Let $K$ be a number field, with degree $n$ and ring of integers $\mathcal{O}_K$. If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. We call such a basis a power basis.

When $K$ is a quadratic field or a cyclotomic field, $\mathcal{O}_K$ admits a power basis, and the use of these two fields as examples in algebraic number theory can lead to the impression that rings of integers always have a power basis. This is false. While it is always true that

$$\mathcal{O}_K = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$$

for some $e_1, \ldots, e_n$, often we can not choose the $e_i$’s to be powers of a single number.

The first published example of $K$ where $\mathcal{O}_K$ has no power basis is due to Dedekind [2, pp. 30–36] in 1878. It is $\mathbb{Q}(\theta)$ where $\theta^3 - \theta^2 - 2\theta - 8 = 0$. Dedekind wrote about this field in a less explicit form in 1871 [1, pp. 1490–1492]. The ring of integers of $\mathbb{Q}(\theta)$ has $\mathbb{Z}$-basis $\{1, \theta, (\theta + \theta^2)/2\}$ but no power basis. We will return to this example in Remark 2.

Our main purpose here is to give infinitely many examples of number fields whose ring of integers does not have a power basis. The examples will be Galois cubic extensions of $\mathbb{Q}$.

Fix a prime $p \equiv 1 \pmod{3}$. Since $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, there is a unique cubic subfield $F_p$ in $\mathbb{Q}(\zeta_p)$ and $\text{Gal}(F_p/\mathbb{Q})$ is the quotient of $(\mathbb{Z}/p\mathbb{Z})^\times$ by its subgroup of cubes. In particular, for each prime $q \neq p$, $q$ splits completely in $F_p$ if and only if the Frobenius of $q$ in $\text{Gal}(F_p/\mathbb{Q})$ is trivial, which is equivalent to $q$ being a cube modulo $p$.

**Theorem 1.** If $p \equiv 1 \pmod{3}$ and $2$ is a cube in $\mathbb{Z}/p\mathbb{Z}$, then $\mathcal{O}_{F_p} \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_{F_p}$ such that $F = \mathbb{Q}(\alpha)$.

*Proof.* Suppose $\mathcal{O}_{F_p} = \mathbb{Z}[\alpha]$ for some $\alpha$. Let $\alpha$ have minimal polynomial $f(T)$ over $\mathbb{Q}$, so $f$ is an irreducible cubic in $\mathbb{Z}[T]$. Then

$$\mathcal{O}_{F_p} = \mathbb{Z}[\alpha] \cong \mathbb{Z}[T]/f(T).$$

Since $2 \mod p$ is a cube, $2$ splits completely in $F_p$, so $f(T)$ splits completely in $(\mathbb{Z}/2\mathbb{Z})[T]$. But cubics in $(\mathbb{Z}/2\mathbb{Z})[T]$ don’t split completely: there are only two (monic) linear polynomials mod 2. □

The set of primes that fit the hypotheses of Theorem 1 are those $p \equiv 1 \pmod{3}$ such that $2^{(p-1)/3} \equiv 1 \pmod{p}$. These are the primes that split completely in the splitting field of $T^3 - 2$ over $\mathbb{Q}$, and by the Chebotarev density theorem there is a positive proportion of such primes (their density is 1/6). The first few are 31, 43, 109, and 127. For each such $p$, Theorem 1 tells us the ring of integers of $F_p$ does not have a power basis.

**Remark 2.** The proof that the integer ring of Dedekind’s field $\mathbb{Q}(\theta)$ lacks a power basis operates on the same principle as Theorem 1: show 2 splits completely in the integers of $\mathbb{Q}(\theta)$, and that implies there is no power basis for the same reason as in Theorem 1. However, to show 2 splits completely in $\mathbb{Q}(\theta)$ requires techniques other than those we used.

---

1Some references use a root of $T^3 + T^2 - 2T + 8$, which is the minimal polynomial for $-\theta$. The mixture of positive and negative coefficients makes it harder to remember this polynomial, so don’t use it.
in the fields $F_p$, since Dedekind’s field is not in a cyclotomic field (for example, $Q(\theta)$ is not Galois over $Q$).

