ACTA ARITHMETICA
LXI.2 (1992)

Determination of $\sum_{k=1}^{p-1} g^{ak^2}$ modulo p

by

KENNETH S. WILLIAMS* and KENNETH HARDY** (Ottawa, Ont.)

1. Introduction. At the Second Canadian Number Theory Association Conference held at the University of British Columbia in August 1989, Michael Robinson of the Supercomputing Research Center in Bowie, Maryland asked the first author for the value modulo p of the sum $\sum_{k=1}^{p-1} g^{k^2}$ where p is an odd prime and g is a primitive root $(\mathrm{mod}\, p)$. In this paper we determine the value modulo p of the more general sum

$$G(p,a,g) = \sum_{k=1}^{p-1} g^{ak^2},$$

where a is an arbitrary integer. The sum $G(p,a,g)$ has the following two basic properties:

(i) if $a' \equiv a \pmod{p-1}$ then (as $g^{p-1} \equiv 1 \pmod{p}$)

$$G(p,a',g) \equiv G(p,a,g) \pmod{p};$$

(ii) if g' is another primitive root $(\mathrm{mod}\, p)$ then

$$G(p,a,g') \equiv G(p,am,g) \pmod{p},$$

where $g' \equiv g^m \pmod{p}$, $1 \le m \le p-2$, $\mathrm{GCD}(m, p-1) = 1$.

If $a \equiv 0 \pmod{p-1}$ we have $g^{ak^2} \equiv 1 \pmod{p}$ for $k = 1, 2, \ldots, p-1$ so that $G(p,a,g) \equiv p-1 \equiv -1 \pmod{p}$. Thus, from now on, we suppose that p is an odd prime, g is a primitive root $(\mathrm{mod}\, p)$, and a is an integer with $a \not\equiv 0 \pmod{p-1}$.

1991 *Mathematics Subject Classification*: 11A07, 11A15, 11L05, 11L10.

* Research supported by Natural Sciences and Engineering Research Council of Canada, Grant A-7233.

** Research supported by Natural Sciences and Engineering Research Council of Canada, Grant A-8049.

We begin by defining integers d, b, q, α and r, which depend on a and p but not on g, which will be used throughout the paper. We set

$$d = \mathrm{GCD}(a, p-1)\,, \tag{1.1}$$

$$b = a/d\,, \quad q = (p-1)/d\,, \tag{1.2}$$

so that b and q are coprime integers with $1 < q \le p-1$. We also let 2^α denote the largest power of 2 dividing q and set

$$r = q/2^\alpha\,, \tag{1.3}$$

so that r is a positive odd integer. We note that $(p-1)/r$ is a positive even integer and that if $\alpha \ge 1$, b is odd. We remark that if a is changed to $a' = a + (p-1)w$, then d, q, α and r remain unchanged but b is changed to $b + qw$.

An important function in our determination of the sum $G(p,a,g)$ modulo p is the function $F(p,a,g)$ defined by

$$F(p,a,g) = \prod_{1\le t<u\le r-1} (g^{(p-1)t/r} - g^{(p-1)u/r})\,, \tag{1.4}$$

where the right hand side of (1.4) is understood to be 1 if $r = 1$. The basic properties of $F(p,a,g)$ are given in Lemma 1 below, which will be proved in Section 2. If n is a positive integer we write ζ_n for the primitive nth root of unity $e^{2\pi i/n}$. We recall that

$$\sqrt{r} \in Q(\zeta_r) \qquad \text{if } r \equiv 1 \pmod 4\,,$$
$$\sqrt{-r} \in Q(\zeta_r) \qquad \text{if } r \equiv 3 \pmod 4\,.$$

As r divides $p-1$ we have $Q(\zeta_r) \subset Q(\zeta_{p-1})$. Clearly $Q(\zeta_{p-1}) \subset Q(\zeta_{p(p-1)})$ so that

$$\sqrt{(-1)^{(r-1)/2}r} \in Q(\zeta_{p(p-1)})\,.$$

Lemma 1. (i) *If* $a' \equiv a \pmod{p-1}$ *then*

$$F(p,a',g) = F(p,a,g)\,.$$

(ii) *If* g' *is another primitive root* $(\mathrm{mod}\, p)$, *say* $g' \equiv g^m \pmod p$, $1 \le m \le p-2$, $\mathrm{GCD}(m, p-1) = 1$, *then*

$$F(p,a,g') \equiv \left(\frac{m}{r}\right) F(p,a,g) \pmod p\,,$$

where $(\frac{m}{r})$ *is the Jacobi symbol.*

(iii) $F(p,a,g)^2 \equiv (-1)^{(r-1)/2} r^{r-2} \pmod p$.

