Roots of Modular Units

A. Beeson

October 20, 2015

Abstract

Let p be a prime. We prove that if a modular unit has a pth root that is again a modular unit, then the level of that root is at most p times the level of the original unit.

1 Introduction

We prove the theorem in section 3, but because the literature contains inconsistent definitions, in section 2 we give a summary of the relevant definitions. The reader interested in learning more about the theory of modular functions should see [DS05].

Our main result is that the pth root of a modular unit, if it is again a modular unit, has the level that one would expect. The source of this question was the study of the Siegel functions and their square roots (see [Kub81]), with an eye towards constructing explicit units in the complement of the Siegel group whose squares *are* in the Siegel group. The special values of these units are of interest in explicit Abelian class field theory.

2 Background

2.1 Modular functions

Let $\mathcal{H} = \{z \in \mathbb{C} | \operatorname{Im}\{z\} > 0\}$ denote the complex upper half plane; let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ be the extended upper half plane and $\hat{\mathbb{C}}$ the compactified complex plane. Let Γ denote the (inhomogeneous) modular group, or the

group of all fractional linear transformations mapping $\mathcal{H}$ to itself. Then Γ is naturally identified with the matrix group

$$\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\} = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad-bc = 1\}/\{\pm I\},$$

which is generated by $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The action of Γ on an upper half-plane variable $z \in \mathcal{H}$ is given via fractional linear transformation:

$$A \circ z = \frac{az+b}{cz+d}.$$

A map $f : \mathcal{H}^* \to \hat{\mathbb{C}}$ is called a *modular function (of level one)* if

1. f is meromorphic on $\mathcal{H}$,
2. $f(A \circ z) = f(z)$ for all $A \in \Gamma$ and $z \in \mathcal{H}^*$,
3. and, if f is not the zero map, there is an $a > 0$ so that for $\mathrm{Im}\{z\} > a$, $f(z)$ has an expansion in the local variable at $i\infty$, $q = e^{2\pi iz}$, of the form

$$f(z) = \sum_{n \geq n_0} a_n q^n, \ n \in \mathbb{Z}, \ a_{n_0} \neq 0.$$

so n_0 determines the behavior of f as $z \to \infty$. If $n_0 < 0$ then $f(i\infty) = \infty$; if $n_0 = 0$ then $f(i\infty) = a_0$; and if $n_0 > 0$ then $f(i\infty) = 0$. In the last case, we call f a *cusp form*.

Fix a natural number $N > 2$. Let $\Gamma(N) \leq \Gamma$ be the (inhomogeneous) principal congruence subgroup modulo N, or the kernel of the reduction mod N map. In other words,

$$1 \longrightarrow \Gamma(N) \longrightarrow \Gamma \longrightarrow PSL_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1$$

is a short exact sequence.

By convention, we take $\Gamma(1) = \Gamma$. The upper half-plane modulo the action of Γ (written, by abuse of notation, $\mathcal{H}/\Gamma$) is a singular surface whose one-point compactification by the image of the point $i\infty$ under the stereographic projection is homeomorphic to the Riemann sphere. The completed non-singular curve is denoted $X(1)$. Similarly, $\mathcal{H}/\Gamma(N)$ can be compactified by

adding finitely many points, the *cusps* of $\Gamma(N)$, or the translates of $i\infty$ under a full set of coset representatives for $PSL_2(\mathbb{Z}/N\mathbb{Z})$ in Γ. In this case, the curve is denoted $X(N)$.

If H is a finite index subgroup in Γ the set of *cusps*, or translates of $i\infty$ under a full set of coset representative for H in Γ, will hereafter be denoted $C(H)$. A finite index subgroup of Γ defined by congruence conditions is called a *congruence subgroup*. The *conductor* of a congruence subgroup H is the largest N for which $\Gamma(N) \subseteq H$.