Theorem 3 is a special case of the following result: if $K/Q$ is cubic then $[O_K : Z[\alpha]]$ is even for all $\alpha \in O_K - Z$ if and only if 2 splits completely in $K$. Having the index always be even implies $O_K \neq Z[\alpha]$ for all $\alpha$ since the index can’t be 1. (In 1882, Kronecker [7, p. 119] said he found an example in 1858 of a field $K$ in $Q(\zeta_{13})$ where $O_K$ has no power basis over $Z$. It is the quartic subfield $K$, where $3 \mid [O_K : Z[\alpha]]$ for all $\alpha \in O_K$ such that $K = Q(\alpha)$. This preceded Dedekind finding the cubic example by over 10 years.)

A broader context for $[O_K : Z[\alpha]]$ always being even is a prime $p$ satisfying $p \mid [O_K : Z[\alpha]]$ for all $\alpha \in O_K$ such that $K = Q(\alpha)$. Call such $p$ a common index divisor for $K$. The existence of such $p$ is sufficient for $O_K$ not to have a power basis. Dedekind [2, Sect. 4] and later Hensel [5, p. 138]) showed a prime $p$ is a common index divisor for a number field $K$ if and only if there is $d \geq 1$ such that the number of different prime ideal factors of $pO_K$ with residue field degree $d$ is greater than the number of monic irreducibles of degree $d$ in $F_p[T]$. In particular, if $[K : Q] \geq 3$ and 2 splits completely, then $[O_K : Z[\alpha]]$ is even for all $\alpha \in O_K$ such that $K = Q(\alpha)$, since there are only two monic irreducibles of degree 1 in $F_2[T]$. (A prime $p$ that is a common index divisor for a number field $K$ must be less than $[K : Q]$ by a theorem of von Zylinski [10]. See [3] for a proof that there are infinitely many cubic fields without a power basis for which this even-index condition does not apply.

The integer ring of $F_p$ (for $p \equiv 1 \mod 3$) has a $Z$-basis and we know it need not be a power basis. What is a $Z$-basis for this ring?

**Theorem 3.** For $p \equiv 1 \mod 3$ let

$$\eta_0 = Tr_{Q(Q_p)/F_p}(\zeta_p) = \sum_{t(p-1)/3 \equiv 1 \mod p} \zeta_p^t.$$  

Fixing an element $r \in (Z/pZ)^\times$ with order 3, let

$$\eta_1 = \sum_{t(p-1)/3 \equiv r \mod p} \zeta_p^t, \quad \eta_2 = \sum_{t(p-1)/3 \equiv r^2 \mod p} \zeta_p^t.$$  

Then $O_{F_p} = Z\eta_0 + Z\eta_1 + Z\eta_2$.

The numbers $\eta_i$ are examples of (cycloptomic) periods [9, pp. 16–17].

**Proof.** For $c \in (Z/pZ)^\times$, $c^{(p-1)/3}$ is a cube root of unity and therefore is in $\{1, r, r^2\}$. For suitable $c$ each of the three values is achieved. Let $\sigma_c \in Gal(Q(Q_p)/Q)$ send $\zeta_p$ to $\zeta_p^c$. Then

$$\sigma_c(\eta_i) = \sigma_c \left( \sum_{t(p-1)/3 \equiv r \mod p} \zeta_p^t \right) = \sum_{t(p-1)/3 \equiv c(r) \mod p} \zeta_p^t = \sum_{t(p-1)/3 \equiv (p-1)/3 \mod p} \zeta_p^t,$$

so $\sigma_c$ permutes $\{\eta_0, \eta_1, \eta_2\}$ the same way multiplication by $c^{(p-1)/3}$ permutes $\{1, r, r^2\}$. Therefore $\eta_0$, $\eta_1$, and $\eta_2$ are $Q$-conjugates, and since $F_p$ is the unique cubic subfield of $Q(Q_p)$ each of $\eta_0, \eta_1, \eta_2$ generates $F_p$ as a field extension of $Q$.

---

This criterion is not necessary: for $K = Q(\sqrt[3]{175})$, $O_K$ has no power basis but $[O_K : Z[\sqrt[3]{175}]] = 5$ and $[O_K : Z[\sqrt[3]{245}]] = 7$. This is explained in Example 4.15 in [https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf](https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf).


