1. Introduction.

In [2] a generalized Dedekind sum is 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

\[ A(r, k, n) = \sum_{(h,k)=1} \exp \{ \pi is(r, h, k) - 2\pi ihn/k \} \]

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

\( (r + 1, k) = 1 \) and \( (r + 1, \varphi(k)) = 1 \)

where \( \varphi \) is Euler’s totient function. In this note we study \( W(p - 3, p, x) \) which has integer coefficients if \( p \) is a prime \( \geq 5 \).

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

\[ \eta_n = \sum_{j=0}^{p-2} \exp \left\{ 2\pi ig^{p^2}(g^p + pn)/p^2 \right\} \]

and

\[ L(p, x) = \prod_{n=1}^{p} (x - \eta_n) \]

the period polynomial (see E. Lehmer and D.H. Lehmer [7]). We show that \( W(p - 3, p, x) \) and \( L(p, x) \) agree up to the sign of \( x \). In [7] the Lehmers ask if the constant term \( L(p, 0) \) could be even. We computed \( L(1093, 0) \) and found it divisible by \( 2^{1102} \) so it is even by some margin. 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 [2] a generalized Dedekind sum is 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

\[ A(r, k, n) = \sum_{(h,k)=1} \exp \{ \pi is(r, h, k) - 2\pi ihn/k \} \]

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

\( (r + 1, k) = 1 \) and \( (r + 1, \varphi(k)) = 1 \)

where \( \varphi \) is Euler’s totient function. In this note we study \( W(p - 3, p, x) \) which has integer coefficients if \( p \) is a prime \( \geq 5 \).

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

\[ \eta_n = \sum_{j=0}^{p-2} \exp \left\{ 2\pi ig^{p^2}(g^p + pn)/p^2 \right\} \]

and

\[ L(p, x) = \prod_{n=1}^{p} (x - \eta_n) \]

the period polynomial (see E. Lehmer and D.H. Lehmer [7]). We show that \( W(p - 3, p, x) \) and \( L(p, x) \) agree up to the sign of \( x \). In [7] the Lehmers ask if the constant term \( L(p, 0) \) could be even. We computed \( L(1093, 0) \) and found it divisible by \( 2^{1102} \) so it is even by some margin. 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. After reflection it is the characteristic polynomial of a circulant matrix.

2. Generalized Wilf polynomials.

In [2] it is 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 have to use $\omega = \exp(2\pi i / p^2)$. Let $G = \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ and $g$ a primitive root in $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Let $\alpha$ be the automorphism of $\mathbb{Q}(\omega)$ determined by $\omega \mapsto \omega^{1+p}$. Then we have

$$G = U \times V$$

where

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

$$V = \langle \omega \mapsto \omega^{hp} \rangle = \{ \omega \mapsto \omega^{hp} ; h = 1, 2, \ldots, p - 1 \}$$

Set

$$E = \mathbb{Q}(\omega)V = \mathbb{Q}(\rho)$$

where

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

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

**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 following two theorems:

**Theorem 2.** Let $u \in \mathbb{Z}$ be such that

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

Then

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

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. 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

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

for any integers \( h, H \) such that \( hH \equiv 1 \pmod{p} \).

Lemma 1. Let \( a \in \mathbb{Z}_p \) such that \(-2a \equiv 1 \pmod{p\mathbb{Z}_p} \). Define for \( H \in \mathbb{Z}, H \not\equiv 0 \pmod{p} \),

\[ f(H) = H^{-1} + aH^{p-2} \pmod{p^2 \mathbb{Z}_p} \]

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

\[
\begin{align*}
    f(H(1+p)) - f(H) &= \frac{1}{H(1+p)} + aH^{p-2}(1+p)^{p-2} - \frac{1}{H} - aH^{p-2} \\
    &= \frac{1}{H(1+p)} \left\{ 1 + aH^{p-1}(1+p)^{p-1} - 1 - p - a(1+p)H^{p-1} \right\} \\
    &\equiv \frac{1}{H(1+p)} \left\{ -p + aH^{p-1}(1-p-1) \right\} \\
    &\equiv \frac{p}{H(1+p)} \left\{ -1 - 2aH^{p-1} \right\} \\
    &\equiv \frac{p}{H(1+p)} \left\{ H^{p-1} - 1 \right\} \equiv 0 \pmod{p^2 \mathbb{Z}_p}
\end{align*}
\]

Proof of Theorem 2. As \( H^p \equiv H \pmod{p} \), using Lemma 1, we may replace \( H \) by \( H^p \) in the right hand side of (1). Hence

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

Here we used the fact that if \( hH \equiv 1 \pmod{p} \) then \( H^{pH} \equiv 1 \pmod{p^2} \).
With Theorem 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
\[
A(p - 3, p, n) = \sum_{h=1}^{p-1} \exp \left\{ \frac{\pi i}{p^2} p^2 s(p - 3, h, p) - 2\pi i \frac{hn}{p} \right\}
\]
\[
= \sum_{h=1}^{p-1} (-1)^{(p^2-1)/2} \omega^{(v-pn)h^p}
\]
\[
= (-1)^{(p^2-1)/8} \sum_{h=1}^{p-1} \omega^{(v-pn)h^p}
\]
where
\[
v \equiv \frac{p^2 + 1}{2} u \quad (\text{mod } p^2)
\]
With $\alpha$ the automorphism of $\mathbb{Q}(\omega)$ determined by $\omega \mapsto \omega^{1+p}$ we now obtain the action of $U \simeq \text{Gal}(E/\mathbb{Q})$ on the $A(p - 3, p, n)$
\[
\alpha(A(p - 3, p, n)) = (-1)^{(p^2-1)/8} \text{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{(1+p)(v-pn)})
\]
\[
= (-1)^{(p^2-1)/8} \text{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{v-p(n-v)})
\]
Thus the $\{A(p - 3, p, n); n = 0, 1, ..., p - 1\}$ form one orbit under the action of $U$. If $n$ is such that
\[
v - pn \equiv v^p \quad (\text{mod } p^2)
\]
then
\[
A(p - 3, p, n) = (-1)^{(p^2-1)/8} \text{Tr}_{\mathbb{Q}(\omega)/E}(\omega^{v^p})
\]
\[
= (-1)^{(p^2-1)/8} \text{Tr}_{\mathbb{Q}(\omega)/E}(\omega) = \pm \rho
\]
and Theorem 1 follows.

