J. Math. Soc. Japan
Vol. 18, No. 1, 1966

Computation of invariants in the theory of cyclotomic fields

By Kenkichi IWASAWA* and Charles C. SIMS

(Received July 26, 1965)

1. Let a prime number p be fixed, and let F_n, $n \geqq 0$, denote the cyclotomic field of p^{n+1}-th roots of unity over the rational field $\boldsymbol{Q}$. Let $p^{c(n)}$ be the highest power of p dividing the class number h_n of F_n. Then there exist integers λ_p, μ_p, and ν_p (λ_p, $\mu_p \geqq 0$), depending only upon p, such that

$$c(n) = \lambda_p n + \mu_p p^n + \nu_p ,$$

for every sufficiently large integer n[1]. In the present paper, we shall determine, by the help of a computer, the coefficients λ_p, μ_p, and ν_p in the above formula for all prime numbers $p \leqq 4001$. We shall see in particular that $\mu_p = 0$ for every $p \leqq 4001$. Let S_n denote the Sylow p-subgroup of the ideal class group of F_n. For the above primes, we shall determine not only the order $p^{c(n)}$ of S_n but also the structure of the abelian group S_n for every $n \geqq 0$.

Let $p=2$. Then we know by Weber's theorem that $c(n)=0$, $S_n=1$ for any $n \geqq 0$ so that $\lambda_2 = \mu_2 = \nu_2 = 0$. Therefore, we shall assume throughout the following that p is an odd prime, $p > 2$.

2. Let $\boldsymbol{Q}_p$ and $\boldsymbol{Z}_p$ denote the field of p-adic numbers and the ring of p-adic integers, respectively. Let F be the union of all fields F_n, $n \geqq 0$. Then F is an abelian extension of $\boldsymbol{Q}$, and we denote the Galois group of $F/\boldsymbol{Q}$ by G. For each p-adic unit u in $\boldsymbol{Q}_p$, there is a unique automorphism σ_u of F such that $\sigma_u(\zeta) = \zeta^u$ for any root of unity ζ in F with order a power of p. The mapping $u \to \sigma_u$ then defines a topological isomorphism of the group of p-adic units in $\boldsymbol{Q}_p$ onto the compact abelian group G. Let Γ and Δ denote the subgroups of G corresponding to the group of 1-units in $\boldsymbol{Q}_p$ and the group $\boldsymbol{V}$ of all $(p-1)$-st roots of unity in $\boldsymbol{Q}_p$, respectively. Then we have

$$G = \Gamma \times \Delta \ ;$$

---

* The work of this author was supported in part by the National Science Foundation grant GP-2496.

1) For the results on cyclotomic fields used in the present paper, see K. Iwasawa, On the theory of cyclotomic fields, Ann. of Math., **70** (1959), 530-561; K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, **16** (1964), 42-82.

Γ is the Galois group of F/F_0, and Δ is a cyclic group of order $p-1$, canonically isomorphic to the Galois group of $F_0/\boldsymbol{Q}$.

For any $m \geqq n \geqq 0$, the injective homomorphism of the ideal group of F_n into that of F_m induces a natural homomorphism $S_n \to S_m$. Let S be the direct limit of S_n, $n \geqq 0$, relative to these homomorphisms. The Galois group G acts on S in the obvious manner. For each integer i, $0 \leqq i < p-1$, let ${}^iS$ denote the subgroup of all elements s in S such that $\sigma_v(s) = s^{v^i}$ for every v in $\boldsymbol{V}$. Then S is the direct product of the G-subgroups ${}^iS$:

$$S = \prod_{i=0}^{p-2} {}^iS .$$

We have a similar decomposition for each S_n, $n \geqq 0$, and ${}^iS$ is the direct limit of the subgroups ${}^iS_n$, $n \geqq 0$.

