# NOTE ON A POLYNOMIAL OF EMMA LEHMER 

HENRI DARMON


#### Abstract

Recently, Emma Lehmer constructed a parametric family of units in real quintic fields of prime conductor $p=t^{4}+5 t^{3}+15 t^{2}+25 t+25$ as translates of Gaussian periods. Later, Schoof and Washington showed that these units were fundamental units. In this note, we observe that Lehmer's family comes from the covering of modular curves $X_{1}(25) \rightarrow X_{0}(25)$. This gives a conceptual explanation for the existence of Lehmer's units: they are modular units (which have been studied extensively). By relating Lehmer's construction with ours, one finds expressions for certain Gauss sums as values of modular units on $X_{1}(25)$.


## 1. Lehmer's polynomial

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

Let

$$
\begin{align*}
P_{5}(Y, T)= & Y^{5}+T^{2} Y^{4}-2\left(T^{3}+3 T^{2}+5 T+5\right) Y^{3} \\
& +\left(T^{4}+5 T^{3}+11 T^{2}+15 T+5\right) Y^{2}  \tag{1}\\
& +\left(T^{3}+4 T^{2}+10 T+10\right) Y+1
\end{align*}
$$

be the quintic polynomial constructed in [5]. The discriminant of $P_{5}(Y, T)$, viewed as a polynomial in $Y$ with coefficients in $\mathbf{Q}(T)$, is

$$
D(T)=\left(T^{3}+5 T^{2}+10 T+7\right)^{2}\left(T^{4}+5 T^{3}+15 T^{2}+25 T+25\right)^{4}
$$

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 [5], 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 $T=-\sqrt{5} \zeta_{5}, \sqrt{5} \zeta_{5}^{2},-\sqrt{5} \zeta_{5}^{-1}, \sqrt{5} \zeta_{5}^{-2}$, the zeros of the

[^0]minimal polynomial
$$
T^{4}+5 T^{3}+15 T^{2}+25 T+25
$$
(Here $\sqrt{5}$ denotes the positive square root.) If $t \in \mathbf{Z}$ is chosen so that
$$
p=t^{4}+5 t^{3}+15 t^{2}+25 t+25
$$
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:
$$
r_{i}=(t / 5) \eta_{i}+\left[(t / 5)-t^{2}\right] / 5
$$
where $\eta_{j}=\sum_{x \in \Gamma_{j}} \zeta_{p}^{x}$ and $\Gamma_{j}$ denotes the $j$ th 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 degree $d=6$, and its arithmetic genus is $(d-1)(d-2) / 2=10$. Let $C^{\prime}$ denote the normalization of $C$; it is a smooth projective curve of genus 4. The covering $C^{\prime} \rightarrow \mathbf{P}_{1}$ 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 $R=\left\{-\sqrt{5} \zeta_{5}, \sqrt{5} \zeta_{5}^{2}\right.$, $\left.-\sqrt{5} \zeta_{5}^{-1}, \sqrt{5} \zeta_{5}^{-2}\right\}$.
2. The closed points of the fiber above $\infty \in \mathbf{P}_{1}$ are rational.

Proposition 1.1. Properties 1 and 2 determine the covering $C^{\prime}$ uniquely up to Q-isomorphism.
Proof. Let $\left(\mathbf{P}_{1}-R\right)$ be the projective line with the points of $R$ removed, viewed as a curve over $\mathbf{Q}$. The space $V=H_{e t}^{1}\left(\mathbf{P}_{1}-R, \mathbf{Z} / 5 \mathbf{Z}\right)$ is a vector space of dimension 3 over $\mathbf{F}_{5}$, and is endowed with a natural action of $\operatorname{Gal}(\overline{\mathbf{Q}} / \mathbf{Q})$. In fact, one has

$$
V=H_{e t}^{1}\left(\mathbf{P}_{1}-R, \mu_{5}\right) \otimes \mu_{5}^{-1}
$$

where $\mu_{5}$ denotes the group scheme of 5th roots of unity. By Kummer theory, $H_{e t}^{1}\left(\mathbf{P}_{1}-R, \mu_{5}\right)$ is identified with the subspace of $\overline{\mathbf{Q}}(T)^{*} / \overline{\mathbf{Q}}(T)^{* 5}$ spanned by the elements

