# Notes for Cryptography

Professor Brian Sittinger

April 25, 2016

## 1 Quadratic Gauss Sums

The final presentation is in 2 weeks. We define *A Quadratic Gauss Sum* as a Gauss sum that is quadratic. In other words, we define

$$g_a \equiv \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta_p^{at}$$

Where $\left(\frac{t}{p}\right)$ for some $a \in \mathbb{Q}$. We propose that

$$g_a = \left(\frac{a}{p}\right) g_1$$

We prove this as follows. If $a = 0, \zeta_p^{at} = 0$, then

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$$

Because there are an equal number of quadratic residues and quadratic non-residues. We now apply the first isomorphism theorem.

$$\zeta : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$$

$$\zeta(x) = x^2$$

homomorphism. Kernel $\zeta = \left\{x | x^2 = 1 \pmod p\right\} = \{\pm 1\}$. Sp

$$mathbbZ_p^*/\ker\zeta \cong \ker\zeta$$

Which implies the cardinality

$$\frac{p-1}{2} = |\ker\zeta|$$

We now consider the case that $a \not\equiv 0 \mod p$.

$$\left(\frac{a}{p}\right) \cdot g_a = \left(\frac{a}{p}\right) \sum \left(\frac{t}{p}\right) \zeta_p^{at} = \sum \left(\frac{at}{p}\right) = \sum_x \left(\frac{x}{p}\right) \zeta_p^x = g_1$$

We now make another proposition. We claim that

$$g^2 = (-1)^{\frac{p-1}{2}} p$$

($p$ is an odd prime for all Legendre symbol stuff, we're not dealing with the Kroniker symbol). Franz Lemmermeyer defined Reciprocity Laws in an important text. We prove the previous proposition as follows. Suppose

$$a \not\equiv 0 \pmod{p}$$

We compute $\sum_a g_a g_a$ in two ways. Firstly, we consider

$$g_a g_{-a} = \left(\frac{a}{p}\right) g \cdot \left(\frac{-a}{p}\right) = \left(\frac{-a^2}{p}\right) g^2 = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right) g^2$$

By proposition 1. Now

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{a^2}{p}\right) = 1$$

And so,

$$g_a g_{-a} = (-1)^{\frac{p-1}{2}} g^2$$

So we sum them all $a \in \mathbb{Z}_p^*$

$$\sum_a g_a g_{-a} = \sum_a (-1)^{\frac{p-1}{2}} g^2 (p-1)$$

We now return to try the other way to add them together.

$$g_a g_{-a} = \left[\sum_x \left(\frac{x}{p}\right) \zeta^{ax}\right] \cdot \left[\sum_y \left(\frac{y}{p}\right) \zeta^{-ay}\right]$$

And then we distribute.

$$= \sum_x \sum_y \left(\frac{xy}{p}\right) \zeta^{a(x-y)}$$

And when $x \neq y$ this is 0, and when $x = y$, this greatly simplifies

$$= 0 + p(p-1) = p(p-1)$$

By combining both approaches, and canceling terms, this yields the proposition. A cultural remark is that Gauss proved that

$$g = +\sqrt{(-1)^{\frac{p-1}{2}} p}$$

A corollary to this is that if we let $m$ be a square free integer. Recall that $g_a \in \mathbb{Z}[\zeta_p]$. We now consider a compositum. Our Theorem/corollary is thus

$$\mathbb{Q}[\sqrt{m}] =\subseteq \begin{cases} \mathbb{Q}(\zeta_{|m|}) & \text{if } m \equiv 1 \pmod 4 \\ \mathbb{Q}(\zeta_{|4m|}) & \text{if } m \not\equiv 1 \pmod 4 \end{cases}$$

Interestingly enough, a prime in $\mathbb{Q}[\sqrt{m}]$ is inert in $\mathbb{Q}[\zeta]$.

Quadratic reciprocity. Let $pq$ be distinct odd primes. Then,

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 0 & \text{if } p|a \\ -1 & \text{if } x^2 \equiv a \pmod p \text{is not solvable} \\ 1 & \text{if } x^2 \equiv a \pmod p \text{is solvable} \end{cases}$$

Laws of quadratic reciprocity.

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Supplementary laws

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

Lemma: $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$. That is, $\mathbb{Z}_p^*$ is cyclic of order $p-1$. Proof: We know that $|\mathbb{Z}_p^*$. Show that the smallest positive integer $h$ such that $x^h = 1 \pmod p$. For all $x$ in the units of $\mathbb{Z}_p$.

Euler's Criterion. Let $p$ be an odd prime and $a$ is not a multiple of $p$. Then

$$a^{\frac{p-2}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$$

That is, that $a$ is a Quadratic Residue mod $p$ iff $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. So there exists $k \in \mathbb{Z} : k^2 \equiv a \pmod p$. Then

$$a^{\frac{p-1}{2}} \equiv k^{p-1} \equiv 1 \pmod p$$

By Fermat's little theorem. Going the other direction, we suppose that

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

since $\mathbb{Z}_p^*$ is cyclic of order $p-1$. Then $\mathbb{Z}_p^* = \langle g \rangle$ for some $g \in \mathbb{Z}_p^*$. Therefore,

$$a \equiv g^j$$

for positive non-zero integer $j$. Therefore,

$$(g^j)^{(p-1)/2} = j^{\frac{j(p-1)}{2}} \equiv 1 \pmod p$$

Since the order of $g$ is $p-1$, this forces $j(p-1)/2$ to be a multiple of $p-1$. Thus $j$ is even. Then $j = 2k$, and we let $b = g^k$. Then

$$b^2 \equiv g^j \equiv a \pmod{p}$$

Therefore $a$ is a quadratic residue mod $p$.

Proof of Quadratic Reciprocity. We define $p^* = (-1)^{\frac{p-1}{2}} p$. We work modulo $q$ in $\mathbb{Z}[\zeta_p]$.

$$g_1^{q-1} = (g^2)^{\frac{q-1}{2}} = (p*)^{\frac{q-1}{2}} = \left(\frac{p^*}{q}\right)$$

$$g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q}$$

Moreover,

$$g^q \equiv \left(\sum_t \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum_t \left(\frac{t}{p}\right)^q \zeta^{qt} = g_q$$

$$\left(\frac{t}{p}\right) = \left(\frac{t}{q}\right)$$

And apply the definition of the quadratic Gauss sums. Therefore,

$$g^q \equiv g_q \equiv \left(\frac{q}{p}\right) g \mod q$$

And because $p$ and $q$ are distinct odd primes,

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

And since

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

And quadratic residue now follows. This proof was developed by Gauss in the search for higher order reciprocity laws. The Eisenstein integers and everything from the start of this class was done in search for said laws.