C. R. Math. Rep. Acad. Sci. Canada Vol. **31** (3) 2009, pp. 65–71

POLYNOMIALS À LA LEHMERS AND WILF

GERT ALMKVIST AND ARNE MEURMAN

Presented by Edward Bierstone, FRSC

Abstract. We show that a period polynomial introduced by the Lehmers coincides with a generalized Wilf polynomial.

Résumé. Nous montrons qu'un polynôme période introduit par les Lehmer coïncide avec un polynôme de Wilf généralisé.

1. **Introduction.** In [2] a generalized Dedekind sum was defined by

$$s(r,h,k) = \frac{k^r}{r+1}\sum_{j=1}^{k-1} B_{r+1}(j/k)((jh/k)),$$

where r is an even integer, $B_{r+1}(x)$ the Bernoulli polynomial, and

$$((x)) = \begin{cases} x - [x] - 1/2 & \text{if } x \notin \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

Further we define

$$A(r,k,n) = \sum_{(h,k)=1} \exp\{\pi i s(r,h,k) - 2\pi i h n/k\}.$$

We define the generalized Wilf polynomial of degree k by

$$W(r,k,x) = \prod_{n=1}^{k} (x - A(r,k,n))$$

T. Dokshitzer [4] proved that $W(r,k,x)$ has integer coefficients if

$$(r+1,k) = 1 \text{ and } (r+1,\varphi(k)) = 1,$$

where φ is Euler's totient function. In this note we study $W(p-3,p,x)$, which has integer coefficients if p is a prime ≥ 5.

Received by the editors on January 23, 2009.
AMS Subject Classification: Primary: 11F20; secondary: 11C08.
Keywords: period polynomial; Wilf polynomial; Dedekind sum.

Let $p \geq 5$ be a prime and g a primitive root (mod p^2). Define

$$\eta_n = \sum_{j=0}^{p-2} \exp\{2\pi i g^{pj}(g^p + pn)/p^2\} \quad \text{and} \quad L(p,x) = \prod_{n=1}^{p} (x - \eta_n),$$

the period polynomial (see [7]). We show that $W(p-3,p,x)$ and $L(p,x)$ agree up to the sign of x. In [7] the Lehmers asked if the constant term $L(p,0)$ could be even. We computed $L(1093,0)$ and found it to be divisible by 2^{1102}, so it is even by some margin. (The referee informed us that $p = 1093$ is the smallest prime for which $L(p,0)$ is even.) More precisely we have the following.

Let q be a prime such that $q^{p-1} \equiv 1 \pmod{p^2}$ (Wieferich condition). Then $L(p,x) \pmod{q}$ splits into linear factors.

In a private communication, A. Granville noted that $W(p-3,p,x)$ could be written as a certain determinant. This is proved here. Up to a simple transformation it is the characteristic polynomial of a circulant matrix.

2. **Generalized Wilf Polynomials.** In [2] it was proved (using Apostol's reciprocity theorem [3]) that if $r \leq p-5$, then $A(r,p,n) \in \mathbb{Q}[\zeta_p]$ where $\zeta_p = \exp(2\pi i/p)$. This is not the case for $r = p-3$. Instead we must use $\omega = \exp(2\pi i/p^2)$. Let $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ and g a primitive root in $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Let α be the automorphism of $\mathbb{Q}(\omega)$ determined by $\omega \mapsto \omega^{1+p}$. Then we have $G = U \times V$, where

$$U = \langle \alpha \rangle = \{\omega \mapsto \omega^{1+jp}; j = 0,1,\ldots,p-1\} \simeq \mathbb{Z}/p\mathbb{Z},$$

$$V = \langle \omega \mapsto \omega^{g^p} \rangle = \{\omega \mapsto \omega^{h^p}; h = 1,2,\ldots,p-1\} \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Set $E = \mathbb{Q}(\omega)^V = \mathbb{Q}(\rho)$, where

$$\rho = \mathrm{Tr}_{\mathbb{Q}(\omega)/E}(\omega) = \sum_{h=1}^{p-1} \omega^{h^p}$$

(it is easy to show that $\rho \notin \mathbb{Q}$ cf. [7]). Then we obtain

$$L(p,x) = \prod_{j=0}^{p-1} (x - \alpha^j(\rho)),$$

since $\eta_{mg^p} = \alpha^m(\rho)$. This has integer coefficients, since ρ is an algebraic integer. We denote by $\mathbb{Z}_p$ the ring of p-adic integers. Our main goal is the following.

