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 \( F_n, \ n \geq 0 \), denote the cyclotomic field of \( p^{n+1} \)-th roots of unity over the rational field \( \mathbb{Q} \). Let \( p^{c(n)} \) be the highest power of \( p \) dividing the class number \( h_n \) of \( F_n \). Then there exist integers \( \lambda_p, \mu_p, \text{ and } \nu_p \) (\( \lambda_p, \mu_p, \nu_p \geq 0 \)), depending only upon \( p \), such that

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

for every sufficiently large integer \( n^{11} \). In the present paper, we shall determine, by the help of a computer, the coefficients \( \lambda_p, \mu_p, \text{ and } \nu_p \) in the above formula for all prime numbers \( p \leq 4001 \). We shall see in particular that \( \mu_p = 0 \) for every \( p \leq 4001 \). 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 \( n \geq 0 \).

Let \( p = 2 \). Then we know by Weber's theorem that \( c(n) = 0 \), \( S_n = 1 \) for any \( n \geq 0 \) 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 \( \mathbb{Q}_p \) and \( \mathbb{Z}_p \) denote the field of \( p \)-adic numbers and the ring of \( p \)-adic integers, respectively. Let \( F \) be the union of all fields \( F_n, \ n \geq 0 \). Then \( F \) is an abelian extension of \( \mathbb{Q} \), and we denote the Galois group of \( F/\mathbb{Q} \) by \( G \). For each \( p \)-adic unit \( u \) in \( \mathbb{Q}_p \), there is a unique automorphism \( \sigma_u \) of \( F \) such that \( \sigma_u(\zeta^a) = \zeta^a u \) for any root of unity \( \zeta \) 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 \( \mathbb{Q}_p \) onto the compact abelian group \( G \). Let \( I \) and \( A \) denote the subgroups of \( G \) corresponding to the group of \( 1 \)-units in \( \mathbb{Q}_p \) and the group \( V \) of all \((p-1)\)-st roots of unity in \( \mathbb{Q}_p \), respectively. Then we have

\[
G = I \times A;
\]

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

Let $\Gamma$ be the Galois group of $F/F_0$, and $\Delta$ be a cyclic group of order $p-1$, canonically isomorphic to the Galois group of $F_0/Q$.

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

3. Let $A$ denote the ring of formal power series in an indeterminate $T$ with coefficients in $\mathbb{Z}_p$: $A = \mathbb{Z}_p[[T]]$. Then there is an injective homomorphism of $\Gamma$ into the multiplicative group of $A$ such that $\sigma_{i+p}(x) = (1+T)x$ for every $x$ in $M$.

For any $a$ in $Q_p$, there exist a rational integer $b$ and a power of $p$, $p^m$ ($m \geq 0$), such that $p^ma \equiv b \mod p^m$, $0 \leq b < p^m$. 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 $i$, $0 < i < p-1$, we shall next define a power series $i'g(T)$ in $A$. First, we put $i'g(T) = 1$. Let $i \neq p-2$. For each $n \geq 0$, let

$$i'g_n(T) = \sum_{m,v} \langle v(1+p)^m/p^{n+1} \rangle v'(1+T)^m,$$

where $0 \leq m < p^n$, $v \in V$. Then $i'g_n(T)$ is a polynomial in $T$ with coefficients in $\mathbb{Z}_p$, and when $n$ tends to infinity, $i'g_n(T)$ converges, on each coefficient of $T^m$, $m \geq 0$, to a power series in $A$, which we denote by $i'g(T)$:

$$i'g(T) = \lim_{n \to \infty} i'g_n(T).$$

We see easily that

$$i'g(T) \equiv i'g_n(T) \mod (1-(1+T)^p)^n A, \quad n \geq 0.$$ 

For each odd $i$, there exist, by Weierstrass' preparation theorem, an integer $e_i \geq 0$, a unit $i'u(T)$ of the ring $A$, and a polynomial $i'm(T)$ of the form

$$i'm(T) = i'a_0 + \cdots + i'a_{d_i-1}T^{d_i-1} + T^{d_i}, \quad i'a_k \in p\mathbb{Z}_p,$$

such that

$$i'g(T) = p^e i'u(T)i'm(T).$$

Now, let

$$i'M = A/i'g(T)A, \quad 0 \leq i < p-1, \quad (i,2) = 1.$$ 

As noted in the above, we may consider $i'M$ as $\Gamma$-modules. These $\Gamma$-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

$$i^2g(T) = i^x + i^y T + i^z T^2 + \cdots,$$

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

For any integer $a$, $1 \leq a \leq p-1$, let $v_a$ denote the element of $V$ such that