3. Let Λ denote the ring of formal power series in an indeterminate T with coefficients in $\boldsymbol{Z}_p$: $\Lambda = \boldsymbol{Z}_p[[T]]$. Then there is an injective homomorphism of Γ into the multiplicative group of Λ such that $\sigma_{1+p} \to 1+T$. Therefore, if M is any Λ-module, we can make it into a Γ-module so that $\sigma_{1+p}(x) = (1+T)x$ for every x in M.

For any a in $\boldsymbol{Q}_p$, there exist a rational integer b and a power of p, p^m $(m \geqq 0)$, such that $p^m a \equiv b \bmod p^m$, $0 \leqq b < p^m$. The rational number b/p^m is then uniquely determined by a so that we denote it by $\langle a \rangle$.

For each odd integer i, $0 \leqq i < p-1$, we shall next define a power series ${}^ig(T)$ in Λ. First, we put ${}^{p-2}g(T) = 1$. Let $i \neq p-2$. For each $n \geqq 0$, let

$${}^ig_n(T) = \sum_m \sum_v \langle v(1+p)^m/p^{n+1} \rangle v^i (1+T)^m ,$$

where $0 \leqq m < p^n$, $v \in \boldsymbol{V}$. Then ${}^ig_n(T)$ is a polynomial in T with coefficients in $\boldsymbol{Z}_p$, and when n tends to infinity, ${}^ig_n(T)$ converges, on each coefficient of T^m, $m \geqq 0$, to a power series in Λ, which we denote by ${}^ig(T)$:

$${}^ig(T) = \lim_{n \to \infty} {}^ig_n(T) .$$

We see easily that

$$(1) \qquad {}^ig(T) \equiv {}^ig_n(T) \quad \bmod (1-(1+T)^{p^n})\Lambda , \qquad n \geqq 0 .$$

For each odd i, there exist, by Weierstrass' preparation theorem, an integer $e_i \geqq 0$, a unit ${}^iu(T)$ of the ring Λ, and a polynomial ${}^im(T)$ of the form

$${}^im(T) = {}^ia_0 + \cdots + {}^ia_{d_i-1}T^{d_i-1} + T^{d_i} , \qquad {}^ia_k \in p\boldsymbol{Z}_p ,$$

such that

$${}^ig(T) = p^{e_i}\, {}^iu(T)\, {}^im(T) .$$

Now, let

$${}^iM = \Lambda / {}^ig(T)\Lambda , \qquad 0 \leqq i < p-1 , \qquad (i, 2) = 1 .$$

As noted in the above, we may consider ${}^iM$ as Γ-modules. These Γ-modules are fundamental in the theory of cyclotomic fields, and we shall next consider some special cases in which the structure of ${}^iM$ can be easily determined.

4. For each odd index i, let

$${}^ig(T)={}^i\alpha+{}^i\beta T+{}^i\gamma T^2+\cdots,$$

with ${}^i\alpha$, ${}^i\beta$, ${}^i\gamma$, etc. in $\boldsymbol{Z}_p$. Then it is clear that ${}^iM=0$ if and only if ${}^i\alpha$ is a p-adic unit, namely, if and only if $d_i=e_i=0$. Since ${}^{p-2}g(T)=1$, we immediately have ${}^{p-2}M=0$.

For any integer a, $1\leqq a\leqq p-1$, let v_a denote the element of $\boldsymbol{V}$ such that

$$v_a\equiv a \mod p.$$

Let

$$A(p,i)=\sum_{a=1}^{p-1}av_a^i, \qquad 0\leqq i<p-1, \qquad (i,2)=1.$$

Then $A(p,i)\equiv 0 \bmod p$ for $i\neq p-2$, and $A(p,p-2)\equiv -1 \bmod p$. Using $v_a\equiv a^p \bmod p^2$, we see easily that $A(p,i)\equiv 0 \bmod p^2$ if and only if the Bernoulli number $B_{(i+1)/2}$ is divisible by p.

