ILLINOIS JOURNAL OF MATHEMATICS
Volume 28, Number 3, Fall 1984

RATIONAL COATES-WILES SERIES

BY

ROBERT GOLD

§**1.** This section will be formal and elementary. Let p be a fixed odd prime and ζ a primitive p-th root of unity. Call $f(T) \in \mathbf{Z}_p[[T]]$ a Coates-Wiles (CW) series if it satisfies

(i) $f(0) \equiv 1 \pmod p$
(ii) $f((1+T)^p - 1) = \prod_{i=0}^{p-1} f(\zeta^i(1+T) - 1)$.

We will call $f(T)$ rational if it is a quotient of elements of $\mathbf{Z}_p[T]$. Define a sequence of p-th power roots of unity $\{\zeta_n\}_{n\geq 0}$ by $\zeta_0 = \zeta$ and $\zeta_{n+1}^p = \zeta_n$. Then $x_n = \zeta_n - 1$ is a prime element in $Q_p(\zeta_n)$ and $f(x_n)$ is a unit in $Q_p(\zeta_n)$ for each n. We will say $f(T)$ is global if $f(x_n) \in Q(\zeta_n)$ for each n.

THEOREM 1. (a) *If $f(T)$ is a rational CW-series then*

$$f(T) = \alpha \prod_{i=1}^{m} (1 + T - \alpha_i)^{s_i},$$

$s_i \in \mathbf{Z}$ *and* α_i *is zero or a root of unity of order prime to* p, $\alpha \in Q_p^\times$.
(b) *If $f(T)$ is a rational and global CW-series then*

$$f(T) = \alpha(1+T)^{a_0} \prod_{i=1}^{r} ((1+T)^{a_i} - 1)^{b_i} \quad \text{for } a_i, b_i \in \mathbf{Z};$$

$(a_i, p) = 1$ *for* $i \geq 1$, $\alpha = \pm 1$.

Proof. If $f(T)$ is rational we may write it in terms of the parameter $x = 1 + T$; i.e. let $h(x) = f(x-1)$. Then condition (ii) for $f(T)$ gives

$$(*) \qquad h(x^p) = f(x^p - 1) = f((1+T)^p - 1) = \prod_{i=0}^{p-1} f(\zeta^i x - 1) = \prod_{i=0}^{p-1} h(\zeta^i x).$$

Let $\{r_1, \ldots, r_s\}$ be the roots and poles of $h(x)$ counted with signed multiplicities. Then the roots-poles of $h(x^p)$ are $\{\zeta^i \cdot r_j^{1/p}\}$, $i = 0, 1, \ldots, p-1$; $j = 1, \ldots, s$; while the roots-poles of $\prod h(\zeta^i x)$ are $\{\zeta^i \cdot r_j\}$, $i = 0, \ldots, p-1$; $j = 1, \ldots, s$. These sets with multiplicities must agree. Raising every element of both sets to the p-th power, we see that $\{r_j\}$ and $\{r_j^p\}$ must agree. If we continue in this manner we see that $\{r_j\}$ and $\{r_j^{p^n}\}$ must agree for every n. Hence, for every j, the sequence $r_j, r_j^p, \ldots, r_j^{p^n}, \ldots$ is finite, so for some $m \geq 1$, $r_j^{p^m} = r_j$. We have then that each r_j is zero or a root of unity of order prime to p and the assertion of (a) is a restatement of this fact.

Received October 27, 1980.

© 1984 by the Board of Trustees of the University of Illinois
Manufactured in the United States of America

By part (a), $h(x)$ is of the form $\alpha \prod_{i=1}^{m} (x - \alpha_i)^{s_i}$ and by (*) satisfies

$$\alpha \prod (x^p - \alpha_i)^{s_i} = \alpha^p \prod (x^p - \alpha_i^p)^{s_i}.$$

Since $\{\alpha_i\} = \{\alpha_i^p\}$ it follows that $\alpha = \alpha^p$ and therefore (by (i)) that α is a $(p-1)$-st root of unity. Thus, the coefficients of $h(x)$ all lie in some cyclotomic field

$$K_m = Q(e^{2\pi i/m}), \quad (m, p) = 1.$$

Assume now that in addition to being rational $f(T)$ is also global. This means that $h(\zeta_n) \in Q(\zeta_n)$ for all n. Let $Q(\zeta_\infty) = \bigcup_n Q(\zeta_n)$ so that $K_m \cap Q(\zeta_\infty) = Q$. Let s be any automorphism of $K_m(\zeta_\infty)$ which is the identity on $Q(\zeta_\infty)$. Then $h(\zeta_n) = [h(\zeta_n)]^s = h^s(\zeta_n^s) = h^s(\zeta_n)$ for all n and it follows that $h(x) = h^s(x)$. If the coefficients of $h(x)$ are fixed by every such s they must lie in Q. Since they are by assumption also in $\mathbf{Z}_p$, they are rational integers.