(iv) *If* $\mathfrak{P}$ *is a prime ideal of* $Q(\zeta_{p(p-1)})$ *lying above the prime ideal* $(1-\zeta_p)$ *of* $Q(\zeta_p)$ *and* g *is a primitive root* $(\mathrm{mod}\, p)$ *with* $g \equiv \zeta_{p-1} \pmod{\mathfrak{P}}$ *then*

$$F(p,a,g) \equiv \left(\frac{-2}{r}\right) r^{(r-3)/2} \sqrt{(-1)^{(r-1)/2} r} \pmod{\mathfrak{P}}\,.$$

It is also convenient to set

$$E(p,a,g)=\begin{cases}1 & \text{if } \alpha=0\,,\\ 0 & \text{if } \alpha=1\,,\\ 2^{\alpha(r-2)/2}(1+g^{(p-1)br/4}) & \text{if } \alpha\,(\text{even})\ge 2\,,\\ 2^{(\alpha(r-2)+1)/2}g^{(p-1)br/8} & \text{if } \alpha\,(\text{odd})\ge 3\,.\end{cases} \tag{1.5}$$

We note that $\alpha(r-2)/2$ is an integer for α even and that $(\alpha(r-2)+1)/2$ is an integer for α odd. If $\alpha\ge 2$ we have $p\equiv 1 \pmod 4$ so that $(p-1)br/4$ is an integer. If $\alpha\ge 3$ we have $p\equiv 1 \pmod 8$, so that $(p-1)br/8$ is an integer. The basic properties of $E(p,a,g)$ are given in Lemma 2 below, which will be proved in Section 2.

LEMMA 2. (i) *If* $a'\equiv a \pmod{p-1}$ *then*

$$E(p,a',g)\equiv E(p,a,g) \pmod p\,.$$

(ii) *If* g' *is another primitive root* $(\bmod p)$, *say* $g'\equiv g^m \pmod p$, $1\le m\le p-2$, $\mathrm{GCD}(m,p-1)=1$, *then*

$$E(p,a,g')\equiv E(p,am,g) \pmod p\,.$$

The following determination of $G(p,a,g)$ modulo p is proved in Section 3.

THEOREM.

$$G(p,a,g)\equiv -\left(\frac{b}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-1)/2}E(p,a,g)F(p,a,g) \pmod p\,.$$

In Section 4 we examine some special cases of this theorem.

2. Properties of $E(p,a,g)$ and $F(p,a,g)$. We recall that for any positive integer n, ζ_n denotes the primitive nth root of unity $e^{2\pi i/n}$. We will need the following result: if n is a positive odd integer and k is an integer with $\mathrm{GCD}(k,n)=1$ then

$$\begin{aligned}\prod_{1\le t<u\le n-1}(\zeta_n^{kt}-\zeta_n^{ku}) &= \left(\frac{k}{n}\right) i^{(n-1)/2} n^{(n-3)/2}\sqrt{n}\\ &= \left(\frac{-2k}{n}\right) n^{(n-3)/2}\sqrt{(-1)^{(n-1)/2}n}\,,\end{aligned} \tag{2.1}$$

where $(\frac{-}{n})$ is the Jacobi symbol. The result (2.1) can be proved as in [3, pp. 462–465] making use of the following result (see for example [2, p. 186]):

$$\prod_{t=1}^{(n-1)/2} 2\sin\frac{2\pi kt}{n}=\left(\frac{k}{n}\right)\sqrt{n}\,. \tag{2.2}$$

Proof of Lemma 1. (i) This follows immediately from the remark following (1.3) and the definition (1.4).

(ii) The result is clearly true for $r = 1$ as in this case $F(p,a,g) = F(p,a,g') = 1$ and $(\frac{m}{r}) = 1$. Hence we may suppose that $r \geq 3$ so that $\zeta_r \neq \pm 1$.

