JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

R. A. MOLLIN
H. C. WILLIAMS

# On the period length of some special continued fractions

*Journal de Théorie des Nombres de Bordeaux 2^e série*, tome 4, n° 1 (1992), p. 19-42

<http://www.numdam.org/item?id=JTNB_1992__4_1_19_0>

*Séminaire de Théorie des Nombres,*
*Bordeaux 4 (1992), 19-42*

# On the period length of some special continued fractions.

par R. A. MOLLIN AND H. C. WILLIAMS

ABSTRACT. We investigate and refine a device which we introduced in [3] for the study of continued fractions. This allows us to more easily compute the period lengths of certain continued fractions and it can be used to suggest some aspects of the cycle structure (see [1]) within the period of certain continued fractions related to underlying real quadratic fields.

## 1. Introduction.

Let $r$ and $s$ be positive integers with $s > r$ ; and define $M(r,s)$ to be the value of $n$ in the continued fraction expansion

$$\frac{s}{r} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}}},$$

where $q_n > 1$.

This may be interpreted as $M(r,s) = T(r,s) - 2$ where $T(r,s)$ is the function of Knuth [2, p. 344].

Let $\gcd(a,q) = 1$ where $a$ and $q$ are positive integers with $a \neq 1$. Set

$$s_i \equiv a^i \pmod{q}$$

where $0 < s_i < q$ and define

$$W(a,q) = 2\sum_{i=1}^{\omega} \lfloor (M(s_i,q)+1)/2 \rfloor \tag{1.1}$$

where $\omega$ is the order of $a$ modulo $q$, and $\lfloor\ \rfloor$ denotes the greatest integer function.

Manuscrit reçu le 19 avril 1991, version révisée le 27 janvier 1992 .

In [3] we proved that if $N = \left(\frac{\sigma}{2}(qa^n + (a^k - 1)/q)\right)^2 + \sigma^2 a^n$ is an integer with

$$\sigma = \left\{ \begin{array}{l} 2 \text{ if } N \equiv 1 (\text{mod } 4) \\ 1 \text{ if } N \equiv 2, 3 (\text{mod } 4) \end{array} \right\}$$

then the continued fraction expansion of $(\sigma - 1 + \sqrt{N})/\sigma$ has period length $\pi$ given by

$$\pi = \frac{1}{d}\left(2n + \frac{k}{\kappa} W'(n, q)\right)$$

when $qa^n > a^k$. Here $\kappa = \omega/\gcd(\omega, n)$, $d = \gcd(n, k)$ and

$$W'(n, q) = \sum_{i=1}^{\kappa} (2\lfloor (M(s_i, q) + 1)/2 \rfloor + 1).$$

(Note that we have made the assumption that $a$, while arbitrary, has been fixed.) It seems, however, to be more appropriate to use the function $W(a, q)$ defined in (1.1). The reason for this is that we may always assume that $d = 1$. (If $d \neq 1$, then replace $a$ by $a^d$, $k$ by $k/d$ and $n$ by $n/d$). Under the condition that $\gcd(n, k) = 1$ we get

$$\pi = 2n + k + \frac{k}{\omega} W(a, q)$$

Bernstein [1] noticed that for certain parametric forms of $D$, the continued fraction expansion of $\sqrt{D}$ has a certain cycle structure within the period. Usually these cycles were not very long, but in some "remarkable" cases he found cycles of length 11. In fact it is possible to develop certain forms of $N$ for which the cycle structure of the continued fraction expansion of $(\sigma - 1 + \sqrt{N})/\sigma$ is quite intricate. A detailed description of this will form the subject of a future paper. For now we will content ourselves with the following example.

Consider the case where $q = a^\omega - 1$ and $k = m\omega$. As we shall see in §2 it is possible in this case to show that $W(a, q) = 2\omega - 2$. Therefore, $\pi = 2n + 3m\omega - 2m$ when $\gcd(n, m\omega) = 1$ and $n > m\omega$. If we put $n = m\omega + 1$ we get $\pi = (5\omega - 2)m + 2$.

Thus for

$$N = \left(\frac{\sigma}{2}((a^\omega - 1)\, a^{m\omega+1} + (a^{m\omega} - 1))\right)^2 + \sigma^2\, a^{m\omega+1}$$

a square-free integer, we get cycles in the continued fraction expansion of $(\sigma - 1 + \sqrt{N})/\sigma$ of length $5\omega - 2$ when $\omega$ is fixed. More complicated cycle structures can also be predicted when we have further results on $W(a, q)$.

It is easy to show that if $m < q/2$ then

$$M(q - m, q) = M(m, q) + 1 \tag{1.2}$$

Hence,

$$\left\lfloor \frac{M(m,q)+1}{2} \right\rfloor + \left\lfloor \frac{M(q-m,q)+1}{2} \right\rfloor = \frac{M(m,q) + M(q-m,q) + 1}{2}.$$

Now, (in what follows all summations assume $\gcd(m, q) = 1$),

$$\begin{aligned}
W(a,q) &\le 2 \sum_{1 \le m < q} \left\lfloor \frac{M(m,q)+1}{2} \right\rfloor \\
&= 2 \left( \sum_{1 \le m < q/2} \left\lfloor \frac{M(m,q)+1}{2} \right\rfloor + \sum_{q/2 < m < q} \left\lfloor \frac{M(q-m,q)+1}{2} \right\rfloor \right) \\
&= 2 \sum_{1 \le m < q/2} \left\lfloor \frac{M(m,q)+1}{2} \right\rfloor + \left\lfloor \frac{M(m,q)+1}{2} \right\rfloor \\
&= \sum_{1 \le m < q/2} M(m,q) + M(q-m,q) + 1 \\
&= \sum_{1 \le m < q} M(m,q) + \phi(q)/2 \\
&= \sum_{1 \le m < q} T(m,q) - 3\,\phi(q)/2 \\
&= \phi(q)\ (\tau_q - 3/2),
\end{aligned}$$

(For the definition of $\tau_q$ see Knuth [2, p. 353]). By a result of Porter [5], we know that

$$\begin{aligned}
\tau_q &= \frac{12 \log 2}{\pi^2} \log q + C + O(q^{-1/6+\epsilon}), \\
C &= \frac{6 \log 2}{\pi^2} (3 \log 2 + 4\gamma - 24\pi^2 \zeta'(2) - 2) - 1/2 \\
&\approx 1.4670780794.
\end{aligned}$$

Also $\phi(q) \le q - 1$ and so we have an upper bound on the value of $W(a, q)$, a bound which is quite good when $q$ is a prime and a is a primitive root of

$q$. For example, 2 is a primitive root of 37 and $W(2,37) = 106$ by direct calculation, whereas

$$36\left(\frac{12\ \log\ 2}{\pi^2}\ \log\ 37 - .032921921\right) = 108.368518.$$

The purpose of this paper is to develop methods for improving the speed of computing $W(a,q)$ beyond that of simply using (1.1).

## 2. Some Alternate Expressions for $W(a,q)$.

We will show in this section how the work of computing $W(a,q)$ can be halved. We first require

LEMMA 2.1. *If* $xy \equiv 1\ (mod\ q)$ *with* $0 < x, y < q$ *then*

$$\left\lfloor \frac{M(x,q)+1}{2} \right\rfloor = \left\lfloor \frac{M(y,q)+1}{2} \right\rfloor .$$

*Proof.* This can be easily proved by making use of results of Perron [4, p. 32].

□

We note that since $s_i\, s_{\omega-i} \equiv 1\ (\text{mod } q)$, we have :

$$\left\lfloor \frac{M(s_i,q)+1}{2} \right\rfloor = \left\lfloor \frac{M(s_{\omega-i},q)+1}{2} \right\rfloor . \tag{2.1}$$

Hence we can write

$$W(a,q) = 4 \sum_{i=1}^{(\omega-1)/2} \left\lfloor \frac{M(s_i,q)+1}{2} \right\rfloor \tag{2.2}$$

when $\omega$ is odd and

$$W(a,q) = 4 \sum_{i=1}^{\omega/2-1} \left\lfloor \frac{M(s_i,q)+1}{2} \right\rfloor + 2 \left\lfloor \frac{M(s_{\omega/2},q)+1}{2} \right\rfloor \tag{2.3}$$

when $\omega$ is even.

