irregular prime had more than 10 cycles. A similar method was employed by Johnson [2, pp. 391, 396] in another connection.

Rather than to q_a only, we in fact applied this cycle method to the entire terms of S_1 and S_2. The same cycles were then used in the calculation of the remaining sums. When calculating S_3 and S_4 this way, one has to perform some computation mod p^2 inside the cycles, too, but the method still appears to be quite efficient. The computation of S_5 did not provide any serious problem, because this sum was needed mod p only.

The first program run by us computed, except for S_1, two additional sums mod p, namely S_3 and

$$S_6 = \sum_{a=1}^{m} a^t q_a.$$

This was a check both for the correctness of our summing method and for the irregularity of the given pairs (p, t). Indeed, for an irregular pair, the latter sums vanish mod p (see Proposition 3 below). There were also some further checks to assure that the Fermat quotients were correctly calculated. The running time for a single irregular pair was generally 12 to 15 sec.

The programs computing S_3 and S_4 mod p^2 took somewhat more time to execute: one irregular pair was settled in 25 to 45 sec. One simple check was provided by the congruences $S_3 \equiv S_4 \equiv 0 \pmod{p}$.

All programs were written in the language C and run on a VAX 6340 computer. After learning that the use of inline optimization (in the C-compiler version 3.0) may produce erroneous code, we ran all the programs once more without this option.

4. Proof of the criteria

The four criteria of the previous section will be proved by transforming the Bernoulli number congruences (i)–(iii) into congruences between the sums involved. The procedure is based on the following two congruences.

Proposition 1. *Let t be a positive even integer prime to p and incongruent to 0 and 2 $\pmod{p-1}$. Then*

(a) $$\frac{B_t}{t} \equiv -\sum_{a=1}^{p-1} a^{t-1} v_a - \frac{t-1}{2} p \sum_{a=1}^{p-1} a^{t-2} v_a^2 \pmod{p^2},$$

where v_a is the p-adic integer defined by $\omega(a) = a + v_a p$; furthermore,

(b) $$(b^t - 1)\frac{B_t}{t} \equiv \sum_{a=1}^{p-1} (ba)^{t-1} \left[\frac{ba}{p}\right] - \frac{t-1}{2} p \sum_{a=1}^{p-1} (ba)^{t-2} \left[\frac{ba}{p}\right]^2 \pmod{p^2},$$

where b is any rational integer with $2 \le b \le p-1$ and $[x]$ denotes the largest integer $\le x$.

Proof. The latter congruence, a sharpening of the Voronoi congruence, is due to Johnson [5, p. 261]; for a different proof see [8, p. 117].

The former congruence can be verified by an argument similar to one in [5, p. 253]: substitute $\omega(a) = a + v_a p$ in the equation $\sum_{a=1}^{p-1} \omega(a)^t = 0$, expand the tth power, and reduce mod p^3, noting that $\sum_{a=1}^{p-1} a^t \equiv pB_t \pmod{p^3}$. This last congruence is proved, e.g., in [5, p. 261]. □

From now on we assume that

$$t \in \{2, 4, \dots, p-3\}.$$

Thus, in particular, $p > 3$.

Proposition 2. *Excluding the case* $t = 2$, *we have*

$$\frac{B_{t+p-1}}{t+p-1} - \frac{B_t}{t} \equiv -\frac{1}{2}p\sum_{a=1}^{p-1} a^t q_a^2 \pmod{p^2}.$$

Proof. This follows from Proposition 1(a). Observe that $a^{p-1} - 1 \equiv pq_a \pmod{p^2}$, $v_a \equiv aq_a \pmod{p}$. □

The next result is an easy consequence of known results. Here we prefer to deduce it from Proposition 1(a), since the same idea also applies to Proposition 4 below.

Proposition 3. *The pair* (p, t) *is irregular if and only if* $S_3 \equiv S_6 \equiv 0 \pmod{p}$.