The standard basis of \(\mathbb{Q}(\zeta_p)\) over \(\mathbb{Q}\) is \(\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}\), and this is also a basis for \(\mathbb{Z}[\zeta_p]\) over \(\mathbb{Z}\). It is more convenient to multiply through by \(\zeta_p\) and use instead \(\mathcal{B} = \{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}\) as a basis of \(\mathbb{Q}(\zeta_p)\) over \(\mathbb{Q}\) or \(\mathbb{Z}[\zeta_p]\) over \(\mathbb{Z}\), since this is a basis of Galois conjugates (a normal basis over \(\mathbb{Q}\)). For example, \(\eta_0, \eta_1, \eta_2\) are sums of different numbers in \(\mathcal{B}\), so \(\eta_0, \eta_1,\) and \(\eta_2\) are linearly independent over \(\mathbb{Q}\) and thus form a \(\mathbb{Q}\)-basis of \(F_p\).

Each \(x \in \mathcal{O}_{F_p}\) has the form \(x = a_0\eta_0 + a_1\eta_1 + a_2\eta_2\) for \(a_0, a_1, a_2 \in \mathbb{Q}\). On the left side, since \(x\) is an algebraic integer in \(\mathbb{Q}(\zeta_p)\) it is a \(\mathbb{Z}\)-linear combination of the numbers in \(\mathcal{B}\). Expanding the right side in terms of \(\mathcal{B}\) the coefficients are \(a_0, a_1,\) and \(a_2\), so comparing coefficients of the numbers in \(\mathcal{B}\) on both sides shows \(a_0, a_1,\) and \(a_2\) are all integers. 

To measure how far \(\mathbb{Z}[\eta_0]\) is from the full ring of integers \(\mathcal{O}_{F_p}\) we'd like to compute the index \([\mathcal{O}_{F_p} : \mathbb{Z}[\eta_0]]\). This can be expressed in terms of discriminants: if \(f(T) \in \mathbb{Z}[T]\) is the minimal polynomial of \(\eta_0\) over \(\mathbb{Q}\) then

\[
\text{disc}(f(T)) = [\mathcal{O}_{F_p} : \mathbb{Z}[\eta_0]]^2 \text{disc}(\mathcal{O}_{F_p}).
\]

What are these discriminants?

**Theorem 4.** For \(p \equiv 1 \mod 3\), \(\text{disc}(\mathcal{O}_{F_p}) = p^2\).

**Proof.** The discriminant of \(\mathcal{O}_{F_p}\) is the \(3 \times 3\) determinant

\[
\begin{vmatrix}
\text{Tr}(\eta_0^2) & \text{Tr}(\eta_0\eta_1) & \text{Tr}(\eta_0\eta_2) \\
\text{Tr}(\eta_1\eta_0) & \text{Tr}(\eta_1^2) & \text{Tr}(\eta_1\eta_2) \\
\text{Tr}(\eta_2\eta_0) & \text{Tr}(\eta_2\eta_1) & \text{Tr}(\eta_2^2)
\end{vmatrix},
\]

where \(\text{Tr} = \text{Tr}_{F_p/\mathbb{Q}}\). Since \(\eta_0, \eta_1, \eta_2\) are \(\mathbb{Q}\)-conjugates, as are \(\eta_0\eta_1, \eta_0\eta_2,\) and \(\eta_1\eta_2\), we have

\[
\text{disc}(\mathcal{O}_{F_p}) = \begin{vmatrix}
\text{Tr}(\eta_0^2) & \text{Tr}(\eta_0\eta_1) & \text{Tr}(\eta_0\eta_2) \\
\text{Tr}(\eta_0\eta_1) & \text{Tr}(\eta_1^2) & \text{Tr}(\eta_1\eta_2) \\
\text{Tr}(\eta_0\eta_2) & \text{Tr}(\eta_2\eta_1) & \text{Tr}(\eta_2^2)
\end{vmatrix}
= a^3 - 3ab^2 + 2b^3,
\]

where \(a = \text{Tr}(\eta_0^2)\) and \(b = \text{Tr}(\eta_0\eta_1)\).

