Genus theory and the factorization of class equations over $\mathbb{F}_p$

Patrick Morton

Aug. 30, 2014

As is well-known, the Hilbert class equation is the polynomial $H_D(X)$ whose roots are the distinct $j$-invariants of elliptic curves with complex multiplication by the maximal order $\mathcal{O}_K$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. A root of $H_D(X)$ generates the Hilbert class field $\Sigma$ of $K$ over $K$. The polynomial $H_D(X)$ always has a real root $\xi$, and over $\mathbb{Q}$ this root generates the real subfield $\Sigma_0 = \mathbb{Q}(\xi)$ of $\Sigma$. Recently, Stankewicz [st] found a criterion for the polynomial $H_D(X)$ to have a root (mod $p$), for a given odd prime $p$ for which the Legendre symbol $(D/p) = -1$. This criterion can be stated as follows.

Theorem (Stankewicz). If $p$ is an odd prime for which $(D/p) = -1$, and $p$ does not divide the discriminant of $H_D(X)$, then $H_D(X)$ has a linear factor over $\mathbb{F}_p$ if and only if

$$\left(\frac{-p}{q}\right) = 1, \quad \forall \ q | D, \ q \text{ an odd prime.}$$

Stankewicz derives this criterion from his analysis of rational $p$-adic points on twists of Shimura curves. In this note I give a more direct proof of the criterion using genus theory and basic properties of the Hilbert class field. The proof shows that the above theorem fits naturally into a discussion of genus theory. (See [co], [has2], and [ish].)

1 Necessity.

In this and the next section the integer $-N$ will denote the square-free part of the fundamental quadratic discriminant $D$, and $K$ is the imaginary quadratic field
$K = \mathbb{Q}(\sqrt{-N})$ with discriminant $D$.

**Theorem 1.** Let $\Sigma_0$ denote the real subfield of the Hilbert class field $\Sigma$ of the quadratic field $K = \mathbb{Q}(\sqrt{-N})$. Assume $p$ is an odd prime for which $\left(\frac{-N}{p}\right) = -1$. If $p$ has a prime divisor $p'$ of degree 1 in $\Sigma_0$, then

$$\left(\frac{-p}{q}\right) = 1, \ \forall \ q | N, \ q \text{ an odd prime.}$$

To prove this we use the decomposition

$$D = \prod_{q | D} q^*, \ q^* = (-1)^{(q-1)/2}q, \ q \text{ odd, } 2^* = -4, 8, -8,$$  

where the product is over all the prime divisors of $D$.

The genus field of $K$ is the field $\Omega$, which is obtained by adjoining all the square-roots $\sqrt{q^*}$ to $K$, as $q$ varies over the prime divisors of $D$. It is the largest unramified extension of $K$ which is abelian over $\mathbb{Q}$, so that $\Omega \subseteq \Sigma$.

Assume that the odd prime $p$ has a first degree prime divisor in $\Sigma_0$. The conditions $\left(\frac{-N}{p}\right) = -1$ and $p$ odd imply that $p$ does not divide $D$, and $p$ has a first degree prime divisor in every subfield of $\Sigma_0$. If $q$ is a prime $\equiv 1 \pmod{4}$, then $q^* = q$, so $\mathbb{Q}(\sqrt{q}) \subseteq \Sigma_0$. Hence, $p$ has a first degree prime divisor in $\mathbb{Q}(\sqrt{q})$, which implies that

$$\left(\frac{q}{p}\right) = 1, \ q \equiv 1 \pmod{4}, \ q | N. \quad (1.1)$$

This implies then that

$$\left(\frac{-p}{q}\right) = 1, \ q \equiv 1 \pmod{4}, \ q | N. \quad (1.2)$$

If $2 | D$ and $2^* = 8$, the same argument also gives $\left(\frac{2}{p}\right) = 1$, so $p \equiv \pm 1 \pmod{8}$.