Suppose that $i\neq p-2$. It follows from (1), with $n=0$, that

$${}^i\alpha={}^ig_0(0)=\sum_{a=1}^{p-1}\langle v_a/p\rangle v_a^i=\frac{1}{p}\sum_{a=1}^{p-1}av_a^i=\frac{1}{p}A(p,i).$$

Hence we obtain the following result (including $i=p-2$):

I. $M_i=0$ if and only if

$$A(p,i)\not\equiv 0 \mod p^2,$$

namely, if and only if

$$B_{(i+1)/2}\not\equiv 0 \mod p.$$

For each odd index i, $0\leqq i<p-1$, let

$$B(p,i)=\sum_{a,b=1}^{p-1}C_{a,b}bv_a^i,$$

where $C_{a,b}$ denotes the integer defined by

$$C_{a,b}\equiv\frac{1}{p}(v_a-a)+ab \mod p, \qquad 0\leqq C_{a,b}<p.$$

It follows from (1), with $n=1$, that

$${}^ig(T)\equiv{}^ig_1(T) \mod (pT,T^2) \qquad i\neq p-2.$$

Hence we obtain

$$\begin{aligned}{}^i\beta&\equiv\sum_{m=0}^{p-1}\sum_{v}\langle v(1+mp)/p^2\rangle v^im\\&\equiv\sum_{a,b=1}^{p-1}\langle(v_a+v_abp)/p^2\rangle bv_a^i \mod p.\end{aligned}$$

However,

$$v_a+v_abp\equiv a+\frac{1}{p}(v_a-a)p+abp\equiv a+C_{a,b}p \mod p^2,$$

$$0\leqq a+C_{a,b}p\leqq(p-1)+(p-1)p<p^2$$

so that

$$\langle(v_a+v_abp)/p^2\rangle=\frac{1}{p^2}(a+C_{a,b}p).$$

Therefore,

$$\begin{aligned} {}^i\beta &\equiv \frac{1}{p^2}\sum_{a,b=1}^{p-1}(a+C_{a,b}p)bv_a^i \\ &\equiv \frac{p-1}{2p}A(p,i)+\frac{1}{p}B(p,i) \mod p. \end{aligned}$$

It follows in particular that $B(p,i)\equiv 0 \bmod p$ for $i\neq p-2$.

Now, suppose that $A(p,i)\equiv 0 \bmod p^2$ and $B(p,i)\not\equiv 0 \bmod p^2$ $(i\neq p-2)$. We see from the above that ${}^i\alpha\equiv 0 \bmod p$, ${}^i\beta\not\equiv 0 \bmod p$ so that $d_i=1$, $e_i=0$. Let

$${}^iM(T)=T-{}^i\omega, \qquad {}^i\omega\in p\boldsymbol{Z}_p.$$

Then ${}^ig(T)={}^iu(T)(T-{}^i\omega)$ and ${}^iM=\Lambda/{}^ig(T)\Lambda=\Lambda/(T-{}^i\omega)\Lambda$. Hence we obtain the following result:

II. Suppose that

$$A(p,i)\equiv 0 \mod p^2, \qquad B(p,i)\not\equiv 0 \mod p^2.$$

Then ${}^ig(T)=0$ has a unique solution $T={}^i\omega$ in $p\boldsymbol{Z}_p$, and there is a Γ-isomorphism

$${}^iM\cong\boldsymbol{Z}_p,$$

where the action of Γ on $\boldsymbol{Z}_p$ is defined by

$$\sigma_{1+p}(y)=(1+{}^i\omega)y, \qquad y\in\boldsymbol{Z}_p.$$

Let p^f, $f\geqq 1$, be the highest power of p dividing ${}^i\omega$. Then, for each $n\geqq 0$, the above isomorphism induces a Γ-isomorphism

$${}^iM/(\sigma_{1+p}^{p^n}-1){}^iM\cong\boldsymbol{Z}_p/p^{n+f}\boldsymbol{Z}_p.$$

It follows in particular that ${}^iM/(\sigma_{1+p}^{p^n}-1){}^iM$ is a cyclic group of order p^{n+f}. We also note that ${}^ig({}^i\omega)=0$ implies

