1 Characters.

Let G be a commutative group with identity element e. Then we recall that a character is a group homomorphism

$$\chi : G \to \mathbb{C}^{\times} = \mathbb{C} - \{0\}.$$

That is $\chi(ab) = \chi(a)\chi(b)$ for $a, b \in G$. We denote by $\widehat{G}$ the set of characters of G. The following properties are satisfied by group characters.

1) $\chi(e) = 1$. This is because $\chi(e) = \chi(ee) = \chi(e)^2$. Thus $\chi(e)(\chi(e) - 1) = 0$. Since $\chi(e) \neq 0$, this implies that $\chi(e) = 1$.

2) $\chi(g^{-1}) = \chi(g)^{-1}$. To see this we note that $1 = \chi(e) = \chi(gg^{-1}) = \chi(g)\chi(g^{-1})$.

3) If G is finite that $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$. For this we note that there exists $l > 0$ such that $g^l = e$. This implies that $\chi(g)^l = 1$. Set $z = \chi(g)$. Since $z \neq 0$ there exists w such that $z = e^w$. Thus $e^{lw} = 1$ and this implies that $lw = 2\pi ik$ with $k \in \mathbb{Z}$. Thus $w = 2\pi i\frac{k}{l}$. This implies that $z = \cos(2\pi\frac{k}{l}) + i\sin(2\pi\frac{k}{l})$. Also,

$$\chi(g^{-1}) = \chi(g)^{-1} = e^{-w} = e^{-2\pi i\frac{k}{l}} = \cos(2\pi\frac{k}{l}) - i\sin(2\pi\frac{k}{l})$$

since $\cos(-x) = \cos(x)$ and $\sin(-x) = -\sin(x)$.

4) We note that the proof of 3) also shows that if G is finite and $g \in G$ then $\chi(g)^{l(g)} = 1$ for some $l(g) > 1$.

Lemma 1 *If G is finite and $\chi \in \widehat{G}$ has the property that $\chi(a) \neq 1$ for some $a \in G$ then*

$$\sum_{g \in G} \chi(g) = 0.$$

Proof. We note that since the map $f : G \to G$ given by $f(g) = ag$ is one to one and onto $G = \{ag | g \in G\}$. Thus if $u = \sum_{g \in G} \chi(g)$ then

$$u = \sum_{g \in G} \chi(ag) = \sum_{g \in G} \chi(a)\chi(g) = \chi(a)\sum_{g \in G} \chi(g) = \chi(a)u.$$

Thus $(\chi(a) - 1)u = 0$. Since $\chi(a) - 1 \neq 0$ we must have $u = 0$. ■

2 Gauss sums.

Throughout this section p be an odd prime. Recall that a Dirichlet character mod p can be considered to be a character of the group $F_p^\times$ in the following way. If $\chi \in \widehat{F_p^\times}$ then extend it as a function to F_p by $\chi(0) = 0$. If $z \in \mathbb{Z}$ then define $\chi(z)$ to be the value of χ on the class of z modulo p. This defines a Dirichlet charcter modulo p. If χ is a Dirichlet charcter modulo p then $\chi(a)$ depends only on the equivalence class of a mod p. We can thus consider it to be a function on F_p. $\chi(0) = 0$ and $\chi_{|F_p^\times} \in \widehat{F_p^\times}$. This shows that we can use the terms "Dirichlet character mod p" and "character of $F_p^\times$" interchangably.

If χ is a Dirichlet character mod p and if $a \in \mathbb{Z}$, $p \nmid a$ then we set

$$g_a(\chi) = \sum_{j=0}^{p-1} \chi(j) e^{2\pi i a j/p}.$$

Then g_a is called a *Gauss sum.*

Lemma 2 *Let $a \in \mathbb{Z}$ be such that $p \nmid a$ then if $a' \in \mathbb{Z}$ satisfies $a'a \equiv 1 \bmod p$ then $g_a(\chi) = \chi(a') g_1(\chi)$.*

Proof. Modulo p the sets $\{0, 1, 2, ..., p-1\}$ and $\{a'0, a'1, a'2, ..., a'(p-1)\}$ are the same thus

$$g_a(\chi) = \sum_{j=0}^{p-1} \chi(j) e^{2\pi i a j/p} = \sum_{j=0}^{p-1} \chi(a'j) e^{2\pi i a a' j/p}.$$

Since $a'a \equiv 1 \bmod p$ we have

$$\sum_{j=0}^{p-1} \chi(a'j) e^{2\pi i a a' j/p} = \sum_{j=0}^{p-1} \chi(a')\chi(j) e^{2\pi i j/p} = \chi(a') \sum_{j=0}^{p-1} \chi(j) e^{2\pi i j/p}.$$

Since $g_1(\chi) = \sum_{j=0}^{p-1} \chi(j) e^{2\pi i j/p}$ the proof is complete. ■

We now come to a truly remarkable theorem of Gauss.

