Note on a polynomial of Emma Lehmer

Henri Darmon

September 9, 2007

1 Abstract

In [Leh], Emma Lehmer constructed a parametric family of units in real quintic fields of prime conductor $p = t^4 + 5t^3 + 15t^2 + 25t + 25$, as translates of Gaussian periods. Later, Schoof and Washington [SW] showed that these units were fundamental units. In this note, we observe that Lehmer's family comes from the covering of modular curves $X_1(25) \longrightarrow X_0(25)$. This gives a conceptual explanation for the existence of Lehmer's units: they are modular units (which have been studied extensively, for example in [K-L]). By relating Lehmer's construction with ours, one finds expressions for certain Gauss sums as values of modular units on $X_1(25)$.

2 Lehmer's polynomial

Throughout the discussion, we fix a choice $\{\zeta_n\}$ of primitive nth roots of unity for each n, say by $\zeta_n = e^{2\pi i/n}$.

Let

$$\begin{aligned} P_5(Y,T) &= Y^5 + T^2Y^4 - 2(T^3+3T^2+5T+5)Y^3 + \\ &\quad (T^4+5T^3+11T^2+15T+5)Y^2 + \\ &\quad (T^3+4T^2+10T+10)Y + 1 \end{aligned} \tag{1}$$

[1]Partially supported by a Doctoral Fellowship from the Natural Sciences and Engineering Research Council of Canada (NSERC).

[2]I wish to thank Dan Abramovich and Noam Elkies for some interesting discussions.

be the quintic polynomial constructed in [Leh]. The discriminant of $P_5(Y, T)$, viewed as a polynomial in Y with coefficients in $\mathbf{Q}(T)$, is

$$D(T) = (T^3 + 5T^2 + 10T + 7)^2(T^4 + 5T^3 + 15T^2 + 25T + 25)^4.$$

The projective curve C in $\mathbf{P}_2$ defined by the affine equation (1) has three nodal singularities whose T-coordinates are the roots of the first factor of $D(T)$. The points (y, t), where t is a root of the second factor, are branch points for the covering of C onto the T-line.

As shown in [Leh] the polynomial $P_5(Y, T)$ defines a regular Galois extension of $\mathbf{Q}(T)$ with Galois group $\mathbf{Z}/5\mathbf{Z}$. By the analysis above, it is ramified at the four conjugate points $T = -\sqrt{5}\zeta_5$, $\sqrt{5}\zeta_5^2$, $-\sqrt{5}\zeta_5^{-1}$, $\sqrt{5}\zeta_5^{-2}$, satisfying the minimal polynomial

$$T^4 + 5T^3 + 15T^2 + 25T + 25.$$

(Here $\sqrt{5}$ denotes the positive square root.) If $t \in \mathbf{Z}$ is chosen so that

$$p = t^4 + 5t^3 + 15t^2 + 25t + 25$$

is prime, (hence in particular $p \equiv 1 \bmod 5$), then the roots $r_1, \ldots, r_5$ of $P_5(Y, t)$ are translates of Gaussian periods:

$$r_i = (\frac{t}{5})\eta_i + [(\frac{t}{5}) - t^2]/5,$$

where

$$\eta_j = \sum_{x \in \Gamma_j} \zeta_p^x,$$

and Γ_j denotes the jth coset of $(\mathbf{Z}/p\mathbf{Z})^{*5}$ in $(\mathbf{Z}/p\mathbf{Z})^*$.

Since C admits a five-to-one map to $\mathbf{P}_1$ which is totally ramified at four points, the geometric genus of C is 4 by the Riemann-Hurwitz theorem. On the other hand, C is realized as a plane curve of degee $d = 6$, and its arithmetic genus is $(d-1)(d-2)/2 = 10$. Let C' denote the normalization of C; it is a smooth projective curve of genus 4. The covering $C' \longrightarrow \mathbf{P}_1$ defines a Galois covering of $\mathbf{P}_1$ with Galois group $\mathbf{Z}/5\mathbf{Z}$, and has the following properties:

1. It is ramified only over the four closed points in $R = \{-\sqrt{5}\zeta_5, \sqrt{5}\zeta_5^2, -\sqrt{5}\zeta_5^{-1}, \sqrt{5}\zeta_5^{-2}\}$.