The trace of \(\eta_0\) is \(\text{Tr}(\eta_0) = \eta_0 + \eta_1 + \eta_2 = \sum_{(t,p) = 1} \zeta_p^t = -1\). To compute \(\text{Tr}(\eta_0^2)\), we compute

\[
\eta_0^2 = \sum_{a + b = 1} \sum_{\substack{a(p-1)/3 = 1 \ b(p-1)/3 = 1 \ a \ b \neq 1}} \zeta_p^{a+b} = \sum_{a(p-1)/3 = 1} \sum_{b(p-1)/3 = 1} \zeta_p^{a+b} = \sum_{b(p-1)/3 = 1} \sum_{a(p-1)/3 = 1} \zeta_p^{a+b} = \frac{p-1}{3} + \sum_{b(p-1)/3 = 1, b \neq 1} \sigma_1 + b(\eta_0)
\]

\[
= \frac{p-1}{3} + c_0\eta_0 + c_1\eta_1 + c_2\eta_2,
\]

where

\[
c_0 = |\{b \neq 0, -1 : b(p-1)/3 = 1, (1 + b)(p-1)/3 = 1\}|,
\]
\[
c_1 = |\{b \neq 0, -1 : b(p-1)/3 = 1, (1 + b)(p-1)/3 = r\}|,
\]
\[
c_2 = |\{b \neq 0, -1 : b(p-1)/3 = 1, (1 + b)(p-1)/3 = s\}|,
\]
\[
c_0 = p - 1 - c_1 - c_2.
\]
\[ c_2 = \{ b \neq 0, -1 : b^{(p-1)/3} = 1, (1 + b)^{(p-1)/3} = r^2 \}. \]

(Recall \( r \) and \( r^2 \) are the elements of order 3 in \( (\mathbb{Z}/p\mathbb{Z})^\times \).)

Taking the trace of both sides of (3) gives

\[ \text{Tr}(\eta_0^2) = (p - 1) + (c_0 + c_1 + c_2) \text{Tr}(\eta_0) = p - 1 - (c_0 + c_1 + c_2). \]

The sum of the \( c_i \)'s is the number of solutions to \( b^{(p-1)/3} = 1 \) in \( \mathbb{Z}/p\mathbb{Z} \) except for \( b = -1 \), so

\[ \text{Tr}(\eta_0^2) = p - 1 - \left( \frac{p - 1}{3} - 1 \right) = 2 \frac{p - 1}{3} (p - 1) + 1. \]

Writing

\[
\begin{align*}
\text{Tr}(\eta_0^2) &= \eta_0^2 + \eta_1^2 + \eta_2^2 \\
&= (\eta_0 + \eta_1 + \eta_2)^2 - 2(\eta_0\eta_1 + \eta_1\eta_2 + \eta_0\eta_2) \\
&= (\text{Tr} \eta_0)^2 - 2 \text{Tr}(\eta_0\eta_1) \\
&= 1 - 2 \text{Tr}(\eta_0\eta_1),
\end{align*}
\]

we compare (4) and (5) to see that \( \text{Tr}(\eta_0\eta_1) = -\frac{(p - 1)}{3} \).

Feeding the formulas for \( \text{Tr}(\eta_0^2) \) and \( \text{Tr}(\eta_0\eta_1) \) into the discriminant formula (2) gives

\[
\text{disc}(\mathcal{O}_{F_p}) = \left( \frac{2}{3} (p - 1) + 1 \right)^3 - 3 \left( \frac{2}{3} (p - 1) + 1 \right) \left( \frac{p - 1}{3} \right)^2 - 2 \left( \frac{p - 1}{3} \right)^3 = p^2.
\]

\[ \square \]

**Remark 5.** The discriminant of \( F_p \) can be calculated using ramification rather than a basis: the extension \( \mathbb{Q}(\zeta_p)/\mathbb{Q} \) is ramified only at \( p \), so if \( K \) is an intermediate field then it is ramified only at \( p \) too. Since \( \mathbb{Q}(\zeta_p)/\mathbb{Q} \) is totally ramified at \( p \), \( K \) is totally ramified at \( p \) as well. If a number field is totally ramified at a prime \( p \) and has degree \( n \) not divisible by \( p \) then it can be shown that its discriminant is divisible by \( p^{n-1} \) but not \( p^n \). Therefore if \( [K : \mathbb{Q}] = d \), \( \text{disc}(K) = \pm p^{d-1} \). The sign of \( \text{disc}(K) \) is \( (-1)^{r_2(K)} \) [9, Lemma 2.2], and when \( p \equiv 1 \text{ mod } 3 \) the cubic field \( F_p \) has \( r_2 = 0 \) since a Galois cubic with a real embedding has \( r_2 = 0 \), so \( \text{disc}(F_p) = p^{3-1} = p^2 \).