Let P be a prime ideal of $Q(\zeta_r)$ lying above p. Then we have

$$\prod_{s=0}^{r-1}(g^{(p-1)/r} - \zeta_r^s) = g^{p-1} - 1 \equiv 0 \pmod{P}$$

so that

$$g^{(p-1)/r} \equiv \zeta_r^s \pmod{P}$$

for some integer s with $0 \leq s \leq r-1$. Clearly we have $\mathrm{GCD}(s,r) = 1$ as g is a primitive root $(\mathrm{mod}\, p)$. Let g' be another primitive root $(\mathrm{mod}\, p)$, say $g' \equiv g^m \pmod{p}$, $1 \leq m \leq p-2$, $\mathrm{GCD}(m, p-1) = 1$. Then we have

$$\begin{aligned}
&\prod_{1\leq t<u\leq r-1}(g'^{(p-1)t/r} - g'^{(p-1)u/r}) \\
&\quad\equiv \prod_{1\leq t<u\leq r-1}(g^{(p-1)mt/r} - g^{(p-1)mu/r}) \pmod{P} \\
&\quad\equiv \prod_{1\leq t<u\leq r-1}(\zeta_r^{smt} - \zeta_r^{smu}) \pmod{P} \\
&\quad\equiv \left(\frac{m}{r}\right)\prod_{1\leq t<u\leq r-1}(\zeta_r^{st} - \zeta_r^{su}) \pmod{P} \quad \text{(by (2.1))} \\
&\quad\equiv \left(\frac{m}{r}\right)\prod_{1\leq t<u\leq r-1}(g^{(p-1)t/r} - g^{(p-1)u/r}) \pmod{P},
\end{aligned}$$

so that

$$F(p,a,g') \equiv \left(\frac{m}{r}\right)F(p,a,g) \pmod{P}.$$

As $P \mid p$ and both sides of this congruence are integers, the congruence holds $(\mathrm{mod}\, p)$, proving (ii).

(iii) Let $\mathfrak{P}$ be a prime ideal of $Q(\zeta_{p(p-1)})$ lying above the prime ideal $(1-\zeta_p)$ of $Q(\zeta_p)$. Let g be a primitive root $(\mathrm{mod}\, p)$. Then we have

$$\prod_{s=0}^{p-2}(g - \zeta_{p-1}^s) = g^{p-1} - 1 \equiv 0 \pmod{\mathfrak{P}},$$

so that $g \equiv \zeta_{p-1}^s \pmod{\mathfrak{P}}$ for some integer s with $0 \leq s \leq p-2$. As g is a primitive root $(\mathrm{mod}\, p)$ we must have $\mathrm{GCD}(s, p-1) = 1$. Let s' be an integer such that $ss' \equiv 1 \pmod{p-1}$, and let g' denote the primitive root $g^{s'} \pmod{p}$. Then, as

$$g' \equiv g^{s'} \equiv \zeta_{p-1}^{ss'} \equiv \zeta_{p-1} \pmod{\mathfrak{P}},$$

by (iv) (to be proved next), we have

$$F(p,a,g') \equiv \left(\frac{-2}{r}\right) r^{(r-3)/2}\sqrt{(-1)^{(r-1)/2}r} \pmod{\mathfrak{P}},$$

so that

$$F(p,a,g')^2 \equiv (-1)^{(r-1)/2} r^{r-2} \pmod{\mathfrak{P}}.$$

As both sides of this congruence are integers, we must have

$$F(p,a,g')^2 \equiv (-1)^{(r-1)/2} r^{r-2} \pmod{p}.$$

Finally, as $F(p,a,g') \equiv \pm F(p,a,g) \pmod{p}$, by (ii), we deduce that

$$F(p,a,g)^2 \equiv (-1)^{(r-1)/2} r^{r-2} \pmod{p},$$

which is (iii).