On the other hand, if there are several primes $q_i \equiv 3 \pmod{4}$, $i = 1, 2$, then $\sqrt{q_1q_2} \in \Sigma$ implies that $\sqrt{q_1q_2} = \sqrt{q_1q_2} \in \Sigma_0$. Then $p$ has a first degree prime divisor in $\mathbb{Q}(\sqrt{q_1q_2})$, so we have

$$\left(\frac{q_1q_2}{p}\right) = 1, \ q_i \equiv 3 \pmod{4}, \ q_i | N.$$
It follows that
\[
\left( \frac{q_1^*}{p} \right) = \left( \frac{q_2^*}{p} \right), \quad q_1 \equiv q_2 \equiv 3 \pmod{4}, \quad q_i | N. \quad (1.3)
\]

We get a similar conclusion when \(2 | D\) and \(2^* = -4, -8\), namely
\[
\left( \frac{2^*}{p} \right) = \left( \frac{q^*}{p} \right), \quad 2^* = -4, -8, \quad q \equiv 3 \pmod{4}, \quad q | N. \quad (1.4)
\]

Now we use the fact that
\[
\left( \frac{D}{p} \right) = \left( \frac{-N}{p} \right) = \prod_{q | D} \left( \frac{q^*}{p} \right) = -1. \quad (1.5)
\]

From (1.1), (1.3), (1.4) the terms with \(q \equiv 1 \pmod{4}\) or \(q^* = 8\) drop out, and we are left with
\[
\left( \frac{q^*}{p} \right)^r = -1,
\]
where \(r\) is the number of prime divisors of \(D\) with \(q \equiv 3 \pmod{4}\) or \(q^* = -4, -8\).

But this implies that \(r\) is odd and \(\left( \frac{q^*}{p} \right) = -1\) for all these prime divisors. Hence,
\[
\left( \frac{-p}{q} \right) = 1, \quad \text{if} \ q \equiv 3 \pmod{4}, \ q | N.
\]

Together with (1.2), this proves Theorem 1. □

**Corollary 1.** If \(p\) does not divide the discriminant of \(H_D(X)\), \(\left( \frac{-N}{p} \right) = -1\), and \(H_D(X) \pmod{p}\) has a root in \(\mathbb{F}_p\), then
\[
\left( \frac{-p}{q} \right) = 1, \quad \forall \ q | N, \ q \text{ an odd prime.}
\]

**Proof.** Since \(p\) does not divide the discriminant of \(H_D(X)\) and a real root of \(H_D(X)\) generates \(\Sigma_0\), it is clear that the factors of \(H_D(X) \pmod{p}\) correspond 1-1 to the prime divisors of \(p\) in \(\Sigma_0\). The corollary is now immediate from Theorem 1. □
2 Sufficiency.

Now we prove the converse of Theorem 1:

**Theorem 2.** Let $\Sigma_0$ denote the real subfield of the Hilbert class field $\Sigma$ of the quadratic field $K = \mathbb{Q}(\sqrt{-N})$. Assume $p$ is an odd prime for which $\left(\frac{-N}{p}\right) = -1$. If $p$ satisfies the condition

$$\left(\frac{-p}{q}\right) = 1, \quad \forall \, q|N, \, q \text{ an odd prime},$$

then $p$ has a prime divisor $\mathfrak{p}$ of degree 1 in $\Sigma_0$. □

To prove this we consider the decomposition group of a prime divisor $\mathfrak{P}$ of $p$ in $\Sigma$. First we note that if $\left(\frac{-p}{q}\right) = 1$ for all odd prime divisors $q$ of $N$, then (1.1) holds, as does

$$\left(\frac{q^*}{p}\right) = -1, \quad q \equiv 3 \pmod{4}, \, q|N, \, q \text{ prime.}$$

Now (1.5) implies that

$$\left(\frac{2^*}{p}\right) = (-1)^{r-1} \cdot (-1) = (-1)^r, \quad \text{if } 2|D,$$

where $r - 1$ is the number of primes $q \equiv 3 \pmod{4}$ dividing $N$. But if $2|D$, then either:

$N \equiv 1 \pmod{4}$, in which case $2^* = -4$ and $r - 1$ is even, so that $r$ is odd, implying that $\left(\frac{2^*}{p}\right) = \left(\frac{-4}{p}\right) = -1$;

$N \equiv 2 \pmod{8}$, in which case $2^* = -8$ and $r$ is again odd, giving $\left(\frac{2^*}{p}\right) = \left(\frac{-8}{p}\right) = -1$;

or $N \equiv 6 \pmod{8}$, in which case $2^* = 8$ and $r - 1$ is odd, giving $\left(\frac{2^*}{p}\right) = \left(\frac{8}{p}\right) = 1$.

Thus, if $2|D$, we have (1.4) and the assertion in the sentence following (1.2). This shows that $p$ splits completely in the real subfield $\Omega_0$ of the genus field $\Omega$. (Note
that \([\Omega : K] = 2^{t-1}\), where \(t\) is the number of distinct prime factors of \(D\). Thus \([\Omega_0 : \mathbb{Q}] = 2^{t-1}\), as well.) Hence, the decomposition field of any prime divisor \(\mathfrak{P}\) of \(p\) in \(\Sigma\) contains the field \(\Omega_0\), and therefore the decomposition group \(G_{\mathfrak{P}}\) is contained in \(H = \text{Gal}(\Sigma/\Omega_0)\).

I claim that it suffices to show \(G_{\mathfrak{P}} = \{1, \tau\}\) for some \(\mathfrak{P}|p\), where \(\tau\) is complex conjugation. If this holds, then \(\Sigma_0\), which is the fixed field of \(\tau\), is the largest field in which the prime below \(\mathfrak{P}\) has degree 1, i.e. \(p = \mathfrak{P}\mathfrak{P}^\tau\) is a first degree prime divisor of \(p\) in \(\Sigma_0\).

Let \(J = H \cap \text{Gal}(\Sigma/K)\) be the subgroup of \(\text{Gal}(\Sigma/K)\) corresponding to \(\Omega\) in the Galois correspondence, so that \([H : J] = 2\) and \(H = J \cup J\tau\). By the genus theory \([h]\), \(J\) corresponds to the subgroup of squares in \(\text{Pic}(R_K)\), in the Artin correspondence between ideal classes in \(R_K\) and elements of the Galois group \(\text{Gal}(\Sigma/K)\).

We now have what we need to complete the proof. The decomposition group \(G_{\mathfrak{P}}\) is a subgroup of \(H\) of order 2. This is because \(p\) is inert in \(K\), so that \((p) = pR_K\) is a principal ideal and therefore \(p\) splits completely in the extension \(\Sigma/K\). Furthermore, we know that \(K\) is not contained in the decomposition field of any \(\mathfrak{P}\), and therefore \(G_{\mathfrak{P}} \not\subset J \subset \text{Gal}(\Sigma/K)\). Hence, \(G_{\mathfrak{P}} \subset H\) is generated by some \(\sigma\tau\), with \(\sigma \in J\).

But \(\sigma = \psi^2\) for some \(\psi \in \text{Gal}(\Sigma/K)\), by the characterization of the group \(J\), and \(\psi^{-1}G_{\mathfrak{P}}\psi = G_{\mathfrak{P}\psi} = \{1, \psi^{-1}\sigma\tau\psi\}\), with \(\psi^{-1}\sigma\tau\psi = \psi^{-2}\sigma\tau = \tau\). This shows that \(G_{\mathfrak{P}\psi} = \{1, \tau\}\) and completes the proof. 

**Corollary 2.** If \(p\) satisfies \((\frac{-N}{p}) = -1\) and \((\frac{-p}{q}) = 1\), for all odd primes \(q\) such that \(q|N\), then \(H_D(X) \pmod{p}\) has a root in \(\mathbb{F}_p\).

**Proof.** Theorem 2 implies that \(H_D(X)\) has a linear factor over \(\mathbb{Q}_p\) and therefore \(H_D(X) \pmod{p}\) has a root in \(\mathbb{F}_p\). 