2.2 Modular functions of level N

A *modular function* for a congruence subgroup $\Gamma(N)$ is a function, $f(z) : \mathcal{H}^* \to \hat{\mathbb{C}}$ such that

1. f is meromorphic on $\mathcal{H}$,
2. $f(A \circ z) = f(z)$ for all $A \in \Gamma(N)$ and $z \in \mathcal{H}^*$,
3. $f(z)$ has an expansion at each of the cusps in the local variable $q = e^{2\pi i z}$ of the form
$$f(z) = \sum_{n \geq n_0} a_n q^n, \ n \in \mathbb{Z}, a_{n_0} \neq 0.$$

If f is modular for $\Gamma(N)$, we say f has *level* N. A modular function of level N descends to a well-defined holomorphic function on $X(N)$. As before, if $n_0 > 0$ for all $\alpha \in C(\Gamma(N))$ then $f(z)$ is called a cusp form for $\Gamma(N)$.

2.3 The full tower of modular functions $\mathcal{F}$

The set of modular functions invariant under the full modular group Γ is, in fact, a function field of genus one and is generated over $\mathbb{C}$ by the classical j-function,

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + O(q^4).$$

We write $\mathcal{F}_1 = \mathbb{Q}(j(z))$ and note that $\mathcal{F}_1$ is the full field of rational functions on $X(1)$ whose Fourier coefficients are rational. The j-function is normalized so that its q-expansion at $i\infty$ (which is the only cusp of $\mathcal{H}/\Gamma$)

has integral coefficients. Thus, it is reasonable to define the ring of integers in this field to be $\mathbb{Z}[j]$.

Furthermore, the set of level N functions together with the Nth roots of unity generate a field extension of $\mathcal{F}_1$, denoted $\mathcal{F}_N$, which is a finite Galois extension of $\mathcal{F}_1$ with Galois group $PGL_2(\mathbb{Z}/N\mathbb{Z}) \cong \Gamma/\Gamma(N) \times (\mathbb{Z}/N\mathbb{Z})^\times$. The Galois action is given by writing $PGL_2(\mathbb{Z}/N\mathbb{Z}) \cong PSL_2(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^\times$ and letting $PSL_2(\mathbb{Z}/N\mathbb{Z})$ act as usual as fractional linear transformations on $z \in \mathcal{H}$. A matrix in $PGL_2(\mathbb{Z}/N\mathbb{Z})$ with determinant $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ acts on a (not necessarily primitive) Nth root of unity ζ via $\sigma_d : \zeta \mapsto \zeta^d$. In other words, if f has Fourier expansion

$$f(z) = \sum_{n \geq n_0} a_n q^n$$

then elements of the form $A = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \in PGL_2(\mathbb{Z}/N\mathbb{Z})$ act as follows:

$$f(A \circ z) = \sum_{n \geq n_0} \sigma_d(a_n) q^n$$

and more general elements A of determinant d act as

$$f(A \circ z) = \sum_{n \geq n_0} \sigma_d(a_n) (A' \circ q)^n$$

where $A' = \frac{1}{\sqrt{d}} A \in PSL_2(\mathbb{Z}/N\mathbb{Z})$.

Taking the integral closure of $\mathbb{Z}[j]$ in $\mathcal{F}_N$, we get a ring R_N, whose units, U_N, are the *modular units of level N*. It is not uncommon, however, to extend scalars to $\mathbb{C}$, that is, to study $U_N \otimes \mathbb{C} \subseteq R_N \otimes \mathbb{C}$. In this setting the set of functions with multiplicative inverses coincide precisely with the set of functions whose divisor of zeros and poles is supported at the cusps of $X(N)$.

Finally, the compositum of the $\mathcal{F}_N$ over all N is called the *full tower of modular functions* $\mathcal{F}$. The set of units U in the full tower of modular functions is the direct limit of the U_N with respect to the natural inclusion maps.

3 On the level of a root of a modular function

Theorem 3.1. *Let $\mathcal{F}_N$ be the field of modular functions of level N with Fourier coefficients in $\mathbb{Q}(\zeta_N)$; that is, $\mathcal{F}_N$ is the fixed field of $\Gamma(N)$ inside $\mathcal{F}$,*

the full field of modular functions. If p is a rational prime and $f(z) \in \mathcal{F}_N \backslash \mathcal{F}_N^p$ is a modular unit and $f(z)^{1/p}$ has level M for some $M \in \mathbb{N}$ with $N|M$ then, in fact, $f(z)^{1/p}$ has level pN.