(iv) Let $\mathfrak{P}$ be a prime ideal of $Q(\zeta_{p(p-1)})$ lying above the prime ideal $(1-\zeta_p)$ of $Q(\zeta_p)$, and let g be a primitive root satisfying $g \equiv \zeta_{p-1} \pmod{\mathfrak{P}}$. Then we have

$$g^{(p-1)/r} \equiv \zeta_{p-1}^{(p-1)/r} \equiv \zeta_r \pmod{\mathfrak{P}}$$

so that

$$\begin{aligned} F(p,a,g) &= \prod_{1\le t<u\le r-1} (g^{(p-1)t/r} - g^{(p-1)u/r}) \\ &\equiv \prod_{1\le t<u\le r-1} (\zeta_r^t - \zeta_r^u) \pmod{\mathfrak{P}} \\ &\equiv \left(\frac{-2}{r}\right) r^{(r-3)/2}\sqrt{(-1)^{(r-1)/2}r} \pmod{\mathfrak{P}}, \end{aligned}$$

by (2.1), as asserted. ∎

Proof of Lemma 2. (i) If a is changed to $a' = a + w(p-1)$, the integers d, q, α and r remain unchanged while b becomes $b' = b + wq$, so that $E(p,a,g) = E(p,a',g)$ if $\alpha = 0$ or 1. If $\alpha \ge 2$ then $q \equiv 0 \pmod 4$ so

$$\begin{aligned} g^{(p-1)b'r/4} &\equiv g^{(p-1)(b+wq)r/4} \equiv g^{(p-1)br/4}(g^{p-1})^{w(q/4)r} \\ &\equiv g^{(p-1)br/4} \pmod{p}, \end{aligned}$$

showing that $E(p,a',g) \equiv E(p,a,g) \pmod{p}$ if α (even) ≥ 2. If α (odd) ≥ 3, then $q \equiv 0 \pmod 8$, and thus

$$\begin{aligned} g^{(p-1)b'r/8} &\equiv g^{(p-1)(b+wq)r/8} \equiv g^{(p-1)br/8}(g^{p-1})^{w(q/8)r} \\ &\equiv g^{(p-1)br/8} \pmod{p}, \end{aligned}$$

proving $E(p,a',g) \equiv E(p,a,g) \pmod{p}$ in this case.

(ii) If a is replaced by am, where $\mathrm{GCD}(m, p-1) = 1$, then d, q, α and r remain unchanged while b becomes bm. Hence we have $E(p,am,g) \equiv E(p,a,g^m) \pmod{p}$. ∎

3. Proof of the Theorem. Let $\mathfrak{P}$ be a prime ideal of $Q(\zeta_{p(p-1)})$ lying above the prime ideal $(1-\zeta_p)$ of $Q(\zeta_p)$. As in the proof of Lemma 1(iii), we may choose g to be a primitive root $(\mathrm{mod}\, p)$ satisfying

$$g \equiv \zeta_{p-1} \pmod{\mathfrak{P}}. \tag{3.1}$$

If $\alpha \geq 2$, so that $p \equiv 1 \pmod 4$, we have

$$g^{(p-1)/4} \equiv \zeta_4 \pmod{\mathfrak{P}}, \tag{3.2}$$

and if $\alpha \geq 3$, so that $p \equiv 1 \pmod 8$,

$$g^{(p-1)/8} \equiv \zeta_8 \pmod{\mathfrak{P}}. \tag{3.3}$$

Hence we have

$$\begin{aligned} G(p,a,g) &\equiv \sum_{k=1}^{p-1} \zeta_{p-1}^{ak^2} \pmod{\mathfrak{P}} \quad \text{(by (3.1))} \\ &\equiv \sum_{k=1}^{dq} \zeta_q^{bk^2} \pmod{\mathfrak{P}} \quad \text{(by (1.2))} \\ &\equiv d\sum_{k=1}^{q} \zeta_q^{bk^2} \pmod{\mathfrak{P}}. \end{aligned}$$

Appealing to the multiplicative property of Gauss sums (see for example [1, p. 163]), we have as $q = 2^\alpha r$

$$G(p,a,g) \equiv d\Big(\sum_{k=1}^{2^\alpha} \zeta_{2^\alpha}^{rbk^2}\Big)\Big(\sum_{k=1}^{r} \zeta_r^{2^\alpha bk^2}\Big) \pmod{\mathfrak{P}}. \tag{3.4}$$

Next, appealing to the well-known evaluation of the Gauss sum (see for example [1, pp. 166–167]), we have

$$\sum_{k=1}^{2^\alpha} \zeta_{2^\alpha}^{rbk^2} = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{if } \alpha = 1, \\ 2^{\alpha/2}(1+\zeta_4^{rb}) & \text{if } \alpha\,(\text{even}) \geq 2, \\ 2^{(\alpha+1)/2}\zeta_8^{rb} & \text{if } \alpha\,(\text{odd}) \geq 3, \end{cases} \tag{3.5}$$

and

$$\sum_{k=1}^{r} \zeta_r^{2^\alpha bk^2} = \left(\frac{2^\alpha b}{r}\right)\sqrt{(-1)^{(r-1)/2}r}. \tag{3.6}$$