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

whose product is 1 . Hence the action of $\operatorname{Gal}(\overline{\mathbf{Q}} / \mathbf{Q})$ on $H_{e t}^{1}\left(\mathbf{P}_{1}-R, \mu_{5}\right)$ factors through $\operatorname{Gal}\left(\mathbf{Q}\left(\zeta_{5}\right) / \mathbf{Q}\right)$, and is isomorphic to the regular representation of $\operatorname{Gal}\left(\mathbf{Q}\left(\zeta_{5}\right) / \mathbf{Q}\right)$ 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 $V^{\omega}, V^{\omega^{2}}$ denote one-dimensional spaces on which $\operatorname{Gal}\left(\mathbf{Q}\left(\zeta_{5}\right) / \mathbf{Q}\right)$ acts via the Teichmüller character $\omega$ and the
square of the Teichmüller character $\omega^{2}$, respectively. In particular, $V_{0}$ is the unique one-dimensional subspace of $V$ which is fixed by $\operatorname{Gal}(\overline{\mathbf{Q}} / \mathbf{Q})$. 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, property 1 determines $C^{\prime}$ uniquely as a curve over $\overline{\mathbf{Q}}$. (Alternatively, one could use the "rigidity criterion" of Matzat, cf. [6, p. 368].) It is not hard to see that there is a unique rational form of the covering $C^{\prime}$ such that the closed points above $\infty \in \mathbf{P}_{1}$ are all rational (twisting this rational form by a cocycle $c$ in $H^{1}\left(\mathbf{Q}, \operatorname{Aut}\left(C^{\prime} / \mathbf{P}_{1}\right)\right)$ will cause these points to be defined over the larger extension "cut out" by $c$ ). Thus, property 2 determines $C^{\prime} \rightarrow \mathbf{P}_{1}$ up to $\mathbf{Q}$-isomorphism.

## 2. 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 [7].

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 $X_{1}(25) \rightarrow X_{0}(25)$ is Galois with Galois group canonically isomorphic to $G=(\mathbf{Z} / 25 Z)^{*} /\langle \pm 1\rangle$. 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 $T_{5}=\eta(z) / \eta(25 z)$ and $F_{5}=(\eta(z) / \eta(5 z))^{6}$ be Hauptmoduls for $X_{0}(25)$ and $X_{0}(5)$, respectively. One has

$$
F_{5}=T_{5}^{5} /\left(T_{5}^{4}+5 T_{5}^{3}+15 T_{5}^{2}+25 T_{5}+25\right)
$$

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. [1]). The covering $X \rightarrow X_{0}(25)$ is ramified at the four nonrational cusps, and the fiber above the cusp $T_{5}=\infty$ is composed of rational points (cf. [1, p. 226]). By Proposition 1.1, $X$ can be described by Lehmer's quintic; the zeros $r_{1}, \ldots, r_{5}$ of $P_{5}\left(Y, T_{5}\right)$ 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 $P_{5}\left(Y, T_{5}\right)=$ 0 , one obtains the following $q$-expansions for the $r_{i}$ :

$$
\begin{align*}
& r_{1}=-q^{3}+q^{4}+q^{10}-q^{11}-q^{12}+q^{13}-q^{15}+q^{17}+\cdots \\
& r_{2}=q^{-1}+1+q^{6}+q^{7}-q^{10}-q^{11}+\cdots \\
& r_{3}=-q-q^{3}+q^{4}+q^{6}-q^{12}-q^{14}+q^{18}+q^{20} \cdots  \tag{2}\\
& r_{4}=-q^{-2}-q-q^{2}-q^{5}+q^{15}+q^{17}+q^{18} \cdots \\
& r_{5}=q^{-1}+q^{5}+q^{7}-q^{8}-q^{12}+q^{13}-q^{14}+\cdots
\end{align*}
$$