THEOREM 1. *Let $p \geq 5$ be a prime. Then*

$$W(p-3,p,x) = \begin{cases} L(p,x) & \text{if } p \equiv \pm 1 \pmod 8, \\ -L(p,-x) & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

This will follow from the next two theorems.

THEOREM 2. *Let $p \geq 5$ be a prime. Let $u \in \mathbb{Z}$ be such that*

$$u \equiv \frac{pB_{p-1}}{p-2} \pmod{p^2\mathbb{Z}_p},$$

where B_{p-1} is the Bernoulli number. Then $p^2 s(p-3,h,p) \equiv uh^p \pmod{p^2}$ for $h = 1, 2, \ldots, p-1$.

Note that the von Staudt–Clausen theorem implies that $u \equiv \frac{p+1}{2} \pmod{p}$, so that in particular $(u,p) = 1$.

THEOREM 3. *Let $p \geq 5$ be a prime. We have*

$$p^2 s(p-3,h,p) \equiv \frac{p^2-1}{8} \pmod{2}$$

for $h = 1, 2, \ldots, p-1$.

The proof of Theorem 19 in [2] is also valid for $r = p-3$ and gives Theorem 3 (one requires r even and $(r+1,p) = 1$). The proof of Theorem 16 in [2] (which uses Apostol's reciprocity theorem [3]) gives

$$p^2 s(p-3,h,p) \equiv \frac{pB_{p-1}}{p-1}\left\{H^{-1} + \frac{1}{p-2}H^{p-2}\right\} \pmod{p^2\mathbb{Z}_p} \tag{1}$$

for any integers h and H such that $hH \equiv 1 \pmod{p}$.

LEMMA 4. *Let $a \in \mathbb{Z}_p$ such that $-2a \equiv 1 \pmod{p\mathbb{Z}_p}$. For $H \in \mathbb{Z}$ with $H \not\equiv 0 \pmod{p}$, define $f(H) = H^{-1} + aH^{p-2} \pmod{p^2\mathbb{Z}_p}$. Then*

$$f(H + bp) \equiv f(H) \pmod{p^2\mathbb{Z}_p}$$

for all $b \in \mathbb{Z}$.

PROOF. It is enough to show $f(H(1+p)) \equiv f(H) \pmod{p^2\mathbb{Z}_p}$, since the general statement follows from this by iteration. We have

$$\begin{aligned} f(H(1+p)) - f(H) &= \frac{1}{H(1+p)} + aH^{p-2}(1+p)^{p-2} - \frac{1}{H} - aH^{p-2} \\ &= \frac{1}{H(1+p)}\{1 + aH^{p-1}(1+p)^{p-1} - 1 - p - a(1+p)H^{p-1}\} \\ &\equiv \frac{1}{H(1+p)}\{-p + aH^{p-1}(1-p-1-p)\} \\ &\equiv \frac{p}{H(1+p)}\{-1 - 2aH^{p-1}\} \\ &\equiv \frac{p}{H(1+p)}\{H^{p-1} - 1\} \equiv 0 \pmod{p^2\mathbb{Z}_p}. \end{aligned}$$

□

PROOF OF THEOREM 2. As $H^p \equiv H \pmod p$, using Lemma 4 with $a = \frac{1}{p-2} \in \mathbb{Z}_p$, we may replace H by H^p in the right-hand side of (1). Hence

$$\begin{aligned} p^2 s(p-3,h,p) &\equiv \frac{pB_{p-1}}{p-1}\left\{\frac{1}{H^p} + \frac{1}{p-2}H^{p(p-2)}\right\} \\ &\equiv \frac{pB_{p-1}}{p-1}\frac{1}{H^p}\left\{1 + \frac{1}{p-2}H^{p(p-1)}\right\} \\ &\equiv \frac{pB_{p-1}}{p-1}\frac{p-1}{p-2}\frac{1}{H^p} \equiv uh^p \pmod{p^2\mathbb{Z}_p}. \end{aligned}$$

Here we used the fact that if $hH \equiv 1 \pmod p$, then $h^p H^p \equiv 1 \pmod{p^2}$. □

With Theorems 2 and 3 we can now evaluate $A(p-3,p,n)$. Note that

$$\exp(\pi i/p^2) = -\omega^{(p^2+1)/2}.$$

Thus

$$\begin{aligned} A(p-3,p,n) &= \sum_{h=1}^{p-1} \exp\Big\{\frac{\pi i}{p^2}p^2 s(p-3,h,p) - 2\pi i\frac{hn}{p}\Big\} \\ &= \sum_{h=1}^{p-1} (-1)^{p^2 s(p-3,h,p)} \omega^{(p^2+1)/2 \cdot uh^p - phn} \\ &= (-1)^{(p^2-1)/8} \sum_{h=1}^{p-1} \omega^{(v-pn)h^p} \\ &= (-1)^{(p^2-1)/8} \operatorname{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{v-pn}), \end{aligned}$$

where $v \equiv \frac{p^2+1}{2}u \pmod{p^2}$.