From (3.2), (3.3) and (3.5) we obtain

$$\sum_{k=1}^{2^\alpha} \zeta_{2^\alpha}^{rbk^2} \equiv \begin{cases} 1 \pmod{\mathfrak{P}} & \text{if } \alpha = 0, \\ 0 \pmod{\mathfrak{P}} & \text{if } \alpha = 1, \\ 2^{\alpha/2}(1+g^{(p-1)rb/4}) \pmod{\mathfrak{P}} & \text{if } \alpha\,(\text{even}) \geq 2, \\ 2^{(\alpha+1)/2}g^{(p-1)rb/8} \pmod{\mathfrak{P}} & \text{if } \alpha\,(\text{odd}) \geq 3, \end{cases}$$

that is, appealing to (1.5),

$$\sum_{k=1}^{2^\alpha} \zeta_{2^\alpha}^{rbk^2} \equiv 2^{\alpha(3-r)/2} E(p,a,g) \pmod{\mathfrak{P}}. \tag{3.7}$$

Next from (3.6) and Lemma 1(iv) we obtain

$$\sum_{k=1}^{r} \zeta_r^{2^\alpha bk^2} \equiv \left(\frac{2^\alpha b}{r}\right)\left(\frac{-2}{r}\right) r^{-(r-3)/2} F(p,a,g) \pmod{\mathfrak{P}}.$$

As $d2^\alpha r \equiv -1 \pmod{p}$ we have

$$r^{-(r-3)/2} \equiv (-1)^{(r-3)/2} d^{(r-3)/2} 2^{\alpha(r-3)/2} \pmod{\mathfrak{P}},$$

so that

$$\sum_{k=1}^{r} \zeta_r^{2^\alpha bk^2} \equiv (-1)\left(\frac{b}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-3)/2} 2^{\alpha(r-3)/2} F(p,a,g) \pmod{\mathfrak{P}}. \tag{3.8}$$

Hence, from (3.4), (3.7) and (3.8), we obtain

$$G(p,a,g) \equiv (-1)\left(\frac{b}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-1)/2} E(p,a,g)F(p,a,g) \pmod{\mathfrak{P}}.$$

As both sides of this congruence are integers and $\mathfrak{P} \mid p$ we have

$$G(p,a,g) \equiv -\left(\frac{b}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-1)/2}\ E(p,a,g)F(p,a,g) \pmod{p}$$

for any primitive root $g \equiv \zeta_{p-1} \pmod{\mathfrak{P}}$. Now let g' be any primitive root $(\mathrm{mod}\, p)$ so that $g' \equiv g^m \pmod{p}$ for some integer m satisfying $1 \le m \le p-2$, $\mathrm{GCD}(m, p-1) = 1$. Then, working modulo p, we have

$$\begin{aligned} G(p,a,g') &\equiv G(p,am,g) \\ &\equiv -\left(\frac{bm}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-1)/2}\ E(p,am,g)F(p,am,g) \\ &\equiv -\left(\frac{b}{r}\right)\left(\frac{m}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-1)/2}\ E(p,a,g')F(p,a,g) \\ &\equiv -\left(\frac{b}{r}\right)\left(\frac{2}{r}\right)^{\alpha+1} d^{(r-1)/2}\ E(p,a,g')F(p,a,g') \end{aligned}$$

as asserted. ∎

4. Special cases of the Theorem. An obvious interesting special case arises when r is a square, say $r = R^2$, $R > 0$. If $\mathfrak{P}$ is a prime ideal of

$Q(\zeta_{p(p-1)})$ lying above the prime ideal $(1-\zeta_p)$ of $Q(\zeta_p)$ and g is a primitive root $(\mathrm{mod}\, p)$ with $g \equiv \zeta_{p-1} \pmod{\mathfrak{P}}$ then, by Lemma 1(iv), we have, as $r = R^2 \equiv 1 \pmod 8$

$$F(p,a,g) \equiv R^{R^2-2} \pmod{\mathfrak{P}}.$$

As both sides of this congruence are integers and $\mathfrak{P} \mid p$, we must have

$$F(p,a,g) \equiv R^{R^2-2} \pmod p. \tag{4.1}$$

By Lemma 1(ii) we see that (4.1) holds for any primitive root $g \pmod p$.