(2) $$ {}^i\omega\equiv-{}^i\alpha/{}^i\beta\equiv -A(p,i)/B(p,i) \mod p^2.$$

Therefore, $f=1$ if and only if

$$A(p,i)\not\equiv 0 \mod p^3.$$

5. We shall now explain the arithmetic meaning of the modules ${}^iM$.

It is well known that the class number h_n of F_n is the product of two integers, the so-called first and the second factor of h_n:

$$h_n = {}^-h_n {}^+h_n .$$

Let $p^{c(n)'}$ denote the highest power of p dividing the first factor ${}^-h_n$ of h_n. Then there exist again integers λ'_p, μ'_p, and ν'_p ($\lambda'_p, \mu'_p \geqq 0$) such that

$$c(n)' = \lambda'_p n + \mu'_p p^n + \nu'_p ,$$

for every sufficiently large n. For the coefficients λ'_p and μ'_p, we then have the following formula:

$$\lambda'_p = \sum_i d_i , \qquad \mu'_p = \sum_i e_i , \qquad 0 \leqq i < p-1, (i, 2) = 1 .$$

Therefore, the integers λ'_p and μ'_p can be obtained by computing d_i and e_i from the power series ${}^ig(T)$.

A prime number p is called regular if the class number h_0 is prime to p. In the following, we shall make an assumption on p which is weaker than the regularity. Namely, we assume that the second factor ${}^+h_0$ of h_0 is prime to p:

(A) $$({}^+h_0, p) = 1 .$$

Under this assumption, we have the following results on F_n:

i) For each $n \geqq 0$, the second factor ${}^+h_n$ of h_n is also prime to p so that $c(n) = c(n)'$. Hence

$$\lambda_p = \lambda'_p , \qquad \mu_p = \mu'_p , \qquad \nu_p = \nu'_p .$$

ii) For every even index i and for every $n \geqq 0$,

$${}^iS = {}^iS_n = 1 .$$

iii) For any $m \geqq n \geqq 0$, the homomorphism $S_n \to S_m$ is injective so that S may be simply regarded as the union of all S_n, $n \geqq 0$. S_n is then the subgroup of S consisting of all s in S such that $\sigma_{1+p}^{p^n}(s) = s$. For each i, a similar result holds also for ${}^iS$ and ${}^iS_n$, $n \geqq 0$.

iv) Let i and j be odd indices such that $i+j = p-1$. Then there exist a non-degenerate pairing of ${}^iM$ and ${}^jS$ into the additive group $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that

$$[\sigma(x), \sigma(s)] = [x, s] , \qquad x \in {}^iM, \ s \in {}^jS ,$$

for any σ in Γ.

v) It follows from iii) that for each $n \geqq 0$, the above pairing induces a similar pairing of ${}^iM/(\sigma_{1+p}^{p^n} - 1){}^iM$ and ${}^jS_n$. Hence these two are isomorphic finite abelian groups.

It is now clear that we can obtain the following results from I and II in the above:

III. Under the assumption (A), suppose that

$$A(p, i) \not\equiv 0 \mod p^2 ,$$

namely,

$$B_{(i+1)}/2 \not\equiv 0 \mod p ,$$

for an odd index i, $0 \leqq i < p-1$. Then, for the odd index $j = p-1-i$ and for every $n \geqq 0$,

$$^{j}S = {^{j}S_n} = 1 .$$

IV. Under the same assumption (A), suppose that

$$A(p, i) \equiv 0 \mod p^2 , \qquad B(p, i) \not\equiv 0 \mod p^2 ,$$

for an odd index i. Let $^{i}\omega$ and f be defined as in II, and let $j = p-1-i$. Then there is a Γ-isomorphism

$$^{j}S \cong \boldsymbol{Q}_p / \boldsymbol{Z}_p ,$$

where the action of Γ on $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ is defined by

$$\sigma_{1+p}(z) = (1 + {^{i}\omega})^{-1} z , \qquad z \in \boldsymbol{Q}_p / \boldsymbol{Z}_p .$$

For each $n \geqq 0$, it induces a Γ-isomorphism

$$^{j}S_n \cong p^{-(n+f)} \boldsymbol{Z}_p / \boldsymbol{Z}_p ,$$

so that $^{j}S_n$ is a cyclic group of order p^{n+f}. Furthermore, if

$$A(p, i) \not\equiv 0 \mod p^3 ,$$

then the above integer f is equal to $1: f = 1$.