Theorem 3 *If χ is a Dirichlet character modulo p that is not the principal character and if $p \nmid a$ then*

$$|g_a(\chi)|^2 = p.$$

Proof. We note that $|\chi(a')| = 1$ (here we use the notation of the previous section and 3) therein. Thus the previous lemma implies that we may assume that $a = 1$. We write

$$|g_1(\chi)|^2 = g_1(\chi)\overline{g_1(\chi)} = \sum_{j=0}^{p-1} \chi(j) e^{2\pi i j/p} \overline{\sum_{k=0}^{p-1} \chi(k) e^{2\pi i k/p}}$$

$$= \sum_{\substack{j=0 \\ k=0}}^{p-1} \chi(j)\overline{\chi(k)} e^{2\pi i (j-k)/p}.$$

since $\overline{e^{ix}} = e^{-ix}$.

We now note that since $F_p^\times$ has a primitive root, ν, we see that modulo p the set $\{0, 1, 2, ..., p-1\}$is the same as $\{0, \nu^0, \nu^1, ..., \nu^{p-2}\}$. Since $\chi(0) = 0$, we see that the last formula above is

$$\sum_{\substack{j=0 \\ k=0}}^{p-2} \chi(\nu^j)\overline{\chi(\nu^k)} e^{2\pi i (\nu^j - \nu^k)/p} = \sum_{\substack{j=0 \\ k=0}}^{p-2} \chi(\nu^{j-k}) e^{2\pi i (\nu^j - \nu^k)/p}.$$

Since $\overline{\chi(\nu^k)} = \chi(\nu^{-k})$. We now make the change of variables modulo $p-1$, $l = j - k$. Then $j = l + k$ modulo $p-1$.Since $\nu^{p-1} = 1$ we the last sum above is

$$\sum_{\substack{l=0 \\ k=0}}^{p-2} \chi(\nu^l) e^{2\pi i (\nu^{k+l} - \nu^k)/p}.$$

We rewrite this sum as

$$\sum_{l=0}^{p-2} \chi(\nu^l) \left(\sum_{k=0}^{p-2} e^{2\pi i (\nu^l - 1)\nu^k/p} \right).$$

We consider the sum

$$\sum_{k=0}^{p-2} e^{2\pi i (\nu^l - 1)\nu^k/p}.$$

We note that $\{\nu^0, \nu^1, ..., \nu^{p-2}\}$ and $\{1, 2, ..., p-1\}$ are the same modulo p. Hence

$$\sum_{k=0}^{p-2} e^{2\pi i(\nu^l-1)\nu^k/p} = \sum_{j=1}^{p-1} e^{2\pi i(\nu^l-1)j/p} = \sum_{j=0}^{p-1} e^{2\pi i(\nu^l-1)j/p} - 1.$$

If $\zeta_b = e^{2\pi ib/p}$with $b \in \mathbb{Z}$ then since $\zeta_b^{p-1} = 1$ and $\zeta_b = 1$ if and only if p divides b we have

$$\sum_{j=0}^{p-1} \zeta_b^j = \begin{cases} p \text{ if } p|b \\ 0 \text{ if } p \nmid b \end{cases}.$$

Applying this with $b = \nu^l - 1$ with $0 \leq l \leq p-2$ we have

$$\sum_{j=0}^{p-1} e^{2\pi i(\nu^l-1)j/p} - 1 = \begin{cases} p-1 \text{ if } l = 0 \\ -1 \text{ if } 1 \leq l \leq p-2 \end{cases}.$$

Returning to our calculation we now plug in the above values

$$\sum_{l=0}^{p-2} \chi(\nu^l) \left(\sum_{k=0}^{p-2} e^{2\pi i(\nu^l-1)\nu^k/p} \right) = (p-1) - \sum_{l=1}^{p-2} \chi(\nu^l).$$

Now Lemma 1 says that the sum

$$\sum_{l=0}^{p-2} \chi(\nu^l) = 0$$

since χ is not principal.Thus $\sum_{l=1}^{p-2} \chi(\nu^l) = -1$. Hence we have

$$(p-1) - \sum_{l=1}^{p-2} \chi(\nu^l) = p.$$

This completes the proof. ■

Corollary 4 *If χ is a real valued Dirichlet character that is not principle and $p \nmid a$ then*

$$g_a(\chi)^2 = (-1)^{\frac{p-1}{2}} p.$$

Note that we have observed that if $\chi$is non-principal then $\chi(x) = \left(\frac{x}{p}\right)$(the Legendre symbol).

We now prove the corollary.

Since $\chi(a') \in \{\pm 1\}$ we may assume $a = 1$. As above

$$g(\chi)^2 = \sum_{\substack{j=0 \\ k=0}}^{p-1} \chi(j)\chi(k)e^{2\pi i(j+k)/p}.$$

We make the change of variables (mod p) $k \to -k$ and get (noting that $-k = (-1)k$ and $\chi((-1)k) = \chi(-1)\chi(k)$)

$$\sum_{\substack{j=0 \\ k=0}}^{p-1} \chi(j)\chi(-k)e^{2\pi i(j-k)/p} = \sum_{\substack{j=0 \\ k=0}}^{p-1} \chi(-1)\chi(j)\chi(k)e^{2\pi i(j-k)/p}.$$

We observe that $\overline{\chi(k)} = \chi(k)$ so we have

$$g(\chi)^2 = \chi(-1) \sum_{\substack{j=0 \\ k=0}}^{p-1} \chi(j)\overline{\chi(k)}e^{2\pi i(j-k)/p} =$$

$$\chi(-1)|g_1(\chi)|^2 = \chi(-1)p$$

by the theorem above. Since $\chi(-1) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ we have completed the proof.