By the characterization of the roots-poles of $h(x)$ already given, we see that $h(x)$ must be of the form $\alpha \cdot x^{a_0} \prod_{i=1}^{r} D(x, m_i)^{\pm 1}$ where $D(x, m_i)$ is the m_i-th cyclotomic polynomial over $\mathbf{Z}$ and $(p, m_i) = 1$. By using the Möbius product

$$D(x, m) = \prod_{d \mid m} (x^d - 1)^{\mu(m/d)},$$

we may write $h(x) = \alpha \cdot x^{a_0} \prod (x^{a_i} - 1)^{d_i}$ with $(a_i, p) = 1$ for $i > 0$. Since $h(x) \in Q(x)$, it must be that $\alpha \in Q$. Then in order for $h(x)$ to satisfy (*), α must equal ± 1. Rewriting in terms of T, we obtain (b).

§2. We will be interested in $Q(\zeta)^+$, the maximal real subfield of the field of p-th roots of unity and in its Iwasawa invariant λ^+, the λ-invariant of the cyclotomic $\mathbf{Z}_p$-extension of $Q(\zeta)^+$. It would be a consequence of either Vandiver's conjecture or of Greenberg's conjecture that $\lambda^+ = 0$.

We begin with a lemma. Let $Q(\zeta_n)^+$ be the maximal real subfield of the field of p^{n+1}-st roots of unity. Let E_n be the group of units of $Q(\zeta_n)^+$ and C_n the subgroup of real cyclotomic or circular units. Denote by $N_{m,n}$ the norm map from $Q(\zeta_m)^+$ to $Q(\zeta_n)^+$. Then, $C_n = N_{m,n}(C_m)$ and $E_n \supseteq N_{m,n}(E_m)$. Let

$$E_n' = \bigcap_{m \geq n} N_{m,n}(E_m),$$

the universal global unit norms.

LEMMA 1. *$\lambda^+ = 0$ iff $p \nmid [E_0' : C_0]$ iff, for all n, $p \nmid [E_n' : C_n]$.*

Proof. Consider the exact sequence (e.g., see [4])

$$1 \longrightarrow H'(G, E_m) \longrightarrow (I_m^G/P_n)_p \xrightarrow{\alpha_{n,m}} (A_m^G)_p \longrightarrow$$
$$\xrightarrow{\beta} E_n/N(E_m) \longrightarrow [Q(\zeta_m)^+]^\times / N([Q(\zeta_m)^+]^\times)$$

where G is the Galois group of the cyclic extension $Q(\zeta_m)^+/Q(\zeta_n)^+$; I, P, A denote the groups of ideals, principal ideals, and ideal classes of the appropriate field; and $(\square)_p$ denotes the p-primary part. The map $\alpha_{n,m}$ is induced by the natural projection $I_m \to I_m/P_m = A_m$.

Since the extension is cyclic with a unique ramified prime,

$$E_n \subseteq N([Q(\zeta_m)^+]^\times).$$

This implies that $\beta = 0$ and also enables us to calculate, by the classical genus formula, that $|A_m^G| = |A_n|$. Greenberg showed in [2] that $\lambda^+ = 0$ iff $\alpha_{0,m} = 0$ for sufficiently large m iff for all n the map $\alpha_{n,m} = 0$ for sufficiently large m. Now, on the other hand $\alpha_{n,m} = 0$ precisely when

$$[E_n: N(E_m)] = |(A_m^G)_p| (= |(A_n)_p|)$$

while on the other hand

$$|(A_n)_p| = [E_n: C_n]_p,$$

by Dirichlet's class number formula. Since $N(E_m) \supseteq N(C_m) \supseteq C_n$, we see that $\alpha_{0,m} = 0$ for large m iff $(N(E_m)/C_0)_p = 0$ for large m iff $(E_0'/C_0)_p = 0$. Similarly, $\alpha_{n,m} = 0$ for sufficiently large m iff $(E_n'/C_n)_p = 0$.

Our next goal is to give in terms of CW-series a criterion for the vanishing of λ^+.

Let R be the set of global and rational CW-series and $\bar{R}$ its closure in $\mathbf{Z}_p[[T]]$ with respect to the (p, T)-topology. Let $\mathscr{C}$ be the set of CW-series corresponding to $\varprojlim_n C_n$ and $\bar{\mathscr{C}}$ its closure. By Theorem 1, $R \subseteq \mathscr{C}$.

LEMMA 2. $\bar{\mathscr{C}} = \bar{R}$.

Proof. Let $f(T)$ be an element of $\mathscr{C}$ so that for each n we have $f(x_n) \in C_n$. It is clear that we can find a $g_n(T) \in R$ such that $g_n(x_n) = f(x_n)$. Since both f and g are CW-series, it follows that $g_n(x_i) = f(x_i)$ for all $i \leq n$. But if $(f - g_n)(T)$ has roots $x_0, x_1, \ldots, x_n$, then $(f - g_n)(T)$ is divisible by

$$\frac{1}{T} W_n(T) = \frac{1}{T} \{(1 + T)^{p^{n+1}} - 1\}$$

in $\mathbf{Z}_p[[T]]$. Therefore, $(f - g_n)(T)$ is in $(p, T)^n$ and, since $g_n(T) \in R$, $f(T) \in \bar{R}$. We finally have $\bar{R} \supseteq \mathscr{C} \supseteq R$ so that $\bar{R} = \bar{\mathscr{C}}$.