If $a^{\omega/2} \equiv -1 \pmod{q}$, then $2\left\lfloor \frac{M(s_{\omega/2}, q)+1}{2} \right\rfloor = 2$ and

$$W(a,q) = 4\sum_{i=1}^{\omega/2-1}\left\lfloor \frac{M(s_i,q)+1}{2}\right\rfloor + 2 \tag{2.4}$$
$$= 4\sum_{i=1}^{\omega/2}\left\lfloor \frac{M(s_i,q)+1}{2}\right\rfloor - 2$$

Notice that if $q = a^{\omega} - 1$, then for $i < \omega$, we have $s_i = a^i$ and $q = a^{\omega} - 1 = (a^{\omega-i} - 1)s_i + a^i - 1$ whereas $s_i = a^i = 1(a^i - 1) + 1$. Hence, $M(s_i, q) = 2$. It follows from (1.1) that

$$W(a, a^{\omega} - 1) = 2\omega - 2. \tag{2.5}$$

Also, if $q = a^{\mu}+1$ then $\omega = 2\mu$ and $s_i = a^i$ for $i \leq \omega/2$. Hence $M(s_i, q) = 1$ for $i \leq \omega/2$ and by (2.4)

$$W(a,\ a^{\mu} + 1) = 4\mu - 2. \tag{2.6}$$

Thus, if $q = a^{\mu} \pm 1$ it is easy to evaluate $W(a,q)$. In the next several sections we will show how to develop formulas for determining the value of $W(a,(a^{\mu} \pm 1)/q)$ in terms of $W(a,q)$ when $a^{\mu} \equiv \pm 1 \pmod{q}$. We will concentrate on the more difficult problem of finding the value of $W(a,(a^{\mu}+1)/q)$ in terms of the value of $W(a,q)$, but will indicate from time to time how the simpler proof for the value of $W(a,(a^{\mu}-1)/q)$ in terms of $W(a,q)$ can be developed. In fact we will show the following.

**Main Results.** In sections 4 and 5 we prove

THEOREM 2.1. (see 5.10).

$$W(a,(a^{\mu}+1)q) = \kappa W(a,q)+6\mu-2\lambda-8\alpha-4\lfloor 2q/a^{\lambda+1}\rfloor+4\lfloor 3a^{\alpha}/2q\rfloor+4\,S(a,q)-8$$

*where $\lambda$ is the least positive integer such that $a^{\lambda} \equiv -1$ (mod $q$), $\alpha$ is defined by $a^{\alpha} < q < a^{\alpha+1}$, and*

$$S(a,q) = \sum_{a^j<q/2}\chi_j + \sum_{a^j>2q}^{\lambda}\chi_j$$

*with*

$$\chi_j = \left\{ \begin{array}{l} 1 \text{ when } a^j > 2q \text{ and } a^j/q - \lfloor a^j/q \rfloor > 1/2 \\ -1 \text{ when } a^j < q/2 \text{ and } q/a^j - \lfloor q/a^j \rfloor > 1/2 \\ 0 \text{ otherwise} \end{array} \right\},$$

*(here* $a \neq 2$, $q \neq 3$ *and* $(a^\mu + 1)/q > q$*).*

THEOREM 2.2. (see (5.11)).

*If* $\mu$ *is the order of* $a$ *modulo* $Q = (a^\mu - 1)/q > q$ *then*

$$W(a, Q) = (\mu/\omega)\, W(a, q) + 2\mu - 4\alpha - 2.$$

In section 6 we conclude with some

Special Cases.

THEOREM 2.3. (see (6.2)).

$$W\left\{a, \frac{a^\mu - 1}{a^\omega - 1}\right\} = 4\mu - 4\omega + 2 - 2\mu/\omega.$$

THEOREM 2.4. (see (6.3)).

*If* $a^\lambda + 1 \neq 3$ *then*

$$W\left\{a, \frac{a^\mu + 1}{a^\lambda + 1}\right\} = 10\mu - 10\lambda - 2\mu/\lambda - e \quad \text{where } e = \left\{ \begin{array}{l} 4 \text{ if } a > 2 \\ 8 \text{ if } a = 2 \end{array} \right\}.$$

Finally,

THEOREM 2.5. (see (6.4)).

$W(2, (2^\mu + 1)/3) = 8\mu - 18$ *for* $\mu > 3$

*and*

$$W(a, (a^\mu + 1)/2) = \left\{ \begin{array}{ll} 8\mu - 10 & \text{when } a = 3 \\ 8\mu - 6 & \text{when } a > 3 \end{array} \right\}.$$

## 3. Some Intermediate Results.

Let $j$ be an arbitrary but fixed integer such that $1 \leq j \leq \omega$. Define $\gamma = \gamma_j \equiv a^{-j} \pmod{q}$ and $\gamma^* = \gamma_j^* \equiv -a^{-j} \pmod{q}$, where $0 < \gamma, \gamma^* < q$. Put $t_{-2} = t_{-2}^* = q, t_{-1} = \gamma, t_{-1}^* = \gamma^*$ and define $t_i, t_i^*$ by

$$t_{i-2} = \mu\, t_{i-1} + t_i \text{ with } \mu_i = \left\lfloor \frac{t_{i-2}}{t_{i-1}} \right\rfloor,$$

$$t_{i-2}^* = \mu_i^*\, t_{i-1}^* + t_i^* \text{ with } \mu_i^* = \left\lfloor \frac{t_{i-2}^*}{t_{i-1}^*} \right\rfloor$$

Also, put $A_{-2} = A_{-2}^* = 0; B_{-2} = B_{-2}^* = 1;$

$$\begin{aligned} A_{-1} &= A_{-1}^* = 1; B_{-1} = B_{-1}^* = 0 \text{ and} \\ A_{i+1} &= \mu_{i+1}\, A_i + A_{i-1}, \\ A_{i+1}^* &= \mu_{i+1}^*\, A_i^* + A_{i-1}^*, \\ B_{i+1} &= \mu_{i+1}\, B_i + B_{i-1}, \\ B_{i+1}^* &= \mu_{i+1}^*\, B_i^* + B_{i-1}^* \end{aligned}$$

for $i = -1, 0, 1, 2, \ldots$

Put $m = m_j = 2\left\lfloor \frac{M(\gamma, q) + 1}{2} \right\rfloor,$

$m^* = m_j^* = \left\lfloor \frac{M(\gamma^*, q) + 1}{2} \right\rfloor,$

$M = M_j = 2\left\lfloor \frac{M(S, Q) + 1}{2} \right\rfloor,$ and

$M^* = M_j^* = 2\left\lfloor \frac{M(S^*, Q^*) + 1}{2} \right\rfloor$ where $Q$ is as in Theorem 2.2,

$Q^* = (a^\mu + 1)/q \geq 3$ and $S \equiv a^j \pmod{Q}$, $S^* \equiv a^j \pmod{Q^*}$.

If $M(\gamma, q)$ is even, then $m = M(\gamma, q)$, $t_m = 0$ and $t_{m-1} = 1$. If $M(\gamma, q)$ is odd then $m = M(\gamma, q) + 1$. We replace the value of $\mu_{m-1}$ by that of $\mu_{m-1} - 1$ and put $\mu_m = 1$, $t_m = 0$, $t_{m-1} = 1$ and $t_{m-2} = 1$. We deal with the continued fraction expansion of $q/\gamma^*$ in the same way.

The purpose of this section is to relate the value of $M$ to that of $m$ and the value of $M^*$ to that of $m^*$. We divide the problem into 2 cases.