2. The closed points of the fiber above $\infty \in \mathbf{P}_1$ are rational.

Proposition 2.1 *The properties 1 and 2 determine the covering C' uniquely up to $\mathbf{Q}$-isomorphism.*

Proof: Let $(\mathbf{P}_1 - R)$ be the projective line with the points of R removed, viewed as a curve over $\bar{\mathbf{Q}}$. The space $V = H^1_{et}(\mathbf{P}_1 - R, \mathbf{Z}/5\mathbf{Z})$ is a vector space of dimension 3 over $\mathbf{F}_5$, and is endowed with a natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. In fact, one has

$$V = H^1_{et}(\mathbf{P}_1 - R, \mu_5) \otimes \mu_5^{-1},$$

where μ_5 denotes the group scheme of 5th roots of unity. By Kummer theory, $H^1_{et}(\mathbf{P}_1 - R, \mu_5)$ is identified with the subspace of $\bar{\mathbf{Q}}(T)^*/\bar{\mathbf{Q}}(T)^{*5}$ spanned by the elements

$$\begin{array}{ll} (T + \zeta_5\sqrt{5})/(T - \zeta_5^2\sqrt{5}), & (T - \zeta_5^2\sqrt{5})/(T + \zeta_5^{-1}\sqrt{5}), \\ (T + \zeta_5^{-1}\sqrt{5})/(T - \zeta_5^{-2}\sqrt{5}), & (T - \zeta_5^{-2}\sqrt{5})/(T + \zeta_5\sqrt{5}), \end{array}$$

whose product is 1. Hence the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $H^1_{et}(\mathbf{P}_1 - R, \mu_5)$ factors through $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$, and is isomorphic to the regular representation of $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$ minus the trivial representation. It follows that V decomposes as a direct sum of three irreducible one-dimensional Galois representations,

$$V = V_0 \oplus V^{\omega} \oplus V^{\omega^2},$$

where V_0 is the trivial representation, and V^{ω}, V^{ω^2} denote one dimensional spaces on which $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$ acts via the Teichmuller character ω and the square of the Teichmuller character ω^2 respectively. In particular, V_0 is the unique one-dimensional subspace of V which is fixed by $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. But the cyclic quintic coverings of $\mathbf{P}_1$ which are Galois over $\mathbf{Q}$ and unramified outside R correspond exactly to such subspaces. Hence the property 1 determines C' uniquely as a curve over $\bar{\mathbf{Q}}$. (Alternately, one could use the "rigidity criterion" of Matzat, cf. [M, p. 368].) It is not hard to see that there is a unique rational form of the covering C' such that the closed points above $\infty \in \mathbf{P}_1$ are all rational (twisting this rational form by a cocycle c in $H^1(\mathbf{Q}, \mathrm{Aut}\,(C'/\mathbf{P}_1))$ will cause these points to be defined over the larger extension "cut out" by c). Thus, property 2 determines $C' \longrightarrow \mathbf{P}_1$ up to $\mathbf{Q}$-isomorphism.

3 A modular covering interpretation of Lehmer's quintic

We assume in this section some basic facts about modular forms and the geometry of modular curves. A good reference for this material is [Ogg].

Let $X_0(25)$ and $X_1(25)$ denote the modular curves of level 25, compactified by adjoining a finite set of cusps. The curve $X_0(25)$ is of genus 0 and is isomorphic to $\mathbf{P}_1$ over $\mathbf{Q}$. The covering $X_1(25) \longrightarrow X_0(25)$ is Galois with Galois group canonically isomorphic to $G = (\mathbf{Z}/25\mathbf{Z})^*/ < \pm 1 >$. The quotient X of $X_1(25)$ by the involution $7 \in G$ gives a cyclic covering of $X_0(25)$ of degree 5.

Let $T_5 = \eta(z)/\eta(25z)$, $F_5 = (\eta(z)/\eta(5z))^6$ be Hauptmoduls for $X_0(25)$ and $X_0(5)$ respectively. One has:

$$F_5 = T_5^5/(T_5^4 + 5T_5^3 + 15T_5^2 + 25T_5 + 25).$$

The curve $X_0(5)$ has two cusps C_1 and C_2 corresponding to the values $F_5 = 0$ and $F_5 = \infty$ respectively. Hence $X_0(25)$ has six cusps: a unique one lying above C_1, corresponding to $T_5 = 0$; and five cusps above C_2, given by $T_5 = \infty$, $-\sqrt{5}\zeta_5$, $\sqrt{5}\zeta_5^2$, $-\sqrt{5}\zeta_5^{-1}$, $\sqrt{5}\zeta_5^{-2}$ (cf. [K]). The covering $X \longrightarrow X_0(25)$ is ramified at the four non-rational cusps, and the fiber above the cusp $T_5 = \infty$ is composed of rational points (cf. [K, p. 226]). By proposition 2.1, X can be described by Lehmer's quintic; the roots $r_1, \ldots, r_5$ of $P_5(Y, T_5)$ are modular functions on $X_1(25)$ (in fact, on X) with divisor supported at the P_i, where $P_1, \ldots, P_5$ are the closed points of X which lie above the cusp $T_5 = \infty$ of $X_0(25)$. By using Hensel's lemma to solve explicitly the equation $P_5(Y, T_5) = 0$, one obtains the following q-expansions for the r_i:

$$\begin{aligned} r_1 &= -q^3 + q^4 + q^{10} - q^{11} - q^{12} + q^{13} - q^{15} + q^{17} + \cdots \\ r_2 &= q^{-1} + 1 + q^6 + q^7 - q^{10} - q^{11} + \cdots \\ r_3 &= -q - q^3 + q^4 + q^6 - q^{12} - q^{14} + q^{18} + q^{20} \cdots \\ r_4 &= -q^{-2} - q - q^2 - q^5 + q^{15} + q^{17} + q^{18} \cdots \\ r_5 &= q^{-1} + q^5 + q^7 - q^8 - q^{12} + q^{13} - q^{14} + \cdots \end{aligned} \tag{2}$$

By [SW, p. 548], the transformation

$$r \mapsto \frac{(T_5 + 2) + T_5 r - r^2}{1 + (T_5 + 2)r}$$

permutes the roots of $P(Y, T_5)$ cyclically; one can thus label the r_i in such a way that a generator of $\mathrm{Gal}(X/X_0(25)) \simeq \mathbf{Z}/5\mathbf{Z}$ sends r_i to r_{i+1}, where the subscripts are taken modulo 5. The five cusps of X lying above the cusp $T_5 = \infty$ are permuted cyclically by the Galois group of X over $X_0(25)$. By considering the q-expansions above, we may fix a labelling of the cusps $P_1, \ldots, P_5$ so that a generator of $\mathrm{Gal}(X/X_0(25))$ sends P_i to P_{i+1} and such that:

$$\mathrm{Divisor}(r_1) = 3P_1 - P_2 + P_3 - 2P_4 - P_5.$$

Now, let a belong to $\mathbf{Z}/25\mathbf{Z}$, and define

$$\wp_a(\tau) = \wp(a/25; \tau),$$

where

$$\wp(z;\tau) = \frac{1}{z^2} + \sum_{(m,n)\in\mathbf{Z}^2-0} \frac{1}{(z-n-m\tau)^2} - \frac{1}{(n+m\tau)^2}$$

is the Weierstrass $\wp$-function. It is well-known that the functions

$$\wp_{a,b}(\tau) = \wp_a(\tau) - \wp_b(\tau)$$

are modular units on $X_1(25)$. The divisors of these functions are computed in [K]. In particular, we find that

$$\mathrm{Divisor}\left(\frac{\wp_{7,9}\wp_{6,3}\wp_{1,12}\wp_{8,4}}{\wp_{1,3}\wp_{7,4}\wp_{6,7}\wp_{8,1}}\right) = 3P_1 - P_2 + P_3 - 2P_4 - P_5,$$

where the P_i denote the cusps on X which are above the cusp ∞ of $X_0(25)$. By expressing the function on the left in terms of so-called Klein forms $t_{(a_1,a_2)}$ (cf. [K-L]), the above simplifies to give:

$$\mathrm{Divisor}\left(\frac{t_{(0,1)}t_{(0,7)}}{t_{(0,9)}t_{(0,12)}}\right) = 3P_1 - P_2 + P_3 - 2P_4 - P_5.$$

Let us abbreviate $t_{(0,a)}$ to t_a. By comparing divisors and q-expansions, one finds the following infinite product expressions for the r_i:

$$r_1 \quad = \quad \frac{t_1 t_7}{t_9 t_{12}}(25\tau) = -q^3 \prod_{n\equiv\pm1,\pm7(25)} (1-q^n) / \prod_{n\equiv\pm9,\pm12(25)} (1-q^n)$$

$$
\begin{aligned}
r_2 &= \frac{t_2 t_{11}}{t_1 t_7}(25\tau) = q^{-1} \prod_{n\equiv \pm 2, \pm 11 (25)} (1-q^n) / \prod_{n\equiv \pm 1, \pm 7 (25)} (1-q^n), \\
r_3 &= \frac{t_4 t_3}{t_{11} t_2}(25\tau) = -q \prod_{n\equiv \pm 4, \pm 3 (25)} (1-q^n) / \prod_{n\equiv \pm 11, \pm 2 (25)} (1-q^n) \\
r_4 &= \frac{t_8 t_6}{t_3 t_4}(25\tau) = -q^{-2} \prod_{n\equiv \pm 8, \pm 6 (25)} (1-q^n) / \prod_{n\equiv \pm 3, \pm 4 (25)} (1-q^n) \\
r_5 &= \frac{t_9 t_{12}}{t_6 t_8}(25\tau) = q^{-1} \prod_{n\equiv \pm 9, \pm 12 (25)} (1-q^n) / \prod_{n\equiv \pm 6, \pm 8 (25)} (1-q^n)
\end{aligned}
$$