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

Let

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

Then $A(p, i) \equiv 0 \mod p$ for $i \neq p-2$, and $A(p, p-2) \equiv -1 \mod p$. Using $v_a \equiv a^p \mod p^2$, we see easily that $A(p, i) \equiv 0 \mod p^2$ 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

$$i^x = i^x0(0) = \sum_{a=1}^{p-1} \left\langle v_a / p \right\rangle v_a^i \equiv \frac{1}{p} \sum_{a=1}^{p-1} av_a^i = \frac{1}{p} A(p, i).$$

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

1. $M_i = 0$ if and only if

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

namely, if and only if

$$B(i+1, 2) \equiv 0 \mod p.$$

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

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

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

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

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

$$i^2g(T) \equiv i^x0(T) \mod (pT, T^2) \quad i \neq p-2.$$

Hence we obtain

$$i^x \equiv \sum_{m=0}^{p-1} \sum_{b} \left\langle v(1+mb)/p^2 \right\rangle v^m b v_a^i \mod p.$$ 

However,
Computation of invariants

\[ v_a + v_a b p = a + \frac{1}{p} (v_a - a) + ab p \equiv a + C_{a,b} p \mod p^2, \]

so that

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

Therefore,

\[ \hat{\beta} \equiv \frac{1}{p^2} \sum_{a,b=1}^{p-1} (a + C_{a,b} p) b v_a \]

\[ \equiv \frac{p-1}{2p} A(p, i) + \frac{1}{p} B(p, i) \mod p. \]

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

Now, suppose that \( A(p, i) \equiv 0 \mod p^2 \) and \( B(p, i) \neq 0 \mod p^2 \) (\( i \neq p-2 \)).

We see from the above that \( \hat{\alpha} \equiv 0 \mod p \), \( \hat{\beta} \neq 0 \mod p \) so that \( d_i = 1 \), \( e_i = 0 \).

Let

\[ g(T) = \omega^r \quad r \in \mathbb{Z}_p. \]

Then \( g(T) = \omega^r (T^{p-1}) \) and \( M = A/g(T)A = A/(T^{p-1})A \). Hence we obtain the following result:

II. Suppose that

\[ A(p, i) \equiv 0 \mod p^2, \quad B(p, i) \neq 0 \mod p^2. \]

Then \( g(T) = 0 \) has a unique solution \( T = \omega^r \) in \( \mathbb{Z}_p \), and there is a \( \Gamma \)-isomorphism

\[ M \cong \mathbb{Z}_p, \]

where the action of \( \Gamma \) on \( \mathbb{Z}_p \) is defined by

\[ \sigma_1 \sigma_2 (y) = (1 + \omega) y, \quad y \in \mathbb{Z}_p. \]

Let \( p^f, f \geq 1 \), be the highest power of \( p \) dividing \( \omega \). Then, for each \( n \geq 0 \), the above isomorphism induces a \( \Gamma \)-isomorphism

\[ M/(\sigma_1^n \sigma_2^n - 1)^t M \cong \mathbb{Z}_p/p^{n+f} \mathbb{Z}_p. \]

It follows in particular that \( M/(\sigma_1^n \sigma_2^n - 1)^t M \) is a cyclic group of order \( p^{n+f} \).

We also note that \( g(\omega) = 0 \) implies

\[ \omega = -\frac{1}{\alpha + \beta} = -A(p, i)/B(p, i) \mod p^2. \]

Therefore, \( f = 1 \) if and only if

\[ A(p, i) \neq 0 \mod p^2. \]

5. We shall now explain the arithmetic meaning of the modules \( \omega^r \).

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 \( h_n \):
\[ h_n = \ell h_n. \]

Let \( p^e(n) \) denote the highest power of \( p \) dividing the first factor \( \ell h_n \) of \( h_n \). Then there exist again integers \( \ell_p, \mu_p, \) and \( \nu_p (\ell_p, \mu_p \geq 0) \) such that

\[ c(n)' = \ell_p n + \mu_p n^\alpha + \nu_p, \]

for every sufficiently large \( n \). For the coefficients \( \ell_p \) and \( \mu_p \), we then have the following formula:

\[ \ell_p = \sum_i d_i, \quad \mu_p = \sum_i e_i, \quad 0 \leq i < p-1, (i, 2) = 1. \]

Therefore, the integers \( \ell_p \) and \( \mu_p \) can be obtained by computing \( d_i \) and \( e_i \) from the power series \( g(T) \).

A prime number \( p \) is called regular if the class number \( h_n \) 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 \( \ell h_n \) of \( h_n \) is prime to \( p \):

(A) \((\ell h_n, p) = 1\).