**Case 1 :** $Q > a^j$ $(Q^* > a^j)$. Here $S = S^* = a^j$.

Define $r_{-2} = q$ and $r_i = (t_{i-1}\ a^j + (-1)^{i-1}A_{i-1})/q$,

$$r_i^* = (t_{i-1}^*\ a^j + (-1)^i A_{i-1}^*)/q \quad (i \geq -1).$$

We have that $r_{-1}$, $r_{-1}^*$, $r_0$, $r_0^*$ are integers.

$$\begin{aligned} r_{-2} &= ((a^{\mu-j} - \gamma)/q)r_{-1} + r_0, \\ r_{-2}^* &= ((a^{\mu-j} - \gamma^*)/q)r_{-1}^* + r_0, \\ r_{i-1} &= \mu_i\ r_i + r_{i+1}, \\ r_{i-1}^* &= \mu_i^*\ r_i^* + r_{i+1}^* (i \geq 0). \end{aligned}$$

Thus for $i \geq -2$ we have that $r_i$ and $r_i^*$ are integers.

LEMMA 3.1. *If* $-2 \leq i < m^* - 3$ *then* $r_i^* > r_{i+1}^*$.

**Proof.** The result certainly holds for $i = -2, -1, 0$. Also the result holds if $i$ is even. Now since $r_i$ is an integer we get

$$t_{i-1}^* a^j \equiv (-1)^{i+1}\ A_{i-1} \pmod{q}$$
$$\text{and}\ \ 0 < A_{i-1}^* < A_{m^*}^* = q, \ \text{with}\ \ t_{i-1}^*\ a^j > 0.$$

Thus, if $i$ is odd and $r_i \leq 0$, then we can only have $r_i^* = 0$. But $r_i^* = 0$ only if $t_{i-j}^* a^j = A_{i-1}^*$. Since

$$A_{i-1}^*\,\gamma^* - q\ B_{i-1}^* = (-1)^i\ t_{i-1}^*, \tag{3.1}$$

we get

$$t_{i-1}^*(a^j\gamma^* + 1)/q = B_{i-1}^*.$$

Thus, gcd $(A_{i-1}^*, B_{i-1}^*) \equiv 0 \pmod{t_{i-1}^*}$ ; whence $t_{i-1}^* = 1$. It follows that $i - 1 = m^* - 1$ or $i - 1 = m^* - 2$. Since $m^*$ is even and $i$ is odd we get $i = m^* - 1$, which is impossible since $i < m^* - 1$.

LEMMA 3.2. *If* $-2 \leq i < m^* - 3$ *then* $r_i^* > r_{i+1}^*$.

**Proof.** The result is certainly true for $i = -2, -1$. Now if $i \geq 0$,

$$q(r_i^* - r_{i+1}^*) = (t_{i-1}^* - t_i^*)a^j + (-1)^i\ (A_{i-1}^* + A_i^*); \tag{3.2}$$

thus if $i$ is even, we get $r_i^* > r_{i+1}^*$. If $i$ is odd, $i \leq m^* - 3$ and $r_i^* \leq r_{i+1}^*$, then $r_i^* = r_{i+1}^*$. For

$$a^j\, t_{i-1}^* \equiv A_{i-1}^* \pmod{q},$$
$$a^j\, t_i^* \equiv -A_i^* \pmod{q},$$

and $0 \leq A^*_{i-1},\ A^*_i \leq A^*_{m^*} = q$.

Thus

$$a^j t^*_{i-1} = A^*_{i-1} + s_1 q,$$
$$a^j t^*_i = -A^*_i + s_2 q,$$

where $s_1$, $s_2$ are integers,

$$a^j(t^*_{i-1} - t^*_i) = A^*_{i-1} + A^*_i + (s_1 - s_2)q,$$

and

$$r^*_i - r^*_{i+1} = s_1 - s_2.$$

If $r^*_i \leq r^*_{i+1}$ then $s_1 - s_2 \leq 0$. Now $A^*_i + A^*_{i-1} \leq A^*_{i+1} < A^*_{m^*} = q$ ; thus, if $s_1 - s_2 \neq 0$, then $s_1 - s_2 \leq -1$ and $t^*_{i-1} < t^*_i$ which is impossible.

Hence $s_1 = s_2$ and $r^*_i = r^*_{i+1}$. Also,

$$a^j\ \mu^*_{i+1}\, t^*_i = -\mu^*_{i+1}\ A^*_i + \mu^*_{i+1} s_2 q \qquad (s_2 > 0),$$
$$a^j\ t^*_{i-1} = A^*_{i-1} + s_2 q\,;$$

hence,

$$a^j(\mu^*_{i+1} t^*_i - t_{i-1}) = -(\mu^*_{i+1}\ A^*_i + A^*_{i-1}) + s_2(\mu^*_{i+1} - 1)q$$

and,

$$0 < a^j\, t^*_{i+1} = A^*_{i+1} - s_2(\mu^*_{i+1} - 1)q.$$

Since $A^*_{i+1} < A^*_{m^*} = q$ we have $\mu^*_{i+1} = 1$, and $a^j\, t^*_{i+1} = A^*_{i+1}$. By the same reasoning as that used in Lemma 3.1 we can now prove Lemma 3.2.

□

We use the notation $\{x\}$ to denote the fractional part of any real $x$; i.e., $\{x\} = x - \lfloor x \rfloor$.

We are now able to prove

THEOREM 3.3. *If $q \neq 2$ and $a^j < Q^*$ then $M^* = m^* + 4$ when $a^j > 2q$ and $\{a^j/q\} > 1/2$, $M^* = m^* - 2$ when $a^j < q/2$ and $\{q/a^j\} > 1/2$ ; otherwise, $M^* = m^* + 2$ when $a^j > 2q/3$ and $M^* = m^*$ when $a^j < 2q/3$.*

**Proof.** For convenience we will use the symbol $k$ to represent $m^*$. We divide the proof into two cases.

**Case A.** $a^j < q$.

From (3.1) we have $A^*_{k-1}\ \gamma^* \equiv 1 \pmod{q}$; hence, $A^*_{k-1} \equiv -a^j \pmod{q}$ and $A^*_{k-1} = q - a^j$, since $0 < A^*_{k-1} < A^*_k = q$. It follows that $A^*_{k-2} = q - \mu^*_k(q - a^j)$ and $\mu^*_k = \lfloor q/(q-a^j)\rfloor$. Thus $\mu^*_k = 1$ if and only if $a^j < q/2$. Also, if $\mu^*_k = 1$, then $t^*_{k-2} = 1$ and $A^*_{k-2} = a^j$.

By definition of $r^*_{k-1}$ we get $r^*_{k-1} = 0$, hence $k > 1$. Also $t^*_{k-3} = \mu^*_{k-1} + 1$ and $A^*_{k-3} = A^*_{k-1} - \mu^*_{k-1}A^*_{k-2} = q - a^j\ t^*_{k-3}$. From this we can deduce that $r^*_{k-2} = 1$ and $r^*_{k-3} = r^*_{k-1} + \mu^*_{k-2}\ r^*_{k-2} = \mu^*_{k-2}$. If $\mu^*_{k-2} > 1$ then $r^*_{k-3} > r^*_{k-2} > r^*_{k-1} = 0$. By Lemmas 3.1 and 3.2 we see that $M(S^*, Q^*) = k - 1$. Since $k$ is even we have $M^* = k = m^*$.

If $\mu^*_{k-2} = 1$, then $r^*_{k-3} = r^*_{k-2} = 1$. In this case we get $M(S^*, Q^*) = k-2$ and $M^* = m^* - 2$. Now

$$\mu^*_{k-1} = \left\lfloor \frac{A^*_{k-1}}{A^*_{k-2}} \right\rfloor = \left\lfloor \frac{q - a^j}{a^j} \right\rfloor = \left\lfloor \frac{q}{a^j} \right\rfloor - 1,$$

$$A^*_{k-3} = q - a^j - a^j\left(\left\lfloor \frac{q}{a^j} \right\rfloor - 1\right) = q - a^j \left\lfloor \frac{q}{a^j} \right\rfloor.$$

Also $\mu^*_{k-2} = 1$ if and only if $A^*_{k-2}/A^*_{k-3} < 2$, which holds if and only if

$$a^j < 2\left(q - a^j \left\lfloor \frac{q}{a^j} \right\rfloor\right)$$

or

$$\left\{ \frac{q}{a^j} \right\} > 1/2$$

if $\mu^*_k > 1$, we get

$$r^*_{k-1} = \frac{\mu^*_k\ a^j - q + \mu^*_k(q - a^j)}{q} = \mu^*_k - 1,$$

and

$$t^*_{k-2} = \mu^*_k\ t^*_{k-1} + t^*_k = \mu^*_k > 1.$$

Since $t^*_{k-2} \neq 1$, we cannot have $r^*_{k-3} = r^*_{k-2}$ ; thus, $r^*_{k-3} > r^*_{k-2}$.