By [8, p. 548], the transformation

$$
r \mapsto \frac{\left(T_{5}+2\right)+T_{5} r-r^{2}}{1+\left(T_{5}+2\right) r}
$$

permutes the roots of $P\left(Y, T_{5}\right)$ cyclically; one can thus label the $r_{i}$ in such a way that a generator of $\operatorname{Gal}\left(X / X_{0}(25)\right) \simeq \mathbf{Z} / 5 \mathbf{Z}$ 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 $\operatorname{Gal}\left(X / X_{0}(25)\right)$ sends $P_{i}$ to $P_{i+1}$ and such that

$$
\operatorname{Divisor}\left(r_{1}\right)=3 P_{1}-P_{2}+P_{3}-2 P_{4}-P_{5}
$$

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

$$
\wp_{a}(\tau)=\wp(a / 25 ; \tau),
$$

where

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

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 [1]. In particular, we find that

$$
\text { Divisor }\left(\frac{\wp_{7,9} \wp_{6,3} \wp_{1,12} \wp_{8,4}}{\wp_{1,3} \wp_{7,4} \wp_{6,7} \wp_{8,1}}\right)=3 P_{1}-P_{2}+P_{3}-2 P_{4}-P_{5}
$$

where the $P_{i}$ denote the cusps on $X$ which are above the cusp $\infty$ of $X_{0}(25)$. By expressing the function on the left in terms of so-called Klein forms $t_{\left(a_{1}, a_{2}\right)}$ (cf. [2]), the above simplifies to give

$$
\text { Divisor }\left(\frac{t_{(0,1)} t_{(0,7)}}{t_{(0,9)} t_{(0,12)}}\right)=3 P_{1}-P_{2}+P_{3}-2 P_{4}-P_{5}
$$

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

$$
\begin{aligned}
& r_{1}=\frac{t_{1} t_{7}}{t_{9} t_{12}}(25 \tau)=-q^{3} \prod_{n \equiv \pm 1, \pm 7(25)}\left(1-q^{n}\right) / \prod_{n \equiv \pm 9, \pm 12(25)}\left(1-q^{n}\right), \\
& r_{2}=\frac{t_{2} t_{11}}{t_{1} t_{7}}(25 \tau)=q^{-1} \prod_{n \equiv \pm 2, \pm 11(25)}\left(1-q^{n}\right) / \prod_{n \equiv \pm 1, \pm 7(25)}\left(1-q^{n}\right)
\end{aligned}
$$

$$
\begin{aligned}
& r_{3}=\frac{t_{4} t_{3}}{t_{11} t_{2}}(25 \tau)=-q \prod_{n \equiv \pm 4, \pm 3(25)}\left(1-q^{n}\right) / \prod_{n \equiv \pm 11, \pm 2(25)}\left(1-q^{n}\right) \\
& r_{4}=\frac{t_{8} t_{6}}{t_{3} t_{4}}(25 \tau)=-q^{-2} \prod_{n \equiv \pm 8, \pm 6(25)}\left(1-q^{n}\right) / \prod_{n \equiv \pm 3, \pm 4(25)}\left(1-q^{n}\right) \\
& r_{5}=\frac{t_{9} t_{12}}{t_{6} t_{8}}(25 \tau)=q^{-1} \prod_{n \equiv \pm 9, \pm 12(25)}\left(1-q^{n}\right) / \prod_{n \equiv \pm 6, \pm 8(25)}\left(1-q^{n}\right)
\end{aligned}
$$

The Galois group $\operatorname{Gal}\left(X_{1}(25) / X_{0}(25)\right)=(\mathbf{Z} / 25 \mathbf{Z})^{*} /\langle \pm 1\rangle$ acts on the $t_{a}$ by multiplying the subscripts (which are viewed as belonging to $\left.(\mathbf{Z} / 25 \mathbf{Z})^{*} /\langle \pm 1\rangle\right)$. Hence, to go from $r_{i}$ to $r_{i+1}$, one applies the Galois automorphism $2 \in$ $\operatorname{Gal}\left(X / X_{0}(25)\right)=(\mathbf{Z} / 25 \mathbf{Z})^{*} /\langle \pm 1, \pm 7\rangle$.