Suppose that p is a regular prime ($p > 2$) so that (A) is satisfied for p. Then, by a theorem of Kummer, the Bernoulli numbers B_k, $1 \leqq k \leqq (p-1)/2$, are not divisible by p. Hence it follows from ii) and III that $^{i}S_n = 1$ for any i and n, namely, that $S_n = 1$ for every $n \geqq 0$. Therefore $c(n) = 0$ for $n \geqq 0$, and, consequently, $\lambda_p = \mu_p = \nu_p = 0$. We note that this result can be proved also by a direct method without referring to the modules ^{i}M.

6. In a sequence of papers[2)], Vandiver and others verified that our assumption (A) is satisfied for all prime numbers $p \leqq 4001$. For such a prime p, they also determined all integers k, $1 \leqq k \leqq (p-1)/2$, such that B_k is divisible by p. Putting

$$i = 2k - 1 ,$$

we then obtain all odd indices i for p such that

$$A(p, i) \equiv 0 \mod p^2 .$$

Let $\{p, i\}$ be such a pair, $p \leqq 4001$, and let

2) D. H. Lehmer, Emma Lehmer, and H. S. Vandiver, An application of high-speed computing to Fermat's last theorem, Proc. Nat. Acad. Sci. USA, **40** (1954), 25-33; H. S. Vandiver, Examination of methods of attack on the second case of Fermat's last theorem, Ibid., **40** (1954), 732-735; J. L. Selfridge, C. A. Nicol, and H. S. Vandiver, Proof of Fermat's last theorem for all prime exponents less than 4002, Ibid., **41** (1955), 970-973.

$$A(p,i)=\sum_{n=0}^{\infty}a_np^n\,,\qquad B(p,i)=\sum_{n=0}^{\infty}b_np^n\,,\qquad 0\leqq a_n,\,b_n<p\,,$$

be the p-adic expansions of the p-adic integers $A(p,i)$ and $B(p,i)$ respectively. We know from the above that

$$a_0=a_1=b_0=0\,.$$

By using a computer, we have computed the next coefficients a_2 and b_1, and found that

$$a_2\neq 0\,,\qquad b_1\neq 0 \tag{3}$$

for every such pair $\{p,i\}$. A part of the results of these computations will be given at the end of the paper.

Now, it follows from (3) that

$$A(p,i)\not\equiv 0 \mod p^3\,,\qquad B(p,i)\not\equiv 0 \mod p^2\,.$$

Therefore the following result is obtained from III and IV above:

Let $p\leqq 4001$ and let δ_p denote the number of those Bernoulli numbers B_k, $1\leqq k\leqq (p-1)/2$, which are divisible by p. Then, for each $n\geqq 0$, the Sylow p-subgroup S_n of the ideal class group of F_n is the direct product of δ_p cyclic groups of order p^{n+1}. Hence

$$c(n)=(n+1)\delta_p\,,$$

for every $n\geqq 0$, and consequently

$$\lambda_p=\nu_p=\delta_p\,,\qquad \mu_p=0\,.$$

Since the values of δ_p are known for $p\leqq 4001$[3], the structure of S_n is completely determined for such primes.

Actually, III and IV provide us more information on the structure of the G-groups $S=\Pi^iS$ and $S_n=\Pi^iS_n$, $n\geqq 0$: if i is an odd index such that $A(p,i)\equiv 0 \bmod p^2$, $p\leqq 4001$, then ${}^jS$, $j=p-1-i$, is isomorphic to the Γ-module $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ as described in IV.