If $r^*_{k-1} \geq 2$, then $r^*_{k-3} > r^*_{k-2} > r^*_{k-1} > r^*_k = 1$.

In this case $M(S^*, Q^*) = k + 1$ and $M^* = m^* + 2$.

If $r^*_{k-1} = 1$, then $r^*_{k-3} > r^*_{k-2} > r^*_{k-1} = r^*_k = 1$, and

$$M(S^*, Q^*) = k, \; M^* = m^*.$$

Since $\mu_k^* = \lfloor A_k^*/A_{k-1}^* \rfloor = \lfloor q/(q-a^j) \rfloor$, we see that $r_{k-1}^* = \mu_k^* - 1 = 1$ if and only if $2 < q/(q-a^j) < 3$ ; i.e., $q/2 < a^j < 2q/3$. Also $r_{k-1}^* \geq 2$ if and only if $a^j > 2q/3$.

**Case B.** $a^j > q$.

By (3.2) with $i = k-3$ we must have $r_{k-3}^* > r_{k-2}$. Also $r_{k-2}^* > r_{k-1}^*$ and $r_{k+1}^* = -1$. Now $r_{k-1}^* \leq r_k^*$ if and only if $(t_{k-2}^* - 1)a^j \leq A_{k-2}^* + A_{k-1}^* \leq A_k^* = q$. Since $q/a^j < 1$, this can occur if and only if $t_{k-2}^* = \mu_k^* = 1$. In this case we get $r_k^* - r_{k-1}^* = 1$, and $r_{k-2}^* = \mu_{k-1}^* r_{k-1}^* + r_k^* = (\mu_{k-1}^* + 1)r_{k-1}^* + 1$. Hence $M(S^*, Q^*) = k+1$ and $M^* = m^* + 2$. Now $t_{k-2}^* = 1$ if and only if $A_k^*/A_{k-1}^* < 2$. Also, since $A_{k-1}^* \equiv -a^j \pmod{q}$ and $A_{k-1}^* < q$, we get $0 < A_{k-1}^* = tq - a^j < q$, where $t = \lfloor a^j/q \rfloor + 1$. Since $A_k^* = q$ we see that $t_{k-1}^* = 1$ if and only if $\{a^j/q\} < 1/2$.

We have seen that if $\mu_k^* > 1$ then $r_{k-1}^* > r_k^*$. Also

$$r_{k-1}^* = (\mu_k^* - 1)r_k^* + r_k^* - 1.$$

If $r_k^* = 2$ then $M(S^*, Q^*) = k+2$ and $M^* = m^* + 2$. If $r_k^* > 2$ then $r_k^* = 1(r_k^* - 1) + 1$, $M(S^*, Q^*) = k+3$ and $M^* = m^* + 4$. Also, $r_m^* = 2$ if and only if $a^j + A_{k-1}^* = 2q$. Since $A_{k-1}^* \equiv -a^j \pmod{q}$, this can hold if and only if $q < a^j < 2q$. Collecting all of the above we get the Theorem.

□

THEOREM 3.4. *If $a^j < Q$ then $M = m+2$ when $a^j > q$ and $M = m$ when $a^j < q$.*

**Proof.** Use similar reasoning on the $r_i$ sequence to get results similar to Lemmas 3.1 - 3.2. The result then follows.

□

**Case 2.** $Q < a^j$ $(Q^* < a^j)$

Here we define $r_{-2} = q$ and

$r_i = (Qt_i + (-1)^i B_i)/a^h$,

$r_i^* = (Qt_i^* + (-1)^{i-1} B_i^*)/a^h$,

where $h = \mu - j$. In this case $\gamma_j = \gamma_j^* = a^h < q$.

As before $r_{-1}$, $r_{-1}^*$, $r_0$, $r_0^*$ are integers. Also (for $i \geq -2$)

$r_{i-2} = \mu_i\, r_{i-1} + r_i,$

$r^*_{i-2} = \mu^*_i\, r^*_{i-1} + r^*_i.$

By using methods similar to those used above we can prove.

LEMMA 3.5. *If* $-2 \leq i < m^* - 3$ *then* $r^*_i > 0$.

LEMMA 3.6. *If* $-2 \leq i < m^* - 5$ *then* $r^*_i > r^*_{i+1}$.

THEOREM 3.7. *If* $a^j > Q$ *then* $M^* = m^* - 4$ *when* $Q^* < a^h/2$ *and* $\{a^h/Q^*\} > 1/2$, $M^* = m^* + 2$ *when* $Q^* > 2a^h$ *and* $\{Q^*/a^h\} > 1/2$ ; *otherwise,* $M^* = m^* - 2$ *when* $Q < 2a^h/3$ *and* $M^* = m^*$ *when* $Q > 2a^h/3$.

THEOREM 3.8. *If* $a^j > Q$ *then* $M = m-2$ *when* $a^h > Q$ *and* $M = m$ *when* $a^h < Q$.

In the next sections we refine some of these results.

## 4. Some Refinements.

We will need to put Theorems 3.3 and 3.7 into forms in which we can use them to relate $W(a, Q^*)$ to $W(a, q)$. We do that in this section.

LEMMA 4.1. *If* $j > 0$ *and* $h = \mu - j$ *then* $\lfloor q/a^j \rfloor = \lfloor a^h/Q^* \rfloor$.

**Proof.** $a^h/Q^* = a^h q/(a^\mu + 1) = q/(a^j + a^{-h}) < q/a^j$.

If $\lfloor q/a^j \rfloor \neq \lfloor a^h/Q^* \rfloor$ then $\lfloor a^h/Q \rfloor \leq \lfloor q/a^j \rfloor - 1$.

Let $1 > a^h/Q - \lfloor a^h/Q^* \rfloor = \epsilon_1 > 0$ and $q/a^j - \lfloor q/a^j \rfloor = \epsilon_2 > 0$. Note that $\epsilon_1 \leq 1 - 1/Q^*$. Also, $a^h/Q^* - q/a^j = -1/(Q^* a^j)$ thus, if $\lfloor a^h/Q^* \rfloor \leq \lfloor q/a^j \rfloor - 1$ then $-1/(Q^* a^j) \leq \epsilon_1 - \epsilon_2 - 1 \leq -1/Q^* - \epsilon_2$, and $1/(Q^* a^j) > 1/Q^*$ which is impossible.

It follows that $\lfloor q/a^j \rfloor = \lfloor a^h/Q^* \rfloor$.

□

LEMMA 4.2. $\{a^h/Q^*\} > 1/2$ *if and only if* $\{q/a^j\} > 1/2$

**Proof.** Let $q = a^j m_1 + r_1$ for $0 < r_1 < a^j$, and $a^h = Q^* m_2 + r_2$ for $0 < r_2 < Q^*$.

By Lemma 4.1 we have that $\lfloor q/a^j \rfloor = m_1 = m_2 = \lfloor a^h/Q^* \rfloor$. Also, since $a^h/Q^* < q/a^j$, we see that if $a^h/Q^* - \lfloor a^h/Q^* \rfloor > 1/2$ then $q/a^j - \lfloor q/a^j \rfloor >$

$1/2$. If $q/a^j - m_1 > 1/2$, then $r_1/a^j > 1/2$ and $r_1 \geq (a^j+1)/2$. Hence, $q/a^j - m_1 \geq 1/2 + 1/(2a^j)$. Now, $a^h/Q^* - m_2 - (q/a^j - m_1) = -1/(Q^* a^j)$, hence

$$a^h/Q^* - \lfloor a^h/Q^* \rfloor = r_1/a^j - 1/Q^* a^j \geq 1/2 + 1/(2a^j) - 1/(Q^* a^j) > 1/2.$$

□

LEMMA 4.3. *If $h = m - j$, then $Q^* < a^h/2$ if and only if $a^j < q/2$.*

**Proof.** If $Q^* < a^h$ then $(a^u+1)/q < a^h/2$, $q > 2(a^{\mu-h}+a^{-h})$ and $q > 2a^j$. If $q > 2a^j$, we must have $a^h \geq 2$. For if $a^h = 1$, then $\mu = j$ and $Q^* = (a^j+1)/q$. Since $Q^* > 1$ we would have $q < a^j$ which is not possible. Also if $q > 2a^j$ then $q \geq 2a^j + 1 = 2(a^j + 1/2) \geq 2(a^{\mu-h} + a^{-h}) \geq 2a^{-h}(a^\mu + 1)$. It follows that $Q^* < a^h/2$. (here $\gcd(Q^*, a) = 1$ and $h \geq 1$).

