MATHEMATICS OF COMPUTATION
VOLUME 59, NUMBER 199
JULY 1992, PAGES 249–250

CYCLOTOMIC INVARIANTS FOR PRIMES TO ONE MILLION

R. ERNVALL AND T. METSÄNKYLÄ

ABSTRACT. Our recent computation of cyclotomic invariants for primes between 125000 and 150000 was extended to one million. No new phenomena appear.

This note is a sequel to our recent report [2] on the computation of certain cyclotomic invariants for primes p between 125000 and 150000. That work was based on the table of irregular primes supplied by Tanner and Wagstaff (see [4]). Meanwhile, the extension of this table to $p < 10^6$ by Buhler, Crandall, and Sompolski [1] enabled us to go on with our computations, and we indeed ran the main part of our earlier program in this new range.

The result is that all the previous statements remain valid. To make this precise, we first introduce the necessary notation; for a more thorough discussion of the notions involved, the interested reader is referred to [2] and [5]. For an odd prime p and for $n \geq 0$, let h_n and A_n denote the class number and p-class group, respectively, of the cyclotomic field K_n generated by the p^{n+1}th roots of 1, and let h_n^- and A_n^- stand for their minus-parts. Denote by r_p the index of irregularity of p, that is, the number of p-divisible Bernoulli numbers B_t with $t \in I = \{2, 4, \ldots, p-3\}$.

Our computations now allow us to state that

$$(1)\quad A_n^- \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^{r_p} \qquad (n = 0, 1, \ldots), \qquad \operatorname{ord}_p(h_0^-) = \operatorname{ord}_p(B_2 B_4 \cdots B_{p-3})$$

for all $p < 10^6$, where $\operatorname{ord}_p(a)$ denotes the exponent of p in the canonical decomposition of a.

Note that the computations of [1], together with earlier computations by Wagstaff et al., imply that $A_n^- \simeq A_n$ for these p. From this and (1) it follows, among other things, that the λ-invariant of the $\mathbb{Z}_p$-extension $\bigcup_{n=0}^{\infty} K_n$ over K_0 equals r_p in this range.

It is worth pointing out that the results in [1] also imply the truth of Fermat's Last Theorem for all prime exponents up to one million.

We now describe briefly the contents of our computations. Let (p, t) be an irregular pair, i.e., a pair with $t \in I$ and $p \mid B_t$. As in [2], put

$$S_1 = \sum_{0<a<p/2} a^{t-1} q_a, \qquad S_2 = \sum_{0<a<p/2} a^t q_a^2,$$

Received by the editor April 15, 1991.
1991 *Mathematics Subject Classification.* Primary 11R18, 11B68, 11R23, 11R29, 11Y40.
Key words and phrases. Cyclotomic fields, Bernoulli numbers, irregular primes, Iwasawa invariants, class numbers, computation.

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

where q_a, the Fermat quotient of a, is defined by the conditions $0 \le q_a < p$, $q_a \equiv (a^{p-1} - 1)/p \pmod{p}$. Our Criteria 1–4 proved in [2] imply that (1) holds true provided each irregular pair (p, t) satisfies one of the following two conditions:

(a) both $2^t - 1$ and S_1 are nondivisible by p and both S_3 and $S_3 - (1-t)pS_1$ are nondivisible by p^2,

(b) the prime p divides $2^t - 1$ but both $3^t - 1$ and S_2 are nondivisible by p, and both $3S_4 - (1-t)pS_5$ and

$$3S_4 - (1-t)pS_5 + \left(\frac{2}{3}\right)^{t-2} \frac{3^t - 1}{2^{t-1} - 1}(1-t)pS_2$$

are nondivisible by p^2.

For the connections of (a) and (b) with the divisibility of Bernoulli numbers, see [2].

Checking each irregular pair (p, t) with $1.5 \cdot 10^5 < p < 10^6$ for the condition (a) we found that this condition is satisfied by all pairs except (599479, 359568). This pair was checked to satisfy (b).

When calculating S_3 and $S_4 \pmod{p^2}$ the program verified that these sums vanish modulo p. This provides a check for the irregularity of the given pairs (p, t); see Proposition 5 in [2].

As before, the computer we used was a VAX 6340. Because of the extensiveness of the data material, new efforts were made to minimize the running time. While the actual computer program remained unchanged, we slightly rearranged the order of some calculations and enlarged the working set in the virtual machine, reaching in this way a time of about $p/10^4$ seconds for a single irregular pair (p, t).

R. Sompolski informed us that he has established (1) for $p < 400000$ by a computation based on an independent method (see [3]).

Acknowledgment

We thank Professor Joe Buhler and his coauthors for permitting us to use their table.

Bibliography

1. J. P. Buhler, R. E. Crandall, and R. Sompolski, *Irregular primes to one million*, Math. Comp., (to appear).
2. R. Ernvall and T. Metsänkylä, *Cyclotomic invariants for primes between* 125000 *and* 150000, Math. Comp. **56** (1991), 851–858.
3. R. Sompolski, Thesis, Univ. of Illinois at Chicago, 1991.
4. J. W. Tanner and S. S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*, Math. Comp. **48** (1987), 341–350.
5. 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@kontu.utu.fi