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

i) For each \( n \geq 0 \), the second factor \( \ell h_n \) of \( h_n \) is also prime to \( p \) so that \( c(n) = c(n)' \). Hence

\[ \ell_p = \ell_p', \quad \mu_p = \mu_p', \quad \nu_p = \nu_p'. \]

ii) For every even index \( i \) and for every \( n \geq 0 \),

\[ tS = tS_n = 1. \]

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

iv) Let \( i \) and \( j \) be odd indices such that \( i+j = p-1 \). Then there exist a non-degenerate pairing of \( tM \) and \( tS \) into the additive group \( \mathbb{Q}/Z_p \) such that

\[ [\sigma(x), \sigma(s)] = [x, s], \quad x \in tM, s \in tS, \]

for any \( \sigma \) in \( \Gamma \).

v) It follows from iii) that for each \( n \geq 0 \), the above pairing induces a similar pairing of \( tM/(\sigma_{\ell_p}^n-1) tM \) and \( tS_n \). 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

\[ A(p, i) \neq 0 \mod p^\alpha, \]

namely,

\[ B_{(i+1)}/2 \neq 0 \mod p, \]
for an odd index $i$, $0 \leq i < p - 1$. Then, for the odd index $j = p - 1 - i$ and for every $n \geq 0$,

$$^iS = ^iS_n = 1.$$  

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

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

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

$$^iS \cong \mathbb{Q}_p / \mathbb{Z}_p,$$

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

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

For each $n \geq 0$, it induces a $\Gamma$-isomorphism

$$^iS_n \cong \mathbb{Q}_p / (n + f) / \mathbb{Z}_p,$$

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

$$A(p, i) \equiv 0 \mod p^3,$$

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 $B_k$, $1 \leq k \leq (p-1)/2$, are not divisible by $p$. Hence it follows from ii) and III that $^iS_n = 1$ for any $i$ and $n$, namely, that $S_n = 1$ for every $n \geq 0$. Therefore $c(n) = 0$ for $n \geq 0$, and, consequently, $\lambda_p = \rho_p = \nu_p = 0$. We note that this result can be proved also by a direct method without referring to the modules $^iM$.

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

$$i = 2k - 1,$$

we then obtain all odd indices $i$ for $p$ such that

$$A(p, i) \equiv 0 \mod p^3.$$

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

---

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

$$(3) \quad a_2 \neq 0, \quad b_1 \neq 0$$

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

$$A(p, i) \equiv 0 \mod p^3, \quad B(p, i) \equiv 0 \mod p^2.$$  

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

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

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

for every $n \geq 0$, and consequently

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

Since the values of $\delta_p$ are known for $p \leq 4001^3$, 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 $S = \prod \Gamma S$ and $S_n = \prod \Gamma S_n$, $n \geq 0$: if $i$ is an odd index such that $A(p, i) \equiv 0 \mod p^2$, $p \leq 4001$, then $\Gamma S, j = p-1-i$, is isomorphic to the $\Gamma$-module $Q_p/Z_p$ as described in IV.

Now, our computations of $a_2$ and $b_1$ show that

$$a_2 = b_1$$

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

$$(\omega \neq -p) \mod p^2.$$  

Therefore, if $z$ is an element of $Q_p/Z_p$ such that $a_{p^{n+1}}(z) = (1+p)p^n z$ for some $n \geq 0$, then $p^{n+1}z = 0$. Since $\Gamma S \cong Q_p/Z_p$, the $\Gamma$-group $\Gamma S$ 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 $p = 491$. 

K. IWASAWA and C. SIMS

\[ A(p, i) = \sum_{n=0}^{\infty} a_n p^n, \quad B(p, i) = \sum_{n=0}^{\infty} b_n p^n, \quad 0 \leq a_n, b_n < p, \]
Let \( p \leq 4001 \). Let \( \Phi_n \), \( n \geq 0 \), be the local cyclotomic field of \( p^{n+1} \)-th roots of unity over \( \mathbb{Q}_p \). Then the group of 1-units in the local field \( \Phi_n \) 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 \( \mathbb{Z}_p \).