Further, as $r = R^2 \equiv 1 \pmod 8$, we see that

$$E(p,a,g) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{if } \alpha = 1, \\ 2^{\alpha(R^2-2)/2}(1+g^{(p-1)b/4}) & \text{if } \alpha\,(\text{even}) \geq 2, \\ 2^{(\alpha(R^2-2)+1)/2} g^{(p-1)b/8} & \text{if } \alpha\,(\text{odd}) \geq 3. \end{cases}$$

Hence, by the Theorem, we obtain (as $d\,2^\alpha R^2 \equiv -1 \pmod p$)

Corollary 1. *If r is a square, say $r = R^2$, where $R > 0$, then*

$$G(p,a,g) \equiv \begin{cases} -1/R \pmod p & \text{if } \alpha = 0, \\ 0 \pmod p & \text{if } \alpha = 1, \\ -(1+g^{(p-1)b/4})/R2^{\alpha/2} \pmod p & \text{if } \alpha\,(\text{even}) \geq 2, \\ -g^{(p-1)b/8}/R2^{(\alpha-1)/2} \pmod p & \text{if } \alpha\,(\text{odd}) \geq 3. \end{cases}$$

A particular case of Corollary 1 is the following result:

If $p = M^2 + 1$ $(M > 0)$ is a prime then

$$\sum_{k=1}^{p-1} g^{k^2} \equiv \begin{cases} M-1 \pmod p & \text{if } g^{(p-1)/4} \equiv M \pmod p, \\ M+1 \pmod p & \text{if } g^{(p-1)/4} \equiv -M \pmod p. \end{cases}$$

Next we examine the relationship between $G(p,l,g)$ and $G(p,4l,g)$, where l is an integer such that $\mathrm{GCD}(l, p-1) = 1$, as in this case the two values of r given by (1.3) with $a = l$ and $a = 4l$ are the same.

Corollary 2. *If $\mathrm{GCD}(l,p-1) = 1$ and $p \equiv 1 \pmod 4$ then*

$$G(p,4l,g) \equiv \varepsilon(p,l,g) G(p,l,g) \pmod p,$$

where

$$\varepsilon(p,l,g) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod{16}, \\ 0 & \text{if } p \equiv 9 \pmod{16}, \\ 1 - g^{l(p-1)^2/16} & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

If $\mathrm{GCD}(l,p-1) = 1$ and $p \equiv 3 \pmod 4$ then

$$G(p,l,g) \equiv 0 \pmod p.$$

P r o o f. With $a = 4l$, where $\mathrm{GCD}(l, p-1) = 1$, we have

$$d = \mathrm{GCD}(a, p-1) = \mathrm{GCD}(4l, p-1) = \mathrm{GCD}(4, p-1)$$
$$= \begin{cases} 4 & \text{if } p \equiv 1 \pmod 4, \\ 2 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$
$$b = a/d = \begin{cases} l & \text{if } p \equiv 1 \pmod 4, \\ 2l & \text{if } p \equiv 3 \pmod 4, \end{cases}$$
$$q = (p-1)/d = \begin{cases} (p-1)/4 & \text{if } p \equiv 1 \pmod 4, \\ (p-1)/2 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$
$$\begin{cases} \alpha \geq 2 & \text{if } p \equiv 1 \pmod{16}, \\ \alpha = 1 & \text{if } p \equiv 9 \pmod{16}, \\ \alpha = 0 & \text{if } p \equiv 5 \pmod 8 \text{ or } p \equiv 3 \pmod 4, \end{cases}$$
$$r = \begin{cases} (p-1)/2^{\alpha+2} & \text{if } p \equiv 1 \pmod 4, \\ (p-1)/2 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

and with $a' = l$, where $\mathrm{GCD}(l, p-1) = 1$, we have

$$d' = \mathrm{GCD}(a', p-1) = \mathrm{GCD}(l, p-1) = 1,$$
$$b' = a'/d' = l,$$
$$q' = (p-1)/d' = p-1,$$
$$\alpha' = \begin{cases} \alpha + 2 & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$
$$r' = q'/2^{\alpha'} = r,$$