Proof. We assume $f(z)^{1/p}$ is known to be invariant under the subgroup $\Gamma(M) \subseteq \Gamma(N)$. We will show that $f(z)^{1/p}$ is invariant under $\Gamma(pN)$.

Let Γ_1 be the subgroup of $\Gamma(N)$ that fixes $f(z)^{1/p}$; ie, for all $A \in \Gamma_1$ and $z \in \mathcal{H}^*$,

$$f(A \circ z)^{1/p} = f(z)^{1/p}.$$

Because $\mathcal{F}_N(f(z)^{1/p})$ is a degree p extension of $\mathcal{F}_N$, the index $[\Gamma(N) : \Gamma_1] = p$, and, thus, Γ_1 is a finite index subgroup of Γ as well. Furthermore, because $f(z)^{1/p}$ is of level M, $\Gamma(M) \subseteq \Gamma_1$. So we have the linear ordering of fields

$$\mathbb{Q}(j(z)) \subseteq \mathcal{F}_N \subseteq \mathcal{F}^{\Gamma_1} \subseteq \mathcal{F}_M \subseteq \mathcal{F}$$

where $\mathcal{F}^{\Gamma_1}$ denotes the fixed field of Γ_1 inside $\mathcal{F}$.

Let $\mathcal{D}$ be a fundamental domain for Γ; so $\mathcal{D}$ is a simply connected subset of $\mathcal{H}^*$ such that $\mathcal{D}$ contains precisely one point from each Γ-orbit. If $\mathcal{D}_1$ is a fundamental domain for the subgroup of finite index $\Gamma_1 \subseteq \Gamma$ then it is made up of translates of $\mathcal{D}$ by a full set of coset representatives for Γ_1 inside Γ. Such a translate is called a *modular triangle*. Define the *fan width* of a fundamental domain at a cusp α to be the order of the cyclic group that permutes the Γ_1-inequivalent modular triangles meeting at α. Schoeneberg proves in [Sho74] that the conductor of a group Γ_1 is equal to the least common multiple of the fan widths at the rational cusps.

The index of $\Gamma(N)$ in Γ is the size of $PSL_2(\mathbb{Z}/N\mathbb{Z})$, which is

$$l = [\Gamma : \Gamma(N)] = \frac{1}{2}N^3 \prod_{p|N}(1 - \frac{1}{p^2}).$$

As observed above, $[\Gamma(N) : \Gamma_1] = p$, hence the group of automorphisms of $\mathcal{F}^{\Gamma_1}$ fixing $\mathcal{F}_N$ is cyclic. If we let σ be a generator then $\Gamma(N)$ decomposes as the disjoint union

$$\Gamma(N) = \Gamma_1 \cup \sigma\Gamma_1 \cup \sigma^2\Gamma_1 \cup \cdots \cup \sigma^{p-1}\Gamma_1.$$

And if $\{A_1, \ldots, A_l\}$ is a complete set of representative for $\Gamma/\Gamma(N)$ then

$$\{A_1, \ldots, A_l, \sigma A_1, \ldots, \sigma A_l, \sigma^2 A_1, \ldots, \sigma^2 A_l, \ldots, \sigma^{p-1} A_1, \ldots, \sigma^{p-1} A_l\}$$

is a complete set of representatives for Γ/Γ_1. Recalling our notation $C(\Gamma(N))$ for the cusps of $\mathcal{H}/\Gamma(N)$, we see that

$$C(\Gamma(N)) \subset C(\Gamma_1)$$

and if α is a cusp of Γ_1 then $\sigma^i\alpha \in C(\Gamma(N))$ for some i with $1 \leq i \leq p$.

Choose $\{A_1, \ldots, A_l\}$ to be a complete set of representatives for $\Gamma/\Gamma(N)$ such that

$$\mathcal{D}_N = \cup_i A_i(\mathcal{D})$$

is a fundamental domain for $\mathcal{H}/\Gamma(N)$. Let $\mathcal{D}_1$ be a fundamental domain for $\mathcal{H}/\Gamma_1$.