With α the automorphism of $\mathbb{Q}(\omega)$ determined by $\omega \mapsto \omega^{1+p}$, we now obtain the action of $U \simeq \operatorname{Gal}(E/\mathbb{Q})$ on the $A(p-3,p,n)$

$$\begin{aligned} \alpha(A(p-3,p,n)) &= (-1)^{(p^2-1)/8} \operatorname{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{(1+p)(v-pn)}) \\ &= (-1)^{(p^2-1)/8} \operatorname{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{v-p(n-v)}) \\ &= A(p-3,p,n-v). \end{aligned}$$

Thus the $\{A(p-3,p,n); n = 0,1,\dots,p-1\}$ form one orbit under the action of U. If n is such that $v - pn \equiv v^p \pmod{p^2}$, then

$$\begin{aligned} A(p-3,p,n) &= (-1)^{(p^2-1)/8} \operatorname{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{v^p}) \\ &= (-1)^{(p^2-1)/8} \operatorname{Tr}_{\mathbb{Q}(\omega)/E}(\omega) = \pm\rho \end{aligned}$$

and Theorem 1 follows.

THEOREM 5. *Let q and p be primes satisfying the Wieferich condition*

$$q^{p-1} \equiv 1 \pmod{p^2}.$$

Then $L(p,x) \pmod q$ splits into linear factors.

PROOF. Let R be the integral closure of $\mathbb{Z}$ in E, the ring of algebraic integers in E. Choose an element γ of (multiplicative) order p^2 in the finite field $\mathbb{F}_{q^{p-1}}$. Let $\phi\colon \mathbb{Z}[\omega] \to \mathbb{F}_{q^{p-1}}$ denote the homomorphism determined by $\phi(\omega) = \gamma$. Then $R \subset \mathbb{Z}[\omega]$, since $\mathbb{Z}[\omega]$ is the ring of algebraic integers in $\mathbb{Q}(\omega)$; see [5, Ch. IV, Theorem 3]. We shall show that $\phi(R) = \mathbb{F}_q$. Certainly $\phi(R)$ is an intermediate field $\mathbb{F}_q \subset \phi(R) \subset \mathbb{F}_{q^{p-1}}$, so $\mathrm{Gal}(\phi(R)/\mathbb{F}_q)$ is a cyclic group of order dividing $p-1$. By [6, Ch. VII, Proposition 2.5] $\mathrm{Gal}(\phi(R)/\mathbb{F}_q)$ is a subquotient of $\mathrm{Gal}(E/\mathbb{Q})$, the quotient of the decomposition group by the inertia group. As $\mathrm{Gal}(E/\mathbb{Q})$ is cyclic of order p, the only possibility is that $\mathrm{Gal}(\phi(R)/\mathbb{F}_q) = 1$, so that $\phi(R) = \mathbb{F}_q$.

As $\eta_n \in R$ we have $\phi(\eta_n) \in \mathbb{F}_q$, so that $\phi(L(p,x)) = \prod_{n=1}^{p}(x - \phi(\eta_n))$, and the theorem is proved. □

REMARK 1. If q, p is a Wieferich pair, Theorem 5 implies that q often divides the constant term $L(p,0)$ to some high power. We give a small table illustrating this phenomenon:

p	factor of $L(p,0)$
11	3^5
13	23^3
43	19^4
47	53^2
59	53^2
71	11^4
79	31^5
97	107^4
103	43^4
113	373^4
137	19^{14}
331	71^7
863	13^{80}
1093	2^{1102}

3. Granville's determinant.

In this section all matrix indices shall be interpreted in $\mathbb{Z}/p\mathbb{Z}$, with representatives $\{1, 2, \ldots, p\}$.

THEOREM 6. *Let $p \geq 3$ be a prime. Let $A = (a_{m,n})$ be the $p \times p$-matrix*

with

$$a_{m,n} = \begin{cases} -x & \text{if } m+n \equiv 0 \pmod{p}, \\ \exp\{2\pi i (m+n)^p/p^2\} & \text{otherwise.} \end{cases}$$

Then $\det(A) = (-1)^{(p+1)/2} L(p,x)$.