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

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

For \( p = 4001 \), the largest value we were considering, this sum has \( 16 \times 10^6 \) 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

\[
\sum_{b=1}^{p-1} C_{a, b} v_a^b .
\]

If \( \frac{1}{p} (v_a - a) \equiv m \mod p \), \( 0 \leq m < p \), then

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

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

\[
\sum_{b=1}^{p-1} C_{a, b} = \sum_{b=1}^{p-1} b \left( m + ab - p \left\lfloor \frac{m + ab}{p} \right\rfloor \right) = m b (p-1) + a p (p-1)(2p-1) - 6 \sum_{b=1}^{p-1} b \left\lfloor \frac{m + ab}{p} \right\rfloor .
\]

For any integers \( m, a, r, \) and \( s \) with \( s > 0 \), \( r > m \geq 0 \), and \( a \geq 0 \), define

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

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

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

We have

4) The computation was done at the M.I.T. Computation Center, Cambridge, Massachusetts.
\[ F, G, \text{ and } H \text{ satisfy certain recursion relations. Let } r = ua + v, m + 1 = xa - y, 0 \leq v, y < a. \text{ Also let} \]
\[ z = \left\lfloor \frac{m + as}{r} \right\rfloor. \]
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
\[ F(m, a, r, s) = z(s + x) - uz(z + 1) - F(y, v, a, z), \]
\[ 2G(m, a, r, s) = zs(s + 1) - zx(x - 1) - uz(z + 1)(2z + 1) - \frac{(1 - 2x)z(z + 1)}{2} - 2uG(y, v, a, z) - (1 - 2x)F(y, v, a, z) - H(y, v, a, z), \]
\[ H(m, a, r, s) = sz^2 - uz(z + 1)(2z + 1) + (2x + u)z(z + 1) - xz. \]
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 \( t \),
\[ \left\lfloor \frac{m + ab}{r} \right\rfloor = t \]
for \( k_t + 1 \leq b \leq k_{t+1} \), where
\[ k_t = \left\lfloor \frac{tr - 1 - m}{a} \right\rfloor. \]
Since \( r > m \) and \( z > 0 \), we have \( 0 \leq k_t < s \). If we redefine \( k_{t+1} \) to be \( s \), then
\[ F(m, a, r, s) = \sum_{b=1}^{s} \left\lfloor \frac{m + ab}{r} \right\rfloor = \sum_{t=1}^{s} \sum_{k_t+1}^{k_{t+1}} t = sz - \sum_{t=1}^{s} k_t. \]
If \( r = ua + v \) and \( m + 1 = xa - y, 0 \leq v, y < a \), then
\[ k_t = tu - x + \left\lfloor \frac{y + tv}{a} \right\rfloor. \]
Thus
\[ \sum_{t=1}^{s} k_t = \frac{uz(z + 1)}{2} - xz + F(y, v, a, z) \]
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
Computation of invariants

8. We possess a complete table of $a_2$ and $b_1$, computed for all pairs $(p, i)$, $p \leq 4001$, satisfying $A(p, i) \equiv 0 \mod p^2$. However, we produce here only the part of the table where $1 < p < 400$ or $3600 < p \leq 4001$. Since the root $i\omega$ of $i\gamma(T) = 0$ 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 $c \equiv -a_2/b_1 \mod p$, $0 \leq c < p$, namely, such that