**Theorem 4.** Let $q$ and $p$ be primes satisfying the Wieferich condition
\[
q^{p-1} \equiv 1 \quad (\text{mod } p^2)
\]
Then $L(p, x) \mod q$ 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 $\gamma$ of (multiplicative) order $p^2$ in the finite field $\mathbb{F}_{q^{p-1}}$. Let
\[
\phi : \mathbb{Z}[\omega] \to \mathbb{F}_{q^{p-1}}
\]
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 e.g. [6] Chapter 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 $\text{Gal}(\phi(R)/\mathbb{F}_q)$ is a cyclic group of order dividing $p-1$. By [5] Chapter VII, Proposition 2.5 $\text{Gal}(\phi(R)/\mathbb{F}_q)$ is a subquotient of $\text{Gal}(E/\mathbb{Q})$, the quotient of the decomposition group by the inertia group. As $\text{Gal}(E/\mathbb{Q})$ is cyclic of order $p$, the only possibility is that $\text{Gal}(\phi(R)/\mathbb{F}_q) = 1$ 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. $\square$

**Remark** If $q, p$ is a Wieferich pair Theorem 4 implies that often $q$ divides the constant term $L(p, 0)$ to some high power. We give a small table of this phenomenon

| $p$  | factor of $L(p, 0)$ |
|------|---------------------|
| 11   | $3^3$               |
| 13   | $23^3$              |
| 43   | $19^4$              |
| 47   | $53^2$              |
| 59   | $53^2$              |
| 71   | $11^4$              |
| 79   | $31^9$              |
| 97   | $107^4$             |
| 103  | $43^4$              |
| 113  | $373^4$             |
| 137  | $19^{14}$           |
| 331  | $71^7$              |
| 863  | $13^{80}$           |
| 1093 | $2^{102}$           |

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 5.** Let $A = (a_{m,n})$ be the $p \times p$-matrix with

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

Then

$$\det(A) = (-1)^{(p+1)/2}L(p, x)$$
**Example:** Let $p = 7$. Then with $\omega = \exp(2\pi i/49)$

\[
A = \begin{bmatrix}
\omega^{30} & \omega^{31} & \omega^{18} & \omega^{48} & -x & \omega \\
\omega^{31} & \omega^{18} & \omega^{48} & -x & \omega & \omega^{30} \\
\omega^{18} & \omega^{19} & \omega^{48} & -x & \omega & \omega^{31} \\
\omega^{19} & \omega^{48} & -x & \omega & \omega^{30} & \omega^{18} \\
\omega^{48} & -x & \omega & \omega^{30} & \omega^{31} & \omega^{18} \\
-x & \omega & \omega^{30} & \omega^{31} & \omega^{18} & \omega^{48} \\
\omega & \omega^{30} & \omega^{31} & \omega^{18} & \omega^{19} & \omega^{48} & -x
\end{bmatrix}
\]

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

\[
B = \sum_{i \neq j} \omega^{(i-j)p} E_{i,j}
\]

and

\[
F = \sum_{j=1}^{p} E_{j,j-p}
\]

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 1.** (cf. [1], page 123) For $k = 0, 1, \ldots, p - 1$ the vector

\[
v_k = \sum_{j=1}^{p} \omega^{pj} e_j
\]

where $e_j$ is the column vector with 1 at place $j$ and 0 elsewhere, is an eigenvector of $B$ with eigenvalue

\[
\rho_k = \sum_{j=1}^{p-1} \omega^{(1-pk)j}
\]

**Proof.** Introduce the matrix

\[
T = \sum_{j=1}^{p} E_{j+1,j}
\]

Then

\[
B = \sum_{j=1}^{p-1} \omega^{j} T^j
\]

and hence each eigenvector of $T$ is an eigenvector of $B$. Now

\[
Tv_k = \omega^{-pk} v_k
\]
so

\[ Bv_k = \sum_{j=1}^{p-1} \omega^{j^p} T^j v_k = \sum_{j=1}^{p-1} \omega^{j^p} \omega^{-p^j k} v_k \]

\[ = \sum_{j=1}^{p-1} \omega^{(1-p^j)j^p} v_k = \rho_k v_k \]

since \( j^p \equiv j \pmod{p} \), completing the proof of the Proposition.

As the \( \rho_k \) 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 5.

**References**

[1] A.C. Aitken, *Determinants and Matrices*, 5th ed., Oliver and Boyd, Edinburgh and London, 1948.

[2] G. Almkvist, *Wilf’s conjecture and a generalization*, Contemp. Math. **166** (1994), 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** (1995), 133–153.

[5] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

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

[7] D.H. and Emma Lehmer, *Cyclotomy for non-squarefree moduli*, Lecture Notes in Math. **899** (1981), 276–300.

Centre for Mathematical Sciences, Mathematics, Lund University, Box 118, SE-221 00 Lund, Sweden

E-mail address: gert@maths.lth.se, arnem@maths.lth.se