□

LEMMA 4.4. *If $h = \mu - j$, then $Q^* < 2a^h/3$ if and only if $a^j < 2q/3$.*

**Proof.** If $Q^* < 2a^h/3$ then $a^j + a^{-h} < 2q/3$ and $a^j < 2q/3$. If $a^j < 2q/3$ then $a^{\mu-h} < 2q/3$ and $3a^\mu = 2qa^h - k$ for $k > 0$. Since $k \equiv 0 \pmod{a^h}$ we have $k \geq a^h$ and it follows that $a^\mu \leq 2qa^h/3 - a^h/3$. If $a^h/3 > 1$, then $Q^* = (a^\mu+1)/q < 2a^h/3$. If $a^h/3 \leq 1$, then $h = 1$, $a = 2, 3$. If $a^h = 3$ then $3^\mu \leq 2q - 1$ and $q \geq (3^\mu + 1)/2$ which means that $Q^* \leq 2$, an impossibility. By similar reasoning it is possible to exclude the case where $a^h = 2$.

□

By using the same kind of reasoning as that used above we can also prove.

LEMMA 4.5. *If $h = \mu - j$ then $Q^* > 2a^h$ if and only if $a^j > 2q$.*

LEMMA 4.6. *If $h = \mu - j > 0$ then $\lfloor a^j/q \rfloor = \lfloor Q^*/a^h \rfloor$ and $\{Q^*/a^h\} > 1/2$ if and only if $\{a^j/q\} > 1/2$.*

With these results we can now give a different version of Theorem 3.7.

THEOREM 4.7. *If $j \neq \mu$ and $a^j > Q$ then $M^* = m^* - 4$ when $a^j < q/2$ and $\{q/a^j\} > 1/2$, $M^* = m^* + 2$ when $a^j > 2q$ and $\{a^j/q\} > 1/2$ ; otherwise, $M^* = m^* - 2$ when $a^j < 2q/3$ and $M^* = m^*$ when $a^j > 2q/3$.*

We define the symbols

$$\epsilon_j = \left\{ \begin{array}{ll} 0 & \text{when } a^j > Q \\ 1 & \text{when } a^j < Q \end{array} \right\} ;$$

and

$$\eta_j = \left\{ \begin{array}{ll} 0 & \text{when } a^j > 2q/3 \\ 1 & \text{when } a^j < 2q/3 \end{array} \right\} .$$

We can now combine the results of Theorems 3.3 and 4.7; (recalling the definition of $\chi_j$ given in theorem 2.1).

THEOREM 4.8. *If $Q > q > 2$ and $j \leq \mu$, then $M_j^* = m_j + 2\chi_j - 2\eta_j + 2\epsilon_j$ when $Q* > q$.*

**Proof.** We note that if $\epsilon_j = 0$ then $\eta_j = 0$. First assume that $j \neq \mu$.

**Case 1.** $\epsilon_j = 0$.

In this case $Q^* > q$ implies that $a^j > q$, hence

$$M^* = m^* + 2\chi_j = m^* + 2\chi_j - 2\eta_j + 2\epsilon_j .$$

**Case 2.** $\epsilon_j = 1$. In this case $a^j < Q^*$.

**Case 2a.** $\eta_j = 0$. Here $a^j > 2q/3$ and $M^* = m^* + 2 + 2\chi_j = m^* + 2\chi_j - 2\eta_j + 2\epsilon_j$.

**Case 2b.** $\eta_j = 1$. Here $a^j < 2q/3$ and $M^* = m^* + 2\chi_j = m^* + 2\chi_j - 2\eta_j + 2\epsilon_j$.

We note that $M_\mu^* = 2$ and $m_\mu^* = 0$. Also in this case

$$a^\mu + 1 > 2Q \geq 2q + 2$$

and we get $a^j > 2q$. Hence $\epsilon_j = 0$, $\eta_j = 0$. Furthermore

$$\{a^\mu/q\} = 1 - 1/q > 1/2.$$

Thus, $M_\mu^* = m_\mu^* + 2\chi_\mu - 2\eta_\mu + 2\epsilon_\mu$.

□

## 5. The formulas.

We are now in a position to derive the formulas relating $W(a, Q)$ and $W(a, Q^*)$ to $W(a, q)$. If $\nu$ is the order of $a$ modulo $Q^*$ then

$$W(a, Q^*) = 2 \sum_{j=1}^{\nu} M_j^* \tag{5.1}$$

Thus our first problem is to determine $\nu$. To this end we give

LEMMA 5.1. *If $Q^* \leq 3$ and $\mu$ is the least positive integer such that $a^\mu + 1 \equiv 0 \pmod{Q^*}$ then $\nu = 2\mu$.*

**Proof.** Certainly $2\mu \equiv 0 \pmod{\nu}$. If $\nu$ is odd then $\mu \equiv 0 \pmod{\nu}$. In this case $-1 \equiv (a^\mu)^{\nu/\mu} = a^\nu \equiv 1 \pmod{Q^*}$ and $Q^*$ divides 2 which contradicts that $Q^* \geq 3$. Thus, $\nu$ is even and $\kappa$ $(= \nu/2)$ divides $\mu$. Put $\lambda = \mu/\kappa$. Since

$$(a^\kappa - 1)(a^\kappa + 1) \equiv 0 \pmod{Q^*},$$

let $Q^* = Q_1 Q_2$ where $a^\kappa \equiv 1 \pmod{Q_1}$ and $a^\kappa \equiv -1 \pmod{Q_2}$. Hence, $a^{\kappa\lambda} \equiv 1 \pmod{Q_1}$ and $a^\mu \equiv 1 \pmod{Q_1}$ whence $Q_1$ is even. If $Q_1 = 1$ then $a^\kappa \equiv -1 \pmod{Q^*}$. By definition of $\mu$ we must have $\kappa \geq \mu$ but since $\mu \equiv 0 \pmod{\kappa}$ we get $\kappa = \mu$, and $\nu = 2\mu$.

If $Q_1 = 2$ and $Q_2$ is odd, then since $a^\kappa \equiv -1 \pmod 2$ we get that $a^\kappa \equiv -1 \pmod{Q^*}$; whence, $\nu = 2\mu$. Suppose $Q_1 = 2$ and $Q_2 = 2^{s-1}\, Q'$ with $s - 1 \geq 1$. If $Q^* = 2^s\, Q'$ does not divide $a^\kappa + 1$ then $2^{s-1}$ properly divides $a^\kappa + 1$ and $a^\kappa = -1 + 2^{s-1}\, t$ for odd $t$. Now, $-1 \equiv a^\mu = a^{\lambda\kappa} \equiv (-1)^{\lambda'} + 2^{s-1}\lambda t \pmod{2^s}$. If $\lambda$ is even then $2^s$ divides 2 which is impossible. If $\lambda$ is odd then $2^s$ divides $2^{s-1}\lambda t$ ; i.e. $\lambda t$ is even which is also impossible. Thus $\kappa = \mu$.