Now, our computations of a_2 and b_1 show that

$$a_2\neq b_1$$

for every pair $\{p,i\}$ as stated above. Hence it follows from (2) that

$${}^i\omega\not\equiv -p \mod p^2\,.$$

Therefore, if z is an element of $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that $\sigma_{1+p}^{p^n}(z)=(1+p)^{p^n}z$ for some $n\geqq 0$, then $p^{n+1}z=0$. Since ${}^jS\cong\boldsymbol{Q}_p/\boldsymbol{Z}_p$, the Γ-group ${}^jS$ has the same property. By the theory of cyclotomic fields, we can then obtain the following result:

3) See the tables in the papers of the footnote 2). For example, $\delta_p=1$ for $p=37$, 59, 67, $\delta_p=2$ for $p=157$, and $\delta_p=3$ for $p=491$.

Let $p \leqq 4001$. Let Φ_n, $n \geqq 0$, be the local cyclotomic field of p^{n+1}-th roots of unity over $\boldsymbol{Q}_p$. Then the group of 1-units in the local field Φ_n contains $\frac{1}{2}(p-1)p^n-1$ global units in F_n which are multiplicatively independent over the ring of p-adic integers $\boldsymbol{Z}_p$.

7. The computations of a_2 and b_1 for those pairs $\{p, i\}$ such that $A(p, i) \equiv 0 \bmod p^2$ were carried out on an IBM 7094 computer[4]. During the preparation of the program it became clear that b_1 presented by far the greater difficulty. As defined,

$$B(p, i) = \sum_{a,b=1}^{p-1} C_{a,b} b v_a^i .$$

For $p = 4001$, the largest value we were considering, this sum has 16×10^6 terms. No more than about 10^4 terms could be computed per second, and so it seemed that for the larger values of p the computation time might be 30 minutes or more for each case. With 278 pairs to be run, this would have required more computer time than could be justified.

The problem was solved by finding a more efficient method of computing

$$\sum_{b=1}^{p-1} C_{a,b} b .$$

If $\frac{1}{p}(v_a - a) \equiv m \bmod p$, $0 \leqq m < p$, then

$$C_{a,b} = m + ab - p\left[\frac{m+ab}{p}\right].$$

(Here and throughout this section $[x]$ denotes the greatest integer less than or equal to x.) Thus

$$\begin{aligned}\sum_{b=1}^{p-1} C_{a,b} b &= \sum_{b=1}^{p-1} b\left(m + ab - p\left[\frac{m+ab}{p}\right]\right) \\ &= \frac{mp(p-1)}{2} + \frac{ap(p-1)(2p-1)}{6} - p\sum_{b=1}^{p-1} b\left[\frac{m+ab}{p}\right].\end{aligned}$$

For any integers m, a, r, and s with $s > 0$, $r > m \geqq 0$, and $a \geqq 0$, define

$$F(m, a, r, s) = \sum_{b=1}^{s}\left[\frac{m+ab}{r}\right],$$

$$G(m, a, r, s) = \sum_{b=1}^{s} b\left[\frac{m+ab}{r}\right],$$

$$H(m, a, r, s) = \sum_{b=1}^{s}\left[\frac{m+ab}{r}\right]^2.$$

We have

4) The computation was done at the M. I. T. Computation Center, Cambridge, Massachusetts.

$$\sum_{b=1}^{p-1} C_{a,b}b = \frac{mp(p-1)}{2} + \frac{ap(p-1)(2p-1)}{6} - pG(m, a, p, p-1).$$

F, G, and H satisfy certain recursion relations. Let $r = ua+v$, $m+1 = xa-y$, $0 \leqq v$, $y < a$. Also let

$$z = \left[\frac{m+as}{r}\right].$$

If $z=0$, then $F(m, a, r, s) = G(m, a, r, s) = H(m, a, r, s) = 0$. If $z>0$, then $a>0$ and

$$F(m, a, r, s) = z(s+x) - \frac{uz(z+1)}{2} - F(y, v, a, z),$$

$$2G(m, a, r, s) = zs(s+1) - zx(x-1) - \frac{u^2z(z+1)(2z+1)}{6}$$
$$- \frac{u(1-2x)z(z+1)}{2} - 2uG(y, v, a, z)$$
$$-(1-2x)F(y, v, a, z) - H(y, v, a, z),$$

$$H(m, a, r, s) = sz^2 - \frac{uz(z+1)(2z+1)}{3} + \frac{(2x+u)z(z+1)}{2} - xz$$
$$-2G(y, v, a, z) + F(y, v, a, z).$$