The first few primes \( p \equiv 1 \text{ mod } 3 \) are

\[
7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97.
\]

For every prime \( p \equiv 1 \text{ mod } 3 \) we can write \( 4p = A^2 + 27B^2 \) and such an equation determines \( A \) and \( B \) up to sign [6, p. 119]. The table below gives the positive \( A \) and \( B \) for the above \( p \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( A, B )</th>
<th>( (A, B) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>7, 13</td>
<td>(1,1), (5,1)</td>
</tr>
<tr>
<td>19</td>
<td>19, 31</td>
<td>(7,1), (4,2)</td>
</tr>
<tr>
<td>31</td>
<td>31, 37</td>
<td>(11,1), (8,2)</td>
</tr>
<tr>
<td>43</td>
<td>43, 61</td>
<td>(13,1), (5,3)</td>
</tr>
<tr>
<td>67</td>
<td>67, 73</td>
<td>(7,3), (17,1)</td>
</tr>
<tr>
<td>79</td>
<td>79, 97</td>
<td>(19,1)</td>
</tr>
</tbody>
</table>

Numerically, for each of the above \( p \) a calculation of \( f(T) \) as \( (T - \eta_0)(T - \eta_1)(T - \eta_2) \) shows the discriminant of \( f(T) \) is \( (pB)^2 \). By (1) and Theorem 4, the formula \( \text{disc}(f(T)) = (pB)^2 \) is equivalent to \( [\mathcal{O}_{F_p} : \mathbb{Z}[\eta_0]] = |B| \), so by the above table \( \mathbb{Z}[\eta_0] \) has index 2 in \( \mathcal{O}_{F_p} \) when \( p \) is 31 and 43, the index is 3 when \( p \) is 61, 67, and 73, and the index is 1 (i.e., \( \mathcal{O}_{F_p} = \mathbb{Z}[\eta_0] \)) for the other \( p \) in the table. For a more rigorous discussion of the formula \( \text{disc}(f(T)) = (pB)^2 \), see [4]. Claude Quitte observed numerically for the above \( p \) an index formula using \( A \): \( [\mathcal{O}_{F_p} : \mathbb{Z}[\eta_0 - \eta_1]] = |A| \).
The formula \( \text{disc}(f(T)) = (pB)^2 \) leads to a formula for \( f(T) \). In terms of its roots \( \eta_i \),

\[
\begin{align*}
f(T) &= (T - \eta_0)(T - \eta_1)(T - \eta_2) \\
&= T^3 - (\eta_0 + \eta_1 + \eta_2)T^2 + (\eta_0\eta_1 + \eta_0\eta_2 + \eta_1\eta_2)T - \eta_0\eta_1\eta_2 \\
&= T^3 - \text{Tr}(\eta_0)T^2 + \text{Tr}(\eta_0\eta_1)T - \eta_0\eta_1\eta_2 \\
&= T^3 - (-\eta_0)T^2 - \frac{1}{3}T - \eta_0\eta_1\eta_2 \\
&= T^3 + T^2 - \frac{p-1}{3}T - \eta_0\eta_1\eta_2.
\end{align*}
\]

We want to write the constant term of \( f(T) \) in terms of \( p \). The general formula

\[
\text{disc} \left( T^3 + T^2 + aT + b \right) = -4a^3 + a^2 + 18ab - 27b^2 - 4b
\]

with \( a = -(p-1)/3 \) and \( b = -\eta_0\eta_1\eta_2 \) is

\[
\frac{4}{27}p^3 - \frac{1}{3}p^2 + \left( \frac{2}{9} - 6b \right)p - 27b^2 + 2b - \frac{1}{27} = \frac{p^2}{27} \left( 4p - 9 - \frac{6(27b - 1)}{p} - \frac{(27b - 1)^2}{p^2} \right)
\]

\[
= \frac{p^2}{27} \left( 4p - \left(3 + \frac{27b - 1}{p} \right)^2 \right).
\]

Setting \( 4p = A^2 + 27B^2 \), this discriminant is

\[
\frac{p^2}{27} \left( A^2 + 27B^2 - \left(3 + \frac{27b - 1}{p} \right)^2 \right) = \frac{p^2}{27} \left( A^2 - \left(3 + \frac{27b - 1}{p} \right)^2 \right) + (pB)^2.
\]