Proof. If $t = 2$, both statements are false. Assume that $t \neq 2$. By Proposition 1(a), (p, t) is irregular if and only if $\sum_{a=1}^{p-1} a^t q_a \equiv 0 \pmod{p}$. Using the congruences

$$q_{p-a} \equiv q_a + a^{-1}, \quad q_{p-2a} \equiv q_{2a} + (2a)^{-1}, \quad q_{2a} \equiv q_2 + q_a \pmod{p}$$

and noting that $\sum_{a=1}^{m} a^t \equiv 0 \pmod{p}$, we reformulate the last sum in two ways:

$$\sum_{a=1}^{p-1} a^t q_a \equiv 2\sum_{a=1}^{m} a^t q_a + \sum_{a=1}^{m} a^{t-1} \pmod{p},$$

$$\sum_{a=1}^{p-1} a^t q_a \equiv 2^{t+1}\sum_{a=1}^{m} a^t q_a + 2^{t-1}\sum_{a=1}^{m} a^{t-1} \pmod{p}.$$

This gives us the claim. □

As mentioned in §3, we used this proposition to check that the pairs (p, t) in the table by Tanner and Wagstaff are irregular.

Proposition 4. *If* (p, t) *is an irregular pair, then*

(a) $$(1 - 2^t)\sum_{a=1}^{p-1} a^t q_a^2 \equiv -2^t S_1 \pmod{p},$$

(b) $$(1 - 2^{t-1})\sum_{a=1}^{p-1} a^t q_a^2 \equiv 2^t S_2 \pmod{p}.$$

Proof. Reformulate the sum $\sum_{a=1}^{p-1} a^t q_a^2$ by the same principles as before. In view of $S_3 \equiv S_6 \equiv 0$ and $\sum_{a=1}^{m} a^{t-2} \equiv 0 \pmod{p}$ it follows that

$$\sum_{a=1}^{p-1} a^t q_a^2 \equiv 2S_2 + 2S_1 \pmod{p},$$

$$\sum_{a=1}^{p-1} a^t q_a^2 \equiv 2^{t+1} S_2 + 2^t S_1 \pmod{p}.$$

This pair of congruences yields the asserted congruences. □

By combining Propositions 2 and 4 we obtain the following formulas for

$$\Delta = \frac{B_{t+p-1}}{t+p-1} - \frac{B_t}{t},$$

provided (p, t) is an irregular pair:

$$(1-2^t)\frac{1}{p}\Delta \equiv 2^{t-1}S_1, \qquad (1-2^{t-1})\frac{1}{p}\Delta \equiv -2^{t-1}S_2 \pmod p.$$

This proves Criteria 1 and 2.

Remark. The former of these congruences also follows from a result of E. Lehmer [7, p. 355]. She traces the congruence back to Mirimanoff.

Proposition 5. *Excluding the case* $t = 2$, *we have*

(a) $$(2^t - 1)\frac{B_t}{t} \equiv -2^{t-1}S_3 \pmod{p^2},$$

(b) $$(3^t - 1)\frac{B_t}{t} \equiv -2\cdot 3^{t-1}S_4 + 2\cdot 3^{t-2}(1-t)pS_5 \pmod{p^2}.$$

Proof. We look at Proposition 1(b) with $b = 2$ and 3, respectively. For $b = 2$ note that $\sum_{a=1}^{m} a^{t-2} \equiv \sum_{a=m+1}^{p-1} a^{t-2} \equiv 0 \pmod p$ and so, in particular,

$$\sum_{a=m+1}^{p-1} a^{t-1} = \sum_{a=1}^{m}(p-a)^{t-1} \equiv -S_3 \pmod{p^2}.$$

For $b = 3$ somewhat more lengthy calculations yield

$$\sum_{a=1}^{p-1} a^{t-1}\left[\frac{3a}{p}\right] \equiv -2\sum_{0<a<p/3} a^{t-1} - (t-1)p\sum_{p/3<a<p/2} a^{t-2} \pmod{p^2},$$

$$\sum_{a=1}^{p-1} a^{t-2}\left[\frac{3a}{p}\right]^2 \equiv -2\sum_{p/3<a<p/2} a^{t-2} \pmod p.$$

Substitute the right-hand sides in the congruence of Proposition 1(b) and simplify. □

Proposition 5 provides us the latter parts of Criteria 3 and 4.