The proof of Theorem 2 shows that when \(p\) has a first degree prime divisor \(p\) in \(\Sigma_0\), then it has as many prime divisors of degree 1 as there are distinct elements \(\psi\) in \(\text{Gal}(\Sigma/K)\) for which \(G_{\mathfrak{P}_\psi} = \psi^{-1}G_{\mathfrak{P}}\psi = \{1, \tau\}\), where \(\mathfrak{P}|p\). This holds if and only if \(\psi^{-1}\tau\psi = \tau\), i.e., if and only if \(\psi^2 = 1\). The number of such elements \(\psi\) is exactly \(2^{t-1}\), since this is the order of the 2-Sylow subgroup of the class group \(\text{Pic}(R_K)\). Thus we have:

**Theorem 3.** If \(p\) is an odd prime for which \((\frac{-N}{p}) = -1\), and \(p\) has a prime divisor of degree 1 in \(\Sigma_0\), then it has exactly \(2^{t-1}\) such prime divisors, where \(t\) is the number of distinct prime factors of \(D\). 

□
Taken together, Theorems 1-3 yield the following Decomposition Law for the real subfield $\Sigma_0$ of $\Sigma$.

**Prime Decomposition Law in $\Sigma_0$.** Let $p$ be an odd prime that does not divide $D$.

(a) If $\left(\frac{D}{p}\right) = 1$, then in $\Sigma_0$, $p$ splits into $h(D)/f$ primes of degree $f$ over $\mathbb{Q}$, where $f$ is the order of a prime ideal divisor $\varphi$ of $p$ in $Pic(R_K)$.

(b) If $\left(\frac{D}{p}\right) = -1$ and $\left(\frac{-p}{q}\right) = 1$ for all odd prime divisors $q$ of $D$, then in $\Sigma_0$, $p$ splits into $r_1 = 2^{t-1}$ primes of degree 1 and $r_2 = (h(D) - 2^{t-1})/2$ primes of degree 2 over $\mathbb{Q}$.

(c) If $\left(\frac{D}{p}\right) = -1$ and $\left(\frac{-p}{q}\right) = -1$ for some odd prime divisor $q$ of $D$, then in $\Sigma_0$, $p$ splits into $h(D)/2$ primes of degree 2 over $\mathbb{Q}$. $\square$

This law immediately implies the following density result.

**Theorem 4.** The density of primes $p \in \mathbb{Z}^+$ for which $H_D(X)$ has a linear factor (mod $p$) is $d(P(\Sigma_0)) = \frac{1}{2h(D)} + \frac{1}{2^t}$, where $t$ is the number of distinct prime factors of $D$.

**References.**

[co] D. A. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley and Sons, New York, 1989.

[hak1] F. Halter-Koch, Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe, J. Number Theory 3 (1971), 412-443.

[hak2] F. Halter-Koch, Geschlechtertheorie der Ringklassenkörper, J. reine angew. Math. 250 (1971), 107-108.

[hak3] F. Halter-Koch, Eine allgemeine Geschlechtertheorie und ihre Anwendung auf Teilbarkeitsaussagen für Klassenzahlen algebraischer Zahlkörper, Math. Annalen 233 (1978), 55-63.

[has1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, I, Ia, II, Physica Verlag, Würzburg-Vienna, 1970.
[has2] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörpern, J. Math. Soc. Japan 3 (1951), 45-51.

[ish] M. Ishida, The Genus Fields of Algebraic Number Fields, Lecture Notes in Mathematics 555, Springer, Berlin, 1976.

[st] J. Stankewicz, Twists of Shimura curves, Canad. J. Math. 66 (2014), 924-960; and at http://arxiv.org/abs/1208.3594

Dept. of Mathematical Sciences
Indiana University - Purdue University at Indianapolis (IUPUI)
402 N. Blackford St., Indianapolis, IN, USA 46202
\textit{e-mail: pmorton@math.iupui.edu}