Therefore

\[
\text{disc}(f(T)) = (pB)^2 \iff 3 + \frac{27b - 1}{p} = \pm A.
\]

Since \( p \equiv 1 \text{ mod } 3 \) we have \( 3 + (27b - 1)/p \equiv -1 \text{ mod } 3 \), so if we choose the sign on \( A \) to make \( A \equiv 1 \text{ mod } 3 \) then \( 3 + (27b - 1)/p = -A \). Rewrite this as \( b = (1 - p(A + 3))/27 \), so the minimal polynomial of \( \eta_0 \) over \( \mathbb{Q} \) is

\[
(6) \quad f(T) = T^3 + T^2 - \frac{p-1}{3}T + \frac{1-p(A+3)}{27}
\]

with \( 4p = A^2 + 27B^2 \) and \( A \equiv 1 \text{ mod } 3 \).

**Example 6.** The first \( p \) fitting the hypotheses of Theorem 1 is \( p = 31 \), for which \( 4p = 124 = (4)^2 + 27(2)^2 \). Therefore the cubic subfield of \( \mathbb{Q}(\zeta_{31}) \) is \( \mathbb{Q}(\eta_0) \) where, by (6), \( \eta_0 \) has minimal polynomial

\[
T^3 + T^2 - \frac{31-1}{3}T + \frac{1-31(4+3)}{27} = T^3 + T^2 - 10T - 8.
\]

The field \( \mathbb{Q}(\eta_0) \) is a cyclic cubic extension of \( \mathbb{Q} \) in which 2 splits completely and its ring of integers has no power basis.

**Example 7.** The second \( p \) fitting the hypotheses of Theorem 1 is \( p = 43 \), for which \( 4p = 172 = (-8)^2 + 27(2)^2 \) (we use \(-8 \) so that \( A = -8 \equiv 1 \text{ mod } 3 \)). Thus the cubic subfield of \( \mathbb{Q}(\zeta_{43}) \) is \( \mathbb{Q}(\eta_0) \) where \( \eta_0 \) has minimal polynomial

\[
T^3 + T^2 - \frac{43-1}{3}T + \frac{1-43(-8+3)}{27} = T^3 + T^2 - 14T + 8
\]

and this cubic field has the same properties as at the end of the previous example.
The minimal polynomial of $\eta_0 - \eta_1$ over $\mathbb{Q}$ is $(T - (\eta_0 - \eta_1))(T - (\eta_1 - \eta_2))(T - (\eta_2 - \eta_0))$. Expanding this out, we get
\begin{equation}
T^3 + (\eta_0\eta_1 + \eta_0\eta_2 + \eta_1\eta_2 - \eta_0^2 - \eta_1^2 - \eta_2^2)T + (\eta_0 - \eta_1)(\eta_1 - \eta_2)(\eta_2 - \eta_0).
\end{equation}
The coefficient of $T$ is $3 \text{Tr}(\eta_0\eta_1) - (\text{Tr} \eta_0)^2 = -3(p - 1)/3 - (-1)^2 = -p$ and the constant term is $\sqrt{\text{disc}(f(T))} = \pm |B|$. The sign of the constant term in (7) is sensitive to the choice of $\zeta_p$ and nontrivial cube root of unity $r \mod p$ in the definition of the $\eta_i$, e.g., changing $r$ can change $\eta_1$ into $\eta_2$ but $\eta_0 - \eta_1$ and $\eta_0 - \eta_2$ are not $\mathbb{Q}$-conjugates. In fact $\eta_0 - \eta_2$ has minimal polynomial $T^3 - pT + p|B|$ with constant term of opposite sign to the minimal polynomial of $\eta_0 - \eta_1$. When the definition of the $\eta_i$ uses $\zeta_p = e^{2\pi i/p}$ and $r$ is the numerically least nontrivial cube root of unity $\mod p$ in $\{1, \ldots, p - 1\}$ then for all $p < 100$ such that $p \equiv 1 \mod 3$ the constant term of (7) turns out to be $p|B|$ except when $p = 61$.

The only $p < 500$ for which $p \equiv 1 \mod 3$ and the class number of $F_p$ is greater than 1 are 163, 277, 313, 349, and 397. For these $p$ the class group of $F_p$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ except for $p = 313$, when it is $\mathbb{Z}/7\mathbb{Z}$.

\textbf{References}