Schoeneberg's theorem implies that the least common multiple of the fan widths for $\mathcal{D}_N$ is N. We will use this to show that, for any cusp α of Γ_1, the fan width of $\mathcal{D}_1$ at α divides pN so, by Schoeneberg's theorem, the conductor of Γ_1 divides pN. Because $f(z)^{1/p} \notin \mathcal{F}_N$, $f(z)^{1/p}$ must have level pN.

Let α be a cusp of Γ_1. As observed above, this implies $\sigma^i\alpha$ is a cusp of $\Gamma(N)$ for at least one i with $1 \leq i \leq p$. Letting $\beta = \sigma^i\alpha$ be a translate of α that is a cusp of $\mathcal{D}_N$, we see that multiplication by σ^i is a homeomorphism between a neighborhood of α and a neighborhood of β. Thus, it suffices to prove the result for the cusps of $\mathcal{D}_1$ that are also cusps of $\mathcal{D}_N$.

Lemma 3.2. *If α is a cusp of Γ_1 and of $\Gamma(N)$ that is of fan width n for $\mathcal{D}_N$ then its width for $\mathcal{D}_1$ is n or pn.*

Proof. Recall $\Gamma_1 \subseteq \Gamma(N)$ so $\Gamma \setminus \Gamma(N) \subseteq \Gamma \setminus \Gamma_1$ and that the fan width n of $\mathcal{D}_1$ at the cusp α is the order of the cyclic group that permutes the n Γ_1-inequivalent triangles meeting at α.

If two triangles are Γ_N-inequivalent then they are Γ_1-inequivalent so, assuming the width for $\mathcal{D}_N$ is n, the width for Γ_1 is at least n. Then since $[\Gamma(N) : \Gamma_1] = p$, we see that the width of a triangle for Γ_1 is no more than pn. □

This concludes the proof of the theorem so any pth root of a level N modular function that has a level, in fact, has level N or pN. As $f(z)^{1/p}$ is not level N by assumption, it must be level pN. □

The special case we are currently most interested in is when $p = 2$, in which case we have the following theorem and its corollary.

Theorem 3.3. *If $f(z) \in \mathcal{F}_N \setminus \mathcal{F}_N^2$ is a modular unit and $\sqrt{f(z)}$ has level M for some $M \in \mathbb{N}$ with $N|M$ then, in fact, $\sqrt{f(z)}$ has level $2N$.*

Theorem 3.4. *If $f(z) \in \mathcal{F}_N \setminus \mathcal{F}_N^2$ is a modular unit with $\sqrt{f(z)} \notin \mathcal{F}_N(\sqrt{j(z) - 1728})$ then $\sqrt{f(z)}$ is not level M for any $M \in \mathbb{N}$.*

Proof. By the index, there is a unique quadratic extension between $\mathcal{F}_N$ and $\mathcal{F}_{2N}$. We observe that $\mathcal{F}_N(\sqrt{j(z) - 1728})$ is such an extension since $j(z) - 1728$ has a holomorphic $PSL_2(\mathbb{Z})$-invariant square root on $\mathcal{H}$. □

The theorem says that if the square root of a modular unit of level N is a modular function on a congruence subgroup then it is level $2N$. Thus, because the Siegel units $\phi_{u,v}$ for $(u, v) \in \frac{1}{N}\mathbb{Z}$ are level $12N^2$, it suffices to show the square roots of Siegel functions are not level $24N^2$ in order to conclude that they do not, in fact, have a level at all. For definitions and further discussion of the Siegel units see [KL81].

References

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer, 2005.

[KL81] D. Kubert and S. Lang. *Modular Units*, volume 224 of *Die Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, 1981.

[Kub81] D. Kubert. The square root of the siegel group. *Proc. London Math. Soc.*, 43(2):193–226, 1981.

[Sho74] B. Shoeneberg. *Elliptic Modular Functions: an Introduction*, volume 203 of *Die Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1974. Translated from the German by J. R. Smart and E. A. Schwandt.