Notes of 29th November and 1st December

0.1 Proof via Gauss Sums

We give a proof of QRL using the so-called Gauss sums. This will need one fact that we will assume without proof for the present. It will be mentioned below.
For a prime p, and a primitive p-th root ζ of unity, we define the Gauss sum

$$G := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\zeta^a.$$

Now

$$G^2 = \sum_{a,b} \left(\frac{ab}{p}\right)\zeta^{a+b} = \sum_{a,c} \left(\frac{c}{p}\right)\zeta^{a(1+c)}$$

where we have put $b = ac$ and used the fact that $\left(\frac{a^2c}{p}\right) = \left(\frac{c}{p}\right)$.
Splitting the term corresponding to $c = p-1$ separately, we obtain

$$G^2 = \sum_{a=1}^{p-1} \left(\frac{-1}{p}\right)1 + \sum_{c\neq -1} \left(\frac{c}{p}\right) \sum_a \zeta^{a(1+c)}.$$

When $c \neq -1$, the sum $\sum_a \zeta^{a(1+c)} = \sum_{d=1}^{p-1} \zeta^d = -1$.
Hence

$$G^2 = \left(\frac{-1}{p}\right)(p-1) + \sum_{c\neq -1} \left(\frac{c}{p}\right).$$

As $\sum_{c=1}^{p-1}(\left(\frac{c}{p}\right) = 0$, we obtain

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

Note, in particular, that $\left(\frac{-1}{p}\right)p \in \mathbb{Q}(\zeta)$.
As $i = \zeta_4$ and $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, this shows that the square-roots of any integer are expressible as integer linear combinations of powers of some roots of unity.

To use this for quadratic reciprocity, we consider an odd prime $q \neq p$. From

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

we get

$$G^{q-1} = (G^2)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}p^{(q-1)/2}.$$

So $G^q = (-1)^{(p-1)(q-1)/4}p^{(q-1)/2}G$. We shall compute G^q in another way. Indeed, by binomial expansion

$$G^q = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta^{aq} + qS$$

where $S \in \mathbb{Z}[\zeta]$, the set of numbers which are expressible as integer polynomial expressions of ζ. We have used the fact that the binomial coefficients $\binom{q}{r}$ are multiples of q when $0 < r < q$. Now

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta^{aq} = \sum_{b=1}^{p-1}\left(\frac{bq^{-1}}{p}\right)\zeta^{b} = \left(\frac{q^{-1}}{p}\right)G$$

putting $aq = b$. Hence,

$$G^q = \left(\frac{q^{-1}}{p}\right)G + qS$$

which gives

$$\left((-1)^{(p-1)(q-1)/4}p^{(q-1)/2} - \left(\frac{q^{-1}}{p}\right)\right)G = qS.$$

Calling the integer $u = (-1)^{(p-1)(q-1)/4}p^{(q-1)/2} - \left(\frac{q^{-1}}{p}\right)$, we have $uG = qS$ which implies

$$u\left(\frac{-1}{p}\right)p = uG^2 = qSG.$$

Thus, the rational number $\frac{1}{q}u\left(\frac{-1}{p}\right)p = SG \in \mathbb{Z}[\zeta]$.

We assume the following fact:

Fact. $\mathbb{Z}[\zeta] \cap \mathbb{Q} = \mathbb{Z}$.

We assume this without proof for now. It implies in our case that $u\left(\frac{-1}{p}\right)p \equiv 0 \bmod q$, and hence $u \equiv 0 \bmod q$.

Recalling that $u = (-1)^{(p-1)(q-1)/4} p^{(q-1)/2} - \left(\frac{q^{-1}}{p}\right)$, and noting that $p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \bmod q$, and that $\left(\frac{q^{-1}}{p}\right) = \left(\frac{q}{p}\right)$, we obtain QRL.

As an immediate application, we see that 3 is a quadratic residue modulo a prime $p > 3$ if, and only if, $p \equiv \pm 1 \bmod 12$.

0.2 Some applications of QRL

Exercise* *Let p, q be odd prime number such that $(\frac{p}{q}) = (\frac{q}{p}) = 1$ and $p \equiv 1$ mod 8. Then, the polynomial $P(X) = (X^2 - p - q)^2 - 4pq$ is irreducible whereas it is reducible modulo any integer.*

Solution. *Look at the proof only after trying the exercise.*
The proof uses only QRL. Before proceeding, we just remark that in the language of Galois theory, this means that the Galois group of this polynomial over $\mathbb{Q}$ has order 4 but is not cyclic.
Now

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X - \sqrt{p} - \sqrt{q})(X + \sqrt{p} + \sqrt{q})(X - \sqrt{p} + \sqrt{q})(X + \sqrt{p} - \sqrt{q}). \end{aligned}$$

Since $\sqrt{p}, \sqrt{q}, \sqrt{p} \pm \sqrt{q}, \sqrt{pq}$ are all irrational, none of the linear or quadratic factors of $P(X)$ are in $\mathbb{Z}[X]$. It suffices to show that a factorization of P exists modulo any prime power as we can use Chinese reminder theorem to get a factorisation modulo a general integer. Let us check modulo prime powers now. We have the equivalent expressions:

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X^2 + p - q)^2 - 4pX^2 \\ &= (X^2 - p + q)^2 - 4qX^2 \\ &= (X^2 - p - q)^2 - 4pq. \end{aligned}$$

The second and third equalities above show that $P(X)$ is reducible modulo any p^n and any q^n. Also since $p \equiv 1 \bmod 8, p$ is a quadratic residue modulo any 2^n and the second equality above again shows that $P(X)$ is reducible mod 2^n.

If ℓ is a prime $\neq 2, p, q$, let us show now that $P(X)$ is reducible modulo l^n for any n.
At least one of $(\frac{p}{\ell}), (\frac{q}{\ell})$ and $(\frac{pq}{\ell})$ is 1 because, by the product formula for Legendre symbols, $(\frac{p}{\ell})(\frac{q}{\ell})(\frac{pq}{\ell}) = 1$.
According as $(\frac{p}{\ell}), (\frac{q}{\ell})$ or $(\frac{pq}{\ell}) = 1$, the expressions $(X^2 + p - q)^2 - 4pX^2$ or $(X^2 - p + q)^2 - 4qX^2$ or $(X^2 - p - q)^2 - 4pq$ shows that $P(X)$ is reducible mod ℓ^n for any n.

1. We know from QRL that the symbol $\left(\frac{3}{p}\right) = 1$ if, and only if, $p \equiv \pm 1$ mod 12. We have noted earlier that 2 is not a primitive root mod a Fermat *prime* $F_n = 2^{2^n} + 1$ with $n > 1$. However, we verify now that 3 is a primitive root mod any Fermat prime F_n with $n > 0$. Indeed, since the order of 3 mod F_n would divide 2^{2^n} if F_n is prime, then the assertion $3^{(F_n-1)/2} \equiv -1$ mod F_n would be equivalent to 3 being a primitive root mod F_n. That is, this is equivalent to $\left(\frac{3}{F_n}\right) = -1$ and hence, equivalent to $F_n \equiv \pm 5$ mod 12. Clearly, $F_n \equiv 5$ mod 12 as it is 1 mod 4 and 2 mod 3.

2. We claim that $2^n - 1$ cannot divide $3^n - 1$ if $n > 1$.
Write $a_n = 2^n - 1$ and $b_n = 3^n - 1