EXAMPLE 1. *Let* $p = 7$. *Then with* $\omega = \exp(2\pi i/49)$,

$$A = \begin{vmatrix} \omega^{30} & \omega^{31} & \omega^{18} & \omega^{19} & \omega^{48} & -x & \omega \\ \omega^{31} & \omega^{18} & \omega^{19} & \omega^{48} & -x & \omega & \omega^{30} \\ \omega^{18} & \omega^{19} & \omega^{48} & -x & \omega & \omega^{30} & \omega^{31} \\ \omega^{19} & \omega^{48} & -x & \omega & \omega^{30} & \omega^{31} & \omega^{18} \\ \omega^{48} & -x & \omega & \omega^{30} & \omega^{31} & \omega^{18} & \omega^{19} \\ -x & \omega & \omega^{30} & \omega^{31} & \omega^{18} & \omega^{19} & \omega^{48} \\ \omega & \omega^{30} & \omega^{31} & \omega^{18} & \omega^{19} & \omega^{48} & -x \end{vmatrix}.$$

We get $\det(A) = x^7 - 21x^5 - 21x^4 + 91x^3 + 112x^2 - 84x - 97 = L(7,x)$.

PROOF. Let $E_{i,j}$ be the $p \times p$-matrix with 1 in place (i,j) and 0 otherwise. Let

$$B = \sum_{i \neq j} \omega^{(i-j)^p} E_{i,j} \quad \text{and} \quad F = \sum_{j=1}^{p} E_{j,p-j}.$$

Let $C = xI - B$. Then we have $C = -FA$. Since $\det(F) = (-1)^{(p-1)/2}$ and the dimension p is odd, we get $\det(C) = (-1)^{(p+1)/2} \det(A)$, so $\det(A)$ is equal to the characteristic polynomial of the circulant B, up to sign. We find the eigenvalues of B.

PROPOSITION 7. (cf. [1, p. 123]) *For* $k = 0, 1, \ldots, p-1$ *the vector* $v_k = \sum_{j=1}^{p} \omega^{pjk} e_j$, *where* e_j *is the column vector with* 1 *at place* j *and* 0 *elsewhere, is an eigenvector of* B *with eigenvalue* $\rho_k = \sum_{j=1}^{p-1} \omega^{(1-pk)j^p}$.

PROOF. Introduce the matrix $T = \sum_{j=1}^{p} E_{j+1,j}$. Then $B = \sum_{j=1}^{p-1} \omega^{j^p} T^j$, and hence each eigenvector of T is an eigenvector of B. Now $Tv_k = \omega^{-pk} v_k$, so

$$\begin{aligned} Bv_k &= \sum_{j=1}^{p-1} \omega^{j^p} T^j v_k = \sum_{j=1}^{p-1} \omega^{j^p} \omega^{-pjk} v_k \\ &= \sum_{j=1}^{p-1} \omega^{(1-pk)j^p} v_k = \rho_k v_k, \end{aligned}$$

since $j^p \equiv j \pmod{p}$. □

As the ρ_k form one orbit of U acting on $\rho = \rho_0$,

$$\det(C) = \det(xI - B) = \prod_{k=0}^{p-1} (x - \rho_k) = L(p, x)$$

finishes the proof of Theorem 6. □

References

1. A. C. Aitken, *Determinants and Matrices.* Fifth edition. Oliver and Boyd, Edinburgh, 1948.

2. G. Almkvist, *Wilf's conjecture and a generalization.* Contemp. Math. 166, American Mathematical Society, Providence, RI, 1994, pp. 211–233.

3. T. Apostol, *Generalized Dedekind sums and transformation formulae of certain Lambert series.* Duke Math. J. **17** (1950), 147–157.

4. T. Dokshitzer, *On Wilf's conjecture and generalizations.* In: Number Theory. CMS Conf. Proc. 15, American Mathematical Society, Providence, RI, 1995, pp. 133–153.

5. S. Lang, *Algebraic Number Theory.* Graduate Texts in Mathematics 110, Springer-Verlag, New York, 1986.

6. S. Lang, *Algebra.* Third revised edition. Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2002.

7. D. H. Lehmer and E. Lehmer, In: *Cyclotomy for non-squarefree moduli.* In: Analytic Number Theory, Lecture Notes in Math. 899, Springer, Berlin, 1981, pp. 276–300.

Centre for Mathematical Sciences, Mathematics,
Lund University,
Box 118, SE-221 00 Lund,
Sweden
email: *gert@maths.lth.se*
arnem@maths.lth.se