## 3. Gauss sums

Given a prime $p \equiv 1(\bmod 5)$, let $\Psi_{p}: \mathbf{F}_{p} \rightarrow \mathbf{C}^{*}$ be the additive character sending 1 to $\zeta_{p}$. We consider the Gauss sum

$$
g(p)=\sum_{x \in \mathbf{F}_{p}} \chi(x) \Psi_{p}(x)
$$

where $\chi$ is a character of $\mathrm{F}_{p}^{*}$ of order 5 . The value of $g(p)$ is independent of $\chi$, up to the action of $\operatorname{Gal}\left(\mathbf{Q}\left(\zeta_{5}\right) / \mathbf{Q}\right)$.

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 3.1. If $\eta(\tau) / \eta(25 \tau)=n \in \mathbf{Z}$, and $\eta(5 \tau)^{6} /\left(\eta(\tau) \eta(25 \tau)^{5}\right)=p$ is prime, then

$$
\prod_{i=1}^{4}\left(\eta(\tau) / \eta(25 \tau)-\sigma_{i}^{-1}\left(\zeta_{5} \sqrt{5}\right)\right)^{i / 5}=(n / 5) g(p),
$$

where $\sigma_{i} \in \operatorname{Gal}\left(\mathbf{Q}\left(\zeta_{5}\right) / \mathbf{Q}\right)$ sends $\zeta_{5}$ to $\zeta_{5}^{i}$.
There is some ambiguity in the formula, since the value of $g(p)$ depends on the choice of a multiplicative character $\chi$, 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 $\left.X_{1}(25) \rightarrow X_{0}(1)\right)$. 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 $X_{1}(N) \rightarrow X_{0}(N)$ has been explored by Odile

Lecacheux (see, for example, the paper [3], which studies units in sextic extensions which arise from the modular covering $\left.X_{1}(13) \rightarrow X_{0}(13)\right)$. Independently of the author, Lecacheux has also observed the connection between Lehmer's quintic and the modular curve $X_{1}(25)$ [4].

## Acknowledgment

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

## Bibliography

1. Daniel S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. (3) 33 (1976), 193-237.
2. Daniel S. Kubert and Serge Lang, Modular units, Springer-Verlag, New York, 1981.
3. Odile Lecacheux, Unités d'une famille de corps cycliques réels de degré 6 liés à la courbe modulaire $X_{1}(13)$, J. Number Theory 31 (1989), 54-63.
4. $\qquad$ , private communication.
5. Emma Lehmer, Connection between Gaussian periods and cyclic units, Math. Comp. 50 (1988), 535-541.
6. B. H. Matzat, Rationality criteria for Galois extensions, Galois Groups Over Q, Proc. Workshop held March 23-27, 1987 (Y. Ihara, K. Ribet, and J.-P. Serre, eds.), MSRI Publications, 1989, pp. 361-384.
7. A. Ogg, Survey of modular functions of one variable, Modular Functions of One Variable (Proc. Antwerp 1972), Lecture Notes in Math., vol. 320, Springer, 1973.
8. René Schoof and Lawrence C. Washington, Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comp. 50 (1988), 543-556.

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138
E-mail address: darmon@zariski.harvard.edu


[^0]:    Received September 18, 1989; revised February 12, 1990, March 22, 1990.
    1980 Mathematics Subject Classification (1985 Revision). Primary 11F11, 11R20, 11R32, $11 \mathrm{Y} 40,12 \mathrm{~F} 10$.

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