so that: $F(p, 4l, g) = F(p, l, g)$ in all cases, and

if $p \equiv 5 \pmod 8$

$$E(p, 4l, g) = 1, \quad E(p, l, g) = 2^{r-2}(1 + g^{(p-1)lr/4});$$

if $p \equiv 3 \pmod 4$

$$E(p, 4l, g) = 1, \quad E(p, l, g) = 0;$$

if $p \equiv 9 \pmod{16}$

$$E(p, 4l, g) = 0, \quad E(p, l, g) = 2^{(3r-5)/2} g^{(p-1)lr/8};$$

if $p \equiv 1 \pmod{16}$

$$E(p, l, g) = 2^{r-2} E(p, 4l, g).$$

Corollary 2 now follows from the Theorem.

We observe that Corollary 2 can be proved directly without appealing to the Theorem. We first treat the case $p \equiv 3 \pmod 4$. We have, modulo p,

$$G(p, l, g) \equiv \sum_{k=1}^{p-1} g^{lk^2} \equiv \sum_{k=1}^{p-1} g^{l(k+(p-1)/2)^2} \equiv g^{l((p-1)/2)^2} \sum_{k=1}^{p-1} g^{lk^2} \equiv -G(p, l, g),$$

so that $G(p,l,g) \equiv 0 \pmod p$.

Next we treat the case $p \equiv 1 \pmod 4$. We have

$$G(p,l,g) \equiv \sum_{k=1}^{p-1} g^{lk^2} \equiv \sum_{k=1}^{p-1} g^{l(k+(p-1)/4)^2} \pmod p,$$

that is,

$$G(p,l,g) \equiv g^{l((p-1)/4)^2} \sum_{k=1}^{p-1} (-1)^k g^{lk^2} \pmod p; \tag{4.2}$$

and working modulo p we have

$$\begin{aligned} G(p,4l,g) &\equiv \sum_{k=1}^{p-1} g^{4lk^2} \equiv \sum_{\substack{k=0 \\ k\neq (p-1)/2}}^{p-1} g^{4lk^2} \equiv 2 \sum_{k=0}^{(p-3)/2} g^{4lk^2} \\ &\equiv 2 \sum_{\substack{k=0 \\ k \text{ even}}}^{p-2} g^{lk^2} \equiv \sum_{k=0}^{p-2} (-1)^k g^{lk^2} + \sum_{k=0}^{p-2} g^{lk^2}, \end{aligned}$$

that is,

$$G(p,4l,g) \equiv \sum_{k=1}^{p-1} (-1)^k g^{lk^2} + G(p,l,g) \pmod p. \tag{4.3}$$

Eliminating $\sum_{k=1}^{p-1} (-1)^k g^{lk^2}$ from (4.2) and (4.3), we obtain

$$G(p,4l,g) \equiv (1 + g^{-l((p-1)/4)^2}) G(p,l,g) \equiv \varepsilon(p,l,g) G(p,l,g) \pmod p. \quad \blacksquare$$

Corollary 3.

$$G(p,a,g)G(p,-a,g) \equiv \begin{cases} -d \pmod p & \text{if } \alpha = 0, \\ 0 \pmod p & \text{if } \alpha = 1, \\ -2d \pmod p & \text{if } \alpha \geq 2. \end{cases}$$

Proof. We have by (1.4)

$$F(p,a,g) = F(p,-a,g)$$

so that by Lemma 1(iii) we obtain

$$F(p,a,g)F(p,-a,g) \equiv F(p,a,g)^2 \equiv (-1)^{(r-1)/2} r^{r-2} \pmod p.$$

From (1.5) we deduce

$$E(p,a,g)E(p,-a,g) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{if } \alpha = 1, \end{cases}$$

$$E(p,a,g)E(p,-a,g) \equiv 2^{\alpha(r-2)+1} \pmod p \quad \text{if } \alpha \geq 2.$$

Hence by the Theorem we have

$$G(p,a,g)G(p,-a,g) \equiv \left(\frac{-1}{r}\right) d^{r-1}(-1)^{(r-1)/2} r^{r-2} \times \left\{ \begin{array}{ll} 1 & \text{if } \alpha = 0 \\ 0 & \text{if } \alpha = 1 \\ 2^{\alpha(r-2)+1} & \text{if } \alpha \geq 2 \end{array} \right\} \pmod{p}$$

$$\equiv \left\{ \begin{array}{ll} -d & \text{if } \alpha = 0 \\ 0 & \text{if } \alpha = 1 \\ -2d & \text{if } \alpha \geq 2 \end{array} \right\} \pmod{p},$$

as $d\,2^{\alpha} r \equiv -1 \pmod{p}$.