□

Note that we may also assume that if $Q^* = (a^\mu + 1)/q$, then $\mu$ is the least positive integer such that $a^\mu \equiv -1 \pmod{Q^*}$. For, if this is not the case, then suppose $\lambda$ is the least such integer. By Lemma 5.1 we have that $2\lambda$ divides $2\mu$ or $\lambda$ divides $\mu$. Since $a^\lambda \equiv -1 \pmod{Q^*}$ we get $q = q'\left(\dfrac{a^\mu + 1}{a^\lambda + 1}\right)$ for some integer $q'$. It follows that we can write $Q^* = (a^\lambda + 1)/q'$ for $q' < q$. Thus by replacing the value of $\mu$ by that of $\lambda$ and the value of $q$ by that of $q'$, we have the form of $Q^*$ which is desired.

In view of the above remarks we can now rewrite 5.1 as

$$W(a, Q^*) = \sum_{j=1}^{2\mu} M_j^* = 2\sum_{j=1}^{2\mu} M_j^* - 2 \tag{5.2}$$

(by 2.4). Now

$$W(a, q) = 2\sum_{i=1}^{\omega} \lfloor (M(s_i, q) + 1)/2 \rfloor.$$

Since $a^\mu \equiv -1 \pmod q$, there is a least positive $\lambda$ such that $a^\lambda \equiv -1 \pmod q$ and $\omega = 2\lambda$. Also $\mu \equiv 0 \pmod \lambda$, $\kappa = \mu/\lambda$ is odd and $\gamma^*_{\lambda - i} \equiv -a^{-(\lambda - i)} \equiv -a^{-\lambda} a^i \equiv a^i \equiv s_i \pmod q$.

Thus

$$\gamma^*_{\lambda-i} = s_i \quad \text{or} \quad \gamma^*_i = s_{\lambda-i}.$$

By (2.4) we have

$$\begin{aligned} W(a,q) &= 4\sum_{i=1}^{\lambda-1} \lfloor (M(s_i,q)+1)/2 \rfloor + 2 \\ &= 4\sum_{i=1}^{\lambda-1} \lfloor (M(\gamma^*_i,q)+1)/2 \rfloor + 2 \\ &= 2\sum_{i=1}^{\lambda-1} m^*_i + 2. \end{aligned}$$

Since $m^*_\lambda = 0$ we get

$$W(a,q) = 2\sum_{i=1}^{\lambda} m^*_i + 2. \tag{5.3}$$

By Theorem 4.8 and (5.2) we get

$$\begin{aligned} W(a,Q^*) &= \sum_{j=1}^{\mu}(m^*_j + 2\chi_j + 2\eta_j + 2\epsilon_j) - 2 \\ &= 2\sum_{j=1}^{\mu} m^*_j + 4\sum_{j=1}^{\mu} \chi_j - 4\sum_{j=1}^{\mu} \eta_j + 4\sum_{j=1}^{\mu} \epsilon_j - 2. \end{aligned} \tag{5.4}$$

We now need to evaluate each of these sums. We note that

$$\gamma^*_{(2t+1)\lambda+i} \equiv -a^t \equiv \gamma^*_{2\lambda-i} \pmod{q};$$

thus

$$\begin{aligned} \sum_{j=1}^{\mu} m^*_j &= \sum_{j=1}^{\lambda} m^*_j + \sum_{t=0}^{(\kappa-3)/2} \sum_{(2t+1)\lambda+1}^{(2t+3)\lambda} m^*_j \\ &= \sum_{j=1}^{\lambda} m^*_j + \left(\frac{\kappa-1}{2}\right)\sum_{j=1}^{2\lambda} m^*_{2\lambda-j} \qquad (\text{where } m^*_0 = 2) \\ &= \sum_{j=1}^{\lambda} m^*_j + \left(\frac{\kappa-1}{2}\right)\left(\sum_{j=1}^{2\lambda-1} m^*_j + 2\right). \end{aligned}$$

Since $\gamma^*_{2\lambda-i}\ \gamma^* \equiv 1 \pmod{q}$ we get,

$$m^*_{2\lambda-i} = m^*_i\ ;$$

whence,

$$\sum_{j=\lambda+1}^{2\lambda-1} m^*_j = \sum_{i=1}^{\lambda-1} m^*_{2\lambda-1} = \sum_{i=1}^{\lambda} m^*_{2\lambda-i} \qquad (\text{where } m^*_\lambda = 0)$$

It follows that

$$\sum_{j=1}^{\mu} m^*_j = \kappa - 1 + \kappa \sum_{j=1}^{\lambda} m^*_j.$$

Thus, by (5.3) we get

$$2 \sum_{j=1}^{\mu} m^*_j = \kappa W(a,q) - 2 \tag{5.5}$$

Recall that $\alpha$ is defined by $a^\alpha < q < a^{\alpha+1}$. Thus we find that

$$a^{\mu-\alpha-1} < a^{\mu-\alpha-1} + a^{-(\alpha+1)} < \frac{a^\mu + 1}{q} = Q^* < q^{\mu-\alpha} + a^{-\alpha}.$$

Thus

$$\sum_{i=1}^{\mu} \epsilon_i = \mu - \alpha - 1. \tag{5.6}$$

Also

$$a^{\alpha-1} < 2a^\alpha/3 < 2q/3 < 2a^{\alpha+1}/3 < a^{\alpha+1}.$$

Thus

$$\sum_{i=1}^{\mu} \eta_i = \alpha - 1 + \sigma,$$

where

$$\sigma = \left\{ \begin{matrix} 0 & \text{if} & a^\alpha > 2q/3 \\ 1 & \text{if} & a^\alpha < 2q/3 \end{matrix} \right\}.$$

Now $\sigma = 1 - \sigma^*$ where

$$\sigma^* = \left\{ \begin{matrix} 0 & \text{if} & a^\alpha > 2q/3 \\ 1 & \text{if} & a^\alpha < 2q/3 \end{matrix} \right\}.$$

However, since $3a^\alpha/4 < a^\alpha < q$ we have $\sigma^* = \lfloor 3a^\alpha/(2q) \rfloor$ and

$$\sum_{i=1}^{\mu} \eta_i = \alpha - \lfloor 3a^\alpha/(2q) \rfloor. \tag{5.7}$$

It remains to evaluate $\sum_{i=1}^{\mu} \chi_i$. We first prove

LEMMA 5.2. *If $j \geq \lambda + 2$ then $\chi_{\lambda+j} + \chi_j = 1$.*

**Proof.** We first note that since $j \geq \lambda + 2$ we have

$$a^{\lambda+j} > a^j \geq a^{\lambda+2} \geq a^2(q-1) \geq 4(q-1) > 2q;$$

Thus

$$\chi_{\rho+j} = \left\{ \begin{matrix} 0 \text{ if } \{a^{\rho+j}/q\} < 1/2 \\ 1 \text{ if } \{a^{\rho+j}/q\} > 1/2 \end{matrix} \right\}$$

and

$$\chi_j = \left\{ \begin{matrix} 0 \text{ if } \{a^j/q\} < 1/2 \\ 1 \text{ if } \{a^j/q\} > 1/2 \end{matrix} \right\}.$$

Now

$$a^{\lambda+j} \equiv -a^j \pmod{q}.$$

Thus, if $a^{\lambda+j} = q\lfloor a^{\lambda+j}/q \rfloor + r$ for $0 < r_1 < q$ and $a^j = q\lfloor a^j/q \rfloor + r_2$ for $0 < r_2 < q$, then $r_1 = q - r_2$. Since $\{a^{\lambda+j}/q\} = r_1/q = 1 - r_2/q$ and $\{a^j/q\} = r_2/q$, the result follows.