The proofs of these formulas are similar and we give only the proof of the first. We may assume $z>0$ and therefore $a>0$. For any positive integer t,

$$\left[\frac{m+ab}{r}\right] = t$$

for $k_t+1 \leqq b \leqq k_{t+1}$, where

$$k_t = \left[\frac{tr-1-m}{a}\right].$$

Since $r>m$ and $z>0$, we have $0 \leqq k_1 < s$. If we redefine k_{z+1} to be s, then

$$F(m, a, r, s) = \sum_{b=1}^{s}\left[\frac{m+ab}{r}\right] = \sum_{t=1}^{z}\sum_{k_t+1}^{k_{t+1}} t = sz - \sum_{t=1}^{z} k_t.$$

If $r = ua+v$ and $m+1 = xa-y$, $0 \leqq v$, $y < a$, then

$$k_t = tu - x + \left[\frac{y+tv}{a}\right].$$

Thus

$$\sum_{t=1}^{z} k_t = \frac{uz(z+1)}{2} - xz + F(y, v, a, z)$$

and

$$F(m, a, r, s) = z(s+x) - \frac{uz(z+1)}{2} - F(y, v, a, z).$$

If these formulas are used to compute $G(m, a, p, p-1)$, the computation time for b_1 becomes proportional to $p \log p$ and for $p=4001$ is under two minutes.

8. We possess a complete table of a_2 and b_1, computed for all pairs $\{p, i\}$, $p \leqq 4001$, satisfying $A(p, i) \equiv 0 \bmod p^2$. However, we produce here only the part of the table where $1 < p < 400$ or $3600 < p \leqq 4001$. Since the root ${}^i\omega$ of ${}^i g(T) = 0$ seems to have an important meaning in the theory of cyclotomic fields, we also indicate in the last column the values of the integer c such that $c \equiv -a_2/b_1 \bmod p$, $0 \leqq c < p$, namely, such that

$$ {}^i\omega \equiv cp \quad \bmod p^2, \qquad 0 \leqq c < p. $$

p	i	a_2	b_1	c
37	31	23	16	24
59	43	20	33	28
67	57	34	46	8
101	67	16	59	10
103	23	1	49	21
131	21	34	106	59
149	129	24	70	55
157	61	66	109	21
157	109	109	106	36
233	83	3	101	143
257	163	124	69	28
263	99	66	176	164
271	83	141	92	78
283	19	272	268	37
293	155	57	200	218
307	87	108	102	17
311	291	152	34	87
347	279	246	241	166
353	185	260	52	348
353	299	289	192	118
379	99	327	103	236
379	173	256	297	188
389	199	340	341	234
3607	1975	3279	2832	2578
3613	2081	1991	1798	2147
3617	15	2574	1314	989
3617	2855	57	667	2733
3631	1103	3591	3510	1200
3637	2525	2894	1313	2139
3637	3201	1685	1504	3174
3671	1579	3619	555	3261
3677	2237	31	3273	2594
3697	1883	3575	1905	1638
3779	2361	2454	2855	1794
3797	1255	3066	1548	3692
3821	3295	2776	1320	160

3833	1839	156	886	95
3833	1997	2944	328	178
3833	3285	1307	1329	547
3851	215	2297	1909	606
3851	403	1828	2438	2555
3853	747	2331	2270	1844
3881	1685	3189	252	1050
3881	2137	2674	692	1645
3917	1489	1658	3382	889
3967	105	2505	1543	2883
3989	1935	679	3616	2130
4001	533	3054	3587	1515

Massachusetts Institute of Technology