We must now invoke the fundamental relation between CW-series and units [1], [5]. Let U_n denote the group of principal units in $Q_p \cdot Q(\zeta_n)^+$ and U, the projective limit of the U_n with respect to the norm map (notation as in [5]). Recall that $x_n = \zeta_n - 1$. Coates and Wiles have shown in [1] that for every $u = \varprojlim u_n \in U$ there is a unique $f_u(T) \in \mathbf{Z}_p[[T]]$ such that $f_u(x_n) = u_n$. The properties of this correspondence imply that $u \to f_u(T)$ is a homomorphism of U onto the multiplicative group of CW-series.

The x_n-adic topology on U_n coincides with the profinite topology; U_n is a pro-p-group. So $U = \varprojlim U_n$ is a profinite group. With respect to the (p, T)-adic topology on $\mathbf{Z}_p[[T]]$, the isomorphism $u \to f_u(T)$ is bicontinuous.

Let $E = \varprojlim E_n$ projective limit with respect to the norm map and $N_{\infty,n}$: $E \to E_n$ the projection to the n-th factor. Since $N_{m,n}(E_m) \supseteq C_n$ which is of finite index in E_n, the sequence $\{N_{m,n}(E_m)\}_{m \geq n}$ stabilizes. Thus, the projective system $\{E_n\}$ satisfies the Mittag-Leffler condition (see [3]). It follows that

$$N_{\infty,n}(E) = E'_n = \bigcap_{m \geq n} N_{m,n}(E_m).$$

Let $C = \varprojlim C_n$ so that $C, E \subseteq U$. We may take closures $\bar{C}, \bar{E}$ in U and we may take closures $\bar{C}_n, \bar{E}'_n$ in U_n. It is not hard to see that $\bar{C} = \varprojlim \bar{C}_n$, $\bar{E} = \varprojlim \bar{E}'_n$. If we denote by $\mathscr{E}$ (resp. $\mathscr{C}$) the CW-series corresponding to E (resp. C), then $\bar{\mathscr{E}}$ (resp. $\bar{\mathscr{C}}$) corresponds (p, T)-adically to $\bar{E}$ (resp. $\bar{C}$). Finally, note that $(E'_n/C_n)_p = 0$ iff $\bar{E}'_n = \bar{C}_n$.

Theorem 2. *The following are equivalent*

(a) $\lambda^+ = 0$.

(b) *If $f(T)$ is a CW-series and, for all n, $f(x_n)$ is a unit in $Q(\zeta_n)$, then $f(T) \in \bar{\mathscr{C}}$.*

(c) *If $f(T)$ is a CW-series and, for all n, $f(x_n)$ is a unit in $Q(\zeta_n)$, then $f(T) \in \bar{R}$.*

Proof. In view of Lemma 2, it suffices to show that (a) and (b) are equivalent.

First assume that $\lambda^+ = 0$. Then by Lemma 1, for all n, the index $[E'_n : C_n]$ is not divisible by p. Therefore, $\bar{E}'_n = \bar{C}_n$ and $\bar{\mathscr{E}} = \bar{\mathscr{C}}$. Now if $f(T)$ is a CW-series such that, for all $n, f(x_n)$ is a global unit, then $f(x_n) \in E'_n$. Hence, $f(T)$ is in $\mathscr{E}$ and is necessarily an element of $\bar{\mathscr{C}}$.

Conversely, assume condition (b) and let $\varepsilon_0 \in E'_0$. Then $\varepsilon_0 = N_0(\varepsilon)$ for some $\varepsilon \in E$. The CW-series $f_\varepsilon(T)$, which corresponds to ε, is therefore in $\mathscr{E}$ and $f_\varepsilon(x_n)$ is a global unit for every n. By the assumption, $f_\varepsilon(T) \in \bar{\mathscr{C}}$ and hence $\varepsilon \in \bar{C}$. Thus, $\varepsilon_0 \in \bar{C}_0$. We conclude that $E'_0 \subset C_0$ so that $E'_0 = C_0$ which in turn implies that $\lambda^+ = 0$.

References

1. J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Austral. Math. Soc., Vol. 26 (1978), pp. 1–25.

2. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math., Vol. 93 (1976), pp. 263–284.

3. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.

4. K. Iwasawa, *A note on the group of units of an algebraic number field*, J. Math. Pures Appl., Vol. 35 (1956), pp. 189–192.

5. S. Lang, *Cyclotomic fields*, Springer-Verlag, New York, 1978.

The Ohio State University
Columbus, Ohio