This result can also be proved directly. We have working modulo p

$$G(p,a,g)G(p,-a,g) \equiv \sum_{k=1}^{p-1} g^{ak^2} \sum_{l=1}^{p-1} g^{-al^2} \equiv \sum_{k,l=1}^{p-1} g^{a(k^2-l^2)}$$

$$\equiv \sum_{l,m=1}^{p-1} g^{a((l+m)^2-l^2)} \equiv \sum_{l,m=1}^{p-1} g^{a(2lm+m^2)} \equiv \sum_{m=1}^{p-1} g^{am^2} \sum_{l=1}^{p-1} g^{2aml}$$

$$\equiv \sum_{\substack{m=1 \\ g^{2am} \equiv 1 \pmod{p}}}^{p-1} g^{am^2}(p-1) \equiv - \sum_{\substack{m=1 \\ 2am \equiv 0 \pmod{p-1}}}^{p-1} g^{am^2},$$

that is,

$$G(p,a,g)G(p,-a,g) \equiv - \sum_{\substack{m=1 \\ 2m \equiv 0 \pmod{q}}}^{p-1} g^{am^2}.$$

If $\alpha = 0$ we have

$$G(p,a,g)G(p,-a,g) \equiv - \sum_{\substack{m=1 \\ m \equiv 0 \pmod{r}}}^{dr} g^{bdm^2} \equiv - \sum_{n=1}^{d} g^{bdr^2n^2}$$

$$\equiv - \sum_{n=1}^{d} g^{(p-1)brn^2} \equiv -d.$$

If $\alpha = 1$, so that $b \equiv 1 \pmod{2}$, we have

$$G(p,a,g)G(p,-a,g) \equiv - \sum_{\substack{m=1 \\ m \equiv 0 \pmod{r}}}^{2dr} g^{bdm^2} \equiv - \sum_{n=1}^{2d} g^{bdr^2n^2}$$

$$\equiv - \sum_{n=1}^{2d} (g^{(p-1)/2})^{brn^2} \equiv - \sum_{n=1}^{2d} (-1)^n \equiv 0.$$

If $\alpha \geq 2$, so that $b \equiv 1 \pmod 2$, we have

$$G(p,a,g)G(p,-a,g) \equiv - \sum_{\substack{m=1 \\ m \equiv 0 \pmod{2^{\alpha-1}r}}}^{2^\alpha dr} g^{bdm^2} \equiv - \sum_{n=1}^{2d} g^{bd2^{2\alpha-2}r^2n^2}$$

$$\equiv - \sum_{n=1}^{2d} (g^{p-1})^{b2^{\alpha-2}rn^2} \equiv -2d\,. \quad \blacksquare$$

We conclude with two other special cases which follow easily from the Theorem.

COROLLARY 4. *If* $\mathrm{GCD}(l, p-1) = 1$ *and* $p \equiv 5 \pmod 8$ *then*

$$G(p, 2l, g) \equiv 0 \pmod p\,.$$

COROLLARY 5. *If* $\mathrm{GCD}(l, p-1) = 1$ *then*

$$G(p, al, g) \equiv \left(\frac{l}{r}\right) \delta(p,a,l,g) G(p,a,g) \pmod p\,,$$

where

$$\delta(p,a,l,g) = \begin{cases} g^{(p-1)br(l-1)/8} & \text{if } \alpha\,(\text{odd}) \geq 3\,, \\ g^{-(p-1)br/4} & \text{if } \alpha\,(\text{even}) \geq 2 \text{ and } l \equiv 3 \pmod 4\,, \\ 1 & \text{otherwise.} \end{cases}$$

References

[1] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin 1982.
[2] T. Nagell, *Introduction to Number Theory*, Almqvist & Wiksell, Stockholm 1951.
[3] H. Weber, *Lehrbuch der Algebra*, Vol. 1, 3rd ed., Chelsea, New York 1961.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA K1S 5B6

Received on 27.9.1990
and in revised form on 12.6.1991 (2085)