The Galois group $\mathrm{Gal}(X_1(25)/X_0(25)) = (\mathbf{Z}/25\mathbf{Z})^*/ < \pm 1 >$ acts on the t_a by multiplying the subscripts (which are viewed as belonging to $(\mathbf{Z}/25\mathbf{Z})^*/ < \pm 1 >$). Hence to go from r_i to r_{i+1}, one applies the Galois automorphism $2 \in \mathrm{Gal}(X/X_0(25)) = (\mathbf{Z}/25\mathbf{Z})^*/ < \pm 1, \pm 7 >$.

4 Gauss sums

Given a prime $p \equiv 1(\mod 5)$, let $\Psi_p : \mathbf{F}_p \longrightarrow \mathbf{C}^*$ be the additive character sending 1 to ζ_p. We consider the Gauss sum:

$$g(p) = \sum_{x \in \mathbf{F}_p} \chi(x) \Psi_p(x),$$

where χ is a character of $\mathbf{F}_p^*$ of order 5. The value of $g(p)$ is independent of χ, up to the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$.

By combining Lehmer's explicit determination of the roots of her polynomial as Gaussian periods, and our identification of these roots with certain modular forms of level 25, we obtain:

Theorem 4.1 *If $\eta(\tau)/\eta(25\tau) = n \in \mathbf{Z}$, and $\eta(5\tau)^6/(\eta(\tau)\eta(25\tau)^5) = p$ is prime, then:*

$$\prod_{i=1}^{4} (\eta(\tau)/\eta(25\tau) - \sigma_i^{-1}(\zeta_5 \sqrt{5}))^{i/5} = (\frac{n}{5}) g(p),$$

where $\sigma_i \in \mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$ sends ζ_5 to ζ_5^i.

There is some ambiguity in the formula, since the value of $g(p)$ depend on the choice of a multiplicative character χ, and the left hand side is really only defined up to a fifth root of 1. We are asserting that there is a way of making these choices so that the formula holds.

Observe that the left hand side is a modular unit (i.e., a unit for the covering $X_1(25) \longrightarrow X_0(1)$). Thus the above expresses Gauss sums as values of certain modular units on $X_1(25)$. It seems that the other coverings of lower degree studied by Lehmer yield similar results. It would be interesting to obtain such formulas a priori: this might provide a justification for the fact that translates of Gaussian period polynomials yield cyclic units for extensions of small degree.

Note: The idea of studying families of units in cyclic extensions of $\mathbf{Q}$ arising from the modular covering $X_1(N) \longrightarrow X_0(N)$ has been explored by Odile Lecacheux (see, for example, the paper [Le1] which studies units in sextic extensions which arise from the modular covering $X_1(13) \longrightarrow X_0(13)$). Independently of the author, Lecacheux has also observed the connection between Lehmer's quintic and the modular curve $X_1(25)$ [Le2].

References

[K] Daniel S. Kubert. *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976) 193-237.

[K-L] Daniel S. Kubert and Serge Lang. Modular Units. Springer-Verlag, 1981, New York.

[Le1] Odile Lecacheux, *Unités d'une famille de corps cycliques réels de degré 6 liés à la courbe modulaire* $X_1(13)$, Journal of Number Theory 31, 54-63 (1989).

[Le2] Odile Lecacheux, private communication.

[Leh] Emma Lehmer. *Connection between Gaussian periods and cyclic units*, Math. Comp., vol. 50, No. 182, April 1988, pp. 535-541.

[M] B.H. Matzat, *Rationality Criteria for Galois Extensions*, in Galois Groups over $\mathbf{Q}$, Poceedings of a Workshop held March 23-27, 1987, MSRI publications, pp. 361-384, 1989.

[Ogg] A. Ogg, *Survey of modular functions of one variable*, in Modular functions of one variable, Proceedings, Antwerp 1972, SLN 320.

[SW] Rene Schoof and Lawrence C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. vol. 50, no. 182, April 1988, pp. 543-556.

Henri Darmon - Harvard Univ. Math. Dept., 1 Oxford St., Cambridge MA 02138.