Proposition 6. *Excluding the case* $t = 2$, *we have*

$$B_1(\omega^{t-1}) \equiv \frac{B_t}{t} - \frac{t-1}{2}p\sum_{a=1}^{p-1} a^t q_a^2 \pmod{p^2}.$$

Proof. We may write

$$B_1(\omega^{t-1}) = \frac{1}{p}\sum_{a=1}^{p-1}(a + v_a p)^{t-1}a.$$

Since $\frac{1}{p}\sum_{a=1}^{p-1} a^t \equiv B_t \pmod{p^2}$, this implies

$$B_1(\omega^{t-1}) \equiv B_t + (t-1)\sum_{a=1}^{p-1} a^{t-1}v_a + \frac{(t-1)(t-2)}{2}p\sum_{a=1}^{p-1} a^{t-2}v_a^2 \pmod{p^2}.$$

Multiply the congruence in Proposition 1(a) by $t-1$ and add to this congruence. □

Proposition 7. *Let (p, t) be an irregular pair. Then*

$$\frac{2^t-1}{2^{t-1}}B_1(\omega^{t-1}) \equiv -S_3 + (1-t)pS_1 \pmod{p^2}$$

and, provided that $2^{t-1} \not\equiv 1 \pmod{p}$,

$$\frac{3^t-1}{2\cdot 3^{t-2}}B_1(\omega^{t-1}) \equiv -3S_4 + (1-t)pS_5 - \left(\frac{2}{3}\right)^{t-2}\frac{3^t-1}{2^{t-1}-1}(1-t)pS_2 \pmod{p^2}.$$

Proof. These two results are verified by multiplying the congruence of Proposition 6 by $2^t - 1$ or $3^t - 1$, respectively, and then using Propositions 5(a) and 4(a), or 5(b) and 4(b), respectively. □

This completes the proof of Criteria 3 and 4.

Acknowledgment

Professor S. S. Wagstaff, Jr. kindly made available to us the unpublished table of irregular primes computed by himself and J. W. Tanner.

Bibliography

1. K. Iwasawa and C. Sims, *Computation of invariants in the theory of cyclotomic fields*, J. Math. Soc. Japan **18** (1966), 86–96.
2. W. Johnson, *On the vanishing of the Iwasawa invariant μ_p for $p < 8000$*, Math. Comp. **27** (1973), 387–396.
3. ——, *Irregular prime divisors of the Bernoulli numbers*, Math. Comp. **28** (1974), 653–657.
4. ——, *Irregular primes and cyclotomic invariants*, Math. Comp. **29** (1975), 113–120.
5. ——, *p-adic proofs of congruences for the Bernoulli numbers*, J. Number Theory **7** (1975), 251–265.
6. S. Lang, *Cyclotomic Fields II*, Springer-Verlag, Berlin and New York, 1980.
7. E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **(2) 39** (1938), 350–360.
8. T. Metsänkylä, *The Voronoi congruence for Bernoulli numbers*, The Very Knowledge of Coding, Univ. of Turku, Turku, 1987, pp. 112–119.
9. J. W. Tanner and S. S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*, Math. Comp. **48** (1987), 341–350.
10. S. S. Wagstaff, Jr., *The irregular primes to* 125000, Math. Comp. **32** (1978), 583–591.
11. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, Berlin and New York, 1982.

Department of Mathematics, University of Turku, SF-20500 Turku, Finland
E-mail address: rernvall@firien.bitnet and rernvall@kontu.utu.fi