□

Since

$$\sum_{a^i>2q}^{\mu} \chi_i = \sum_{a^i>2q}^{\lambda} \chi_i + \sum_{i=\lambda+1}^{2\lambda} \chi_i + \cdots + \sum_{i=(\kappa-1)\lambda+1}^{\kappa\lambda} \chi_i$$

and $\kappa$ is odd we get

$$\sum_{a^i>2q}^{\mu} = \left(\frac{\kappa-1}{2}\right)\lambda + (\chi_{\lambda+1} + \chi_{2\lambda+1}) - 1 + \sum_{a^i>2q}^{\lambda} \chi_i$$

by lemma 5.6. If $a^{\lambda+1} > 2q$, then $\chi_{\lambda+2} + \chi_{2\lambda+1} = 1$ ; if $a^{\lambda+1} < 2q$ then $q = 2^\lambda + 1$ (here $a = 2$). In this case $\chi_{\lambda+1} = 0$ and since $2^\lambda \equiv -1 \pmod{q}$ we

get $2^{2\lambda+1} \equiv 2 \pmod{q}$; thus $\{a^{2\lambda+1}/q\} < 1/2$ when $\lambda > 1$ and $\chi_{2\rho+1} = 0$. Thus, if $q \neq 3$ and $a \neq 2$ then when $a^{\lambda+1} < 2q$ we get $\chi_{\rho+1} + \chi_{2\rho+1} = 0$. Since $0 < \dfrac{2q}{a^{\lambda+1}} < 2$ we get

$\chi_{\rho+1} + \chi_{2\rho+1} = 1 - \lfloor 2q/a^{\lambda+1} \rfloor$ unless $q = 3$and $a = 2$ in which case

$\chi_{\rho+1} + \chi_{2\rho+1} = 1$. With the exception of this case we get

$$\sum_{i=\lambda+1}^{\mu} \chi_i = \left(\frac{\kappa - 1}{2}\right) \lambda - \lfloor 2q/a^{\lambda+1} \rfloor.$$

Given the definition of $S(a,q)$ in Theorem 2.1 we see that it depends for its value only on the values of $a$ and $q$. Now $\{r/s\} \geq 1/2$ implies that $\lfloor 2r/s \rfloor - 2\lfloor r/s \rfloor = 1$, and $\{r/s\} < 1/2$ implies $\lfloor 2r/s \rfloor - 2\lfloor r/s \rfloor = 0$ ; thus, we can write

$$\begin{aligned} S(a,q) = \lfloor 2/a \rfloor &+ \sum_{a^i < q/2} (2\lfloor q/a^i \rfloor - \lfloor 2q/a^i \rfloor) \\ &+ \sum_{a^i > 2q}^{\lambda} (\lfloor 2a^i/q \rfloor - 2\lfloor a^i/q \rfloor). \end{aligned} \tag{5.8}$$

The $\lfloor 2/a \rfloor$ term here occurs because $\{q/a^i\} = 1/2$ when $a^i = 2$.

Also

$$\sum_{i=1}^{\mu} \chi_i = \left(\frac{\kappa - 1}{2}\right) \lambda - \lfloor 2q/a^{\lambda+1} \rfloor + S(a,q) \tag{5.9}$$

If we put together the formulas (5.3)-(5.7) and (5.9) we get

$$\begin{aligned} W(a,Q^*) = \kappa W(a,q) + 6\mu - 2\lambda - 8\alpha - 4\lfloor 2q/a^{\lambda+1} \rfloor \\ + 4\lfloor 3a^\alpha/2q \rfloor + 4S(a,q) - 8 \end{aligned} \tag{5.10}$$

(here $a \neq 2$, $q \neq 3$ and $Q^* > q$). This is Theorem 2.1.

By using the results of section 3 we can also derive by much simpler methods that

$$W(a,q) = (\mu/\omega)\, W(a,q) + 2\mu - 4\alpha - 2 \tag{5.11}$$

under the assumption that $\mu$ is the order of $a$ modulo $Q$, (an assumption which can be made without loss of generality), and the assumption that $q < Q$. This is Theorem 2.2.

## 6. Special Cases.

In this section we will develop formulas for $W(a,q)$ for certain special values of $q$. We first note that when $q = a^\lambda + 1$, then we can easily evaluate $S(a,q)$. We have that $a^j < q/2$ for $j = 1, 2 \cdots, \lambda - 1$. For such values of $j$ we get

$$\lfloor q/a^j \rfloor = \lfloor a^{\lambda - j} + 1/a^j \rfloor = a^{\lambda - j}$$

and

$$\lfloor 2q/a^j \rfloor = \lfloor 2a^{\lambda - j} + 2/a^j \rfloor - 2a^{\lambda - j}$$

unless $a^j = 2$.

Since $q/2 < a^\lambda < 2q$, we get

$$S(a,q) = 2a^{\lambda-1} - \lfloor 2a^{\lambda-1} + 2/a \rfloor = \left\{ \begin{array}{ll} 0 & \text{if } a \neq 2 \\ -1 & \text{if } a = 2 \end{array} \right\}.$$

Now, when $q = a^\lambda + 1$ and $Q^* = (a^\mu + 1)/(a^\lambda + 1)$ is an integer larger than 2, then $\mu \equiv 0 \pmod{\lambda}$ and we have

LEMMA 6.1. *If $Q^*$ is as given above, $\lambda \neq 1$, and $a \neq 2$, then the least value $\nu$ such that $a^\nu \equiv -1 \pmod{Q^*}$ is $\mu$.*

**Proof.** Let $\kappa = \mu/\lambda$. Since $2\nu$ is the order of $a$ modulo $Q^*$ and $a^{2\lambda\kappa} \equiv 1 \pmod{Q^*}$ we have $2\nu$ dividing $2\lambda\kappa$ or $\lambda\kappa \equiv 0 \pmod{\nu}$. Put $\nu = \lambda\kappa/t$ for $t \geq 1$. Since $a^\nu \equiv -1 \pmod{\dfrac{a^{\lambda\kappa}+1}{a^\lambda+1}}$ we get that $a^{\lambda\kappa} + 1 \leq (a^\nu + 1)(a^\lambda + 1)$

$$a^{\lambda\kappa} \leq a^{\nu+\lambda} + a^\nu + a^\lambda. \tag{6.1}$$

Since $Q^* > 1$ we must have $\kappa > 1$ and since $\kappa$ is odd we must have $\kappa \geq 3$. Also, $\nu \geq 1$, and $\lambda \geq 1$. If $\lambda\kappa > \mu + \lambda + 1$ then $\lambda\kappa - \nu - \lambda > 1$ and

$$a^2 \leq a^{\lambda\kappa - \nu - \lambda} \leq 1 + a^{-\lambda} + a^{-\nu} \leq 1 + 2/a, \quad \text{by (6.1).}$$

Since $a \geq 2$, this is impossible.

Hence,

$$\lambda\kappa \leq \nu + \lambda + 1$$

or

$$\lambda\kappa \leq \lambda\kappa/t + \lambda + 1.$$

It follows that $(t-1)(\kappa-1) \leq 1+t/\lambda$. Since $\kappa \geq 3$, we have that $2(t-1) \leq 1 + t/\lambda$ or $2t - t/\lambda \leq 3$. If $t = 3$, this can only occur for $\lambda = 1$. But from (6.1) we get

$$a^{\kappa} \leq a^{\kappa/3} + a^{\kappa/3+1} + a,$$

whence

$$a \leq a^{2\kappa/3-1} \leq 1 + a^{-\kappa/3} + a^{-1} \leq 1 + 2/a$$

which means that $a = 2$ ; this value is excluded by hypothesis. If $t = 2$ then $\lambda$ is even and $\lambda \geq 2$. If $\lambda > 2$, then $2t - t/\lambda > 2t - t/2 > 3t/2 > 3$, which is impossible. If $t = 2$ and $\lambda = 2$, then by (6.1)

$$a^{2\kappa} \leq a^{\kappa+2} + a^{\kappa} + a^2$$

and we get

$$2 \leq a \leq a^{\kappa-2} \leq 1 + a^{-2} + a^{-\kappa} < 1 + 2/a^2 < 3/2$$

a contradiction. Hence we must have $t = 1$ and $\nu = \lambda\kappa = \mu$.

□

By using similar techniques it is easy to prove

LEMMA 6.2. *If $q = a^{\omega} - 1$ and $Q = (a^{\mu} - 1)/(a^{\omega} - 1)$ is an integer greater than 1 then the order of $a$ modulo $Q$ is $\mu$.*

From Lemma 6.2 and (5.11) with $q = a^{\omega} - 1$ we get $\alpha = \omega - 1$ and

$$W\left[a, \frac{a^{\mu}-1}{a^{\omega}-1}\right] = \frac{\mu}{\omega} W(a, a^{\omega} - 1) + 2\mu - 4\omega + 2.$$

By (2.5) this becomes

$$W\left[a, \frac{a^{\mu}-1}{a^{\omega}-1}\right] = 4\mu - 4\omega + 2 - 2\mu/\omega, \tag{6.2}$$

which is Theorem 2.3.