$$i\omega \equiv cp \mod p^2, \quad 0 \leq c < p.$$ 

<table>
<thead>
<tr>
<th>$p$</th>
<th>$i$</th>
<th>$a_2$</th>
<th>$b_1$</th>
<th>$c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>31</td>
<td>23</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>59</td>
<td>43</td>
<td>20</td>
<td>33</td>
<td>28</td>
</tr>
<tr>
<td>67</td>
<td>57</td>
<td>34</td>
<td>46</td>
<td>8</td>
</tr>
<tr>
<td>101</td>
<td>67</td>
<td>16</td>
<td>59</td>
<td>10</td>
</tr>
<tr>
<td>103</td>
<td>23</td>
<td>1</td>
<td>49</td>
<td>21</td>
</tr>
<tr>
<td>131</td>
<td>21</td>
<td>34</td>
<td>106</td>
<td>59</td>
</tr>
<tr>
<td>149</td>
<td>129</td>
<td>24</td>
<td>70</td>
<td>55</td>
</tr>
<tr>
<td>157</td>
<td>61</td>
<td>66</td>
<td>109</td>
<td>21</td>
</tr>
<tr>
<td>157</td>
<td>109</td>
<td>106</td>
<td>21</td>
<td>143</td>
</tr>
<tr>
<td>233</td>
<td>83</td>
<td>3</td>
<td>101</td>
<td>28</td>
</tr>
<tr>
<td>233</td>
<td>163</td>
<td>124</td>
<td>69</td>
<td>21</td>
</tr>
<tr>
<td>263</td>
<td>99</td>
<td>66</td>
<td>176</td>
<td>164</td>
</tr>
<tr>
<td>271</td>
<td>83</td>
<td>141</td>
<td>92</td>
<td>78</td>
</tr>
<tr>
<td>283</td>
<td>19</td>
<td>272</td>
<td>268</td>
<td>37</td>
</tr>
<tr>
<td>293</td>
<td>155</td>
<td>57</td>
<td>200</td>
<td>218</td>
</tr>
<tr>
<td>307</td>
<td>87</td>
<td>108</td>
<td>102</td>
<td>17</td>
</tr>
<tr>
<td>311</td>
<td>291</td>
<td>152</td>
<td>34</td>
<td>87</td>
</tr>
<tr>
<td>347</td>
<td>279</td>
<td>246</td>
<td>241</td>
<td>166</td>
</tr>
<tr>
<td>353</td>
<td>185</td>
<td>260</td>
<td>52</td>
<td>348</td>
</tr>
<tr>
<td>353</td>
<td>299</td>
<td>289</td>
<td>192</td>
<td>118</td>
</tr>
<tr>
<td>379</td>
<td>99</td>
<td>327</td>
<td>103</td>
<td>236</td>
</tr>
<tr>
<td>379</td>
<td>173</td>
<td>256</td>
<td>297</td>
<td>188</td>
</tr>
<tr>
<td>389</td>
<td>199</td>
<td>340</td>
<td>341</td>
<td>234</td>
</tr>
<tr>
<td>3607</td>
<td>1975</td>
<td>3279</td>
<td>2832</td>
<td>2573</td>
</tr>
<tr>
<td>3613</td>
<td>2081</td>
<td>1991</td>
<td>1798</td>
<td>2147</td>
</tr>
<tr>
<td>3617</td>
<td>15</td>
<td>2574</td>
<td>1314</td>
<td>989</td>
</tr>
<tr>
<td>3617</td>
<td>2855</td>
<td>57</td>
<td>667</td>
<td>2733</td>
</tr>
<tr>
<td>3631</td>
<td>1103</td>
<td>3591</td>
<td>3510</td>
<td>1200</td>
</tr>
<tr>
<td>3637</td>
<td>2525</td>
<td>2894</td>
<td>1313</td>
<td>2139</td>
</tr>
<tr>
<td>3637</td>
<td>3201</td>
<td>1685</td>
<td>1504</td>
<td>3174</td>
</tr>
<tr>
<td>3671</td>
<td>1579</td>
<td>3619</td>
<td>555</td>
<td>3261</td>
</tr>
<tr>
<td>3677</td>
<td>2237</td>
<td>31</td>
<td>3273</td>
<td>2594</td>
</tr>
<tr>
<td>3697</td>
<td>1883</td>
<td>3575</td>
<td>1905</td>
<td>1638</td>
</tr>
<tr>
<td>3779</td>
<td>2361</td>
<td>2454</td>
<td>2855</td>
<td>1794</td>
</tr>
<tr>
<td>3797</td>
<td>1255</td>
<td>3066</td>
<td>1548</td>
<td>3692</td>
</tr>
<tr>
<td>3821</td>
<td>3295</td>
<td>2776</td>
<td>1320</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>3833</td>
<td>1839</td>
<td>156</td>
<td>886</td>
<td>95</td>
</tr>
<tr>
<td>3833</td>
<td>1997</td>
<td>2944</td>
<td>328</td>
<td>178</td>
</tr>
<tr>
<td>3833</td>
<td>3285</td>
<td>1307</td>
<td>1329</td>
<td>547</td>
</tr>
<tr>
<td>3851</td>
<td>215</td>
<td>2297</td>
<td>1909</td>
<td>606</td>
</tr>
<tr>
<td>3851</td>
<td>403</td>
<td>1828</td>
<td>2438</td>
<td>2555</td>
</tr>
<tr>
<td>3853</td>
<td>747</td>
<td>2331</td>
<td>2270</td>
<td>1844</td>
</tr>
<tr>
<td>3881</td>
<td>1685</td>
<td>3189</td>
<td>252</td>
<td>1050</td>
</tr>
<tr>
<td>3881</td>
<td>2137</td>
<td>2674</td>
<td>692</td>
<td>1645</td>
</tr>
<tr>
<td>3917</td>
<td>1489</td>
<td>1658</td>
<td>3382</td>
<td>889</td>
</tr>
<tr>
<td>3967</td>
<td>105</td>
<td>2505</td>
<td>1543</td>
<td>2883</td>
</tr>
<tr>
<td>3989</td>
<td>1935</td>
<td>679</td>
<td>3616</td>
<td>2130</td>
</tr>
<tr>
<td>4001</td>
<td>533</td>
<td>3054</td>
<td>3587</td>
<td>1515</td>
</tr>
</tbody>
</table>

Massachusetts Institute of Technology