When $q = a^\lambda + 1$ we get $2q > a^i$ for $1 \leq i \leq \lambda$ and $S(a,q) = 0$.

Furthermore, $\alpha = \lambda$,

$$\lfloor 2q/a^{\lambda+1} \rfloor = \left\{ \begin{matrix} 1 & \text{if} & a = 2 \\ 0 & \text{if} & a > 2 \end{matrix} \right\},$$

$\lfloor 3a^\alpha/q \rfloor = 1$ and $W(a,q) = 4\lambda - 2$ by (2.6). Hence by Lemma 6.1 and (5.10) we get

$$W\left[a, \frac{a^\mu + 1}{a^\lambda + 1}\right] = 10\mu - 10\lambda - 2\mu/\lambda - e \tag{6.3}$$

where $e$ is as in Theorem 2.4 which is now proved.

It should be noted that we have only proved (6.3) when $a^\lambda + 1 \neq 3$. However, it can be easily shown that in this case

$$W(2,\ (2^\mu + 1)/3) = 8\mu - 18 \quad \text{for} \quad \mu > 3$$

This holds because $M^*(2^k, (2^\mu + 1)/3) = 4$ for $3 \leq k \leq \mu - 2$ and $M^*(2, (2^\mu+1)/3) = M^*(4, (2^\mu+1)/3) = M^*(2^{\mu-1}, (2^\mu+1)/3) = M^*(2^\mu, (2^\mu+1)/3) = 2$. Thus (6.3) holds for $a^\lambda - 1 = 3$.

We have also excluded the case where $q = 2$, but it is also easy to show that

$$M^*(a^i, (a^\mu + 1)/2) = 4 \quad \text{for} \quad 2 \leq i \leq \mu - 1,\ M^*(a^\mu, (a^\mu + 1)/2) = 2 \quad \text{and}$$

$$M^*(a, (a^\mu + 1)/2) = \left\{ \begin{matrix} 2 & \text{if} & a = 3 \\ 4 & \text{if} & a > 3 \end{matrix} \right\}.$$

Thus by (2.4) we get

$$W\left(a, \frac{a^\mu + 1}{2}\right) = \left\{ \begin{matrix} 8\mu - 10 & \text{when} & a = 3 \\ 8\mu - 6 & \text{when} & a > 3 \end{matrix} \right\}, \tag{6.4}$$

which is Theorem 2.5.

Undoubtedly many more results concerning this remarkable function $W(a,q)$ remain to be discovered. We conclude this paper with a short table of values $W(a,q)$.

## Table of Values for $W(a,q)$

Parameters : $2 \leq a \leq 10$

$2 < q \leq 50$

| $q/a$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 2 | - | 0 | 2 | - | 0 | 2 | - | 0 |
| 4 | - | 2 | - | 0 | - | 2 | - | 0 | - |
| 5 | 6 | 6 | 2 | - | 0 | 6 | 6 | 2 | - |
| 6 | - | - | - | 2 | - | 0 | - | - | - |
| 7 | 4 | 10 | 4 | 10 | 2 | - | 0 | 4 | 10 |
| 8 | - | 2 | - | 4 | - | 2 | - | 0 | - |
| 9 | 10 | - | 4 | 10 | - | 4 | 2 | - | 0 |
| 10 | - | 6 | - | - | - | 6 | - | 2 | - |
| 11 | 22 | 8 | 8 | 8 | 22 | 22 | 22 | 8 | 2 |
| 12 | - | - | - | 2 | - | 4 | - | - | - |
| 13 | 26 | 4 | 10 | 10 | 26 | 26 | 10 | 4 | 10 |
| 14 | - | 14 | - | 14 | - | - | - | 8 | - |
| 15 | 6 | - | 2 | - | - | 6 | 6 | - | - |
| 16 | - | 8 | - | 8 | - | 2 | - | 4 | - |
| 17 | 14 | 38 | 6 | 38 | 38 | 38 | 14 | 14 | 38 |
| 18 | - | - | - | 18 | - | 8 | - | - | - |
| 19 | 46 | 46 | 20 | 20 | 20 | 8 | 18 | 20 | 46 |
| 20 | - | 6 | - | - | - | 6 | - | 2 | - |
| 21 | 12 | - | 4 | 10 | - | - | 4 | - | 14 |
| 22 | - | 8 | - | 8 | - | 22 | - | 8 | - |
| 23 | 28 | 28 | 28 | 62 | 28 | 62 | 28 | 28 | 62 |
| 24 | - | - | - | 2 | - | 2 | - | - | - |
| 25 | 50 | 50 | 26 | - | 12 | 10 | 50 | 26 | - |
| 26 | - | 4 | - | 6 | - | 34 | - | 4 | - |
| 27 | 50 | - | 24 | 50 | - | 24 | 18 | - | 8 |
| 28 | - | 10 | - | 14 | - | - | - | 4 | - |
| 29 | 82 | 82 | 34 | 34 | 34 | 20 | 82 | 34 | 82 |
| 30 | - | - | - | - | - | 10 | - | - | - |
| 31 | 8 | 86 | 8 | 4 | 10 | 40 | 8 | 40 | 40 |
| 32 | - | 24 | - | 24 | - | 12 | - | 12 | - |
| 33 | 18 | - | 8 | 28 | - | 26 | 18 | - | 2 |
| 34 | - | 50 | - | 50 | - | 50 | - | 30 | - |
| 35 | 32 | 28 | 12 | - | 2 | - | 12 | 12 | - |
| 36 | - | - | - | 14 | - | 16 | - | - | - |

Table of values for $W(a,q)$ (continued)

| $q/a$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 37 | 106 | 46 | 46 | 106 | 6 | 20 | 42 | 20 | 8 |
| 38 | - | 54 | - | 24 | - | 4 | - | 24 | - |
| 39 | 34 | - | 18 | 10 | - | 38 | 10 | - | 18 |
| 40 | - | 6 | - | - | - | 10 | - | 2 | - |
| 41 | 54 | 22 | 30 | 54 | 126 | 126 | 54 | 10 | 12 |
| 42 | - | - | - | 14 | - | - | - | - | - |
| 43 | 38 | 134 | 16 | 134 | 4 | 10 | 38 | 64 | 64 |
| 44 | - | 32 | - | 12 | - | 26 | - | 12 | - |
| 45 | 36 | - | 16 | - | - | 36 | 12 | - | - |
| 46 | - | 36 | - | 66 | - | 66 | - | 36 | - |
| 47 | 72 | 72 | 72 | 154 | 72 | 72 | 72 | 72 | 154 |
| 48 | - | - | - | 12 | - | 2 | - | - | - |
| 49 | 64 | 130 | 64 | 130 | 42 | - | 20 | 64 | 130 |
| 50 | - | 74 | - | - | - | 6 | - | 42 | - |

*Acknowledgements* : The author's research is supported by NSERC Canada grants No. A8484 and No. A7649 respectively.

## REFERENCES

[1] L. BERNSTEIN, *Fundamental units and cycles*, J. Number Theory **8** (1976), 446-491.

[2] D.E. KNUTH, The Art of Computer Programing II : Seminumerical Algorithms, Addison-Wesley, 1981.

[3] R.A. MOLLIN and H.C. WILLIAMS, *Consecutive powers in continued fractions*, (to appear : Acta Arithmetica).

[4] O. PERRON, *Die Lehre von den Kettenbrüchen*, Chelsea, New-York (undated).

[5] J.W. PORTER, *On a theorem of Heilbronn*, Mathematika **22** (1975), 20-28.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta T2N 1N4
Canada
e-mail: ramollin@acs-ucalgary.ca.

Computer Science Department
University of Manitoba
Winnipeg, Manitoba R3T 2N2
Canada
e-mail: Hugh_Williams@CSMail.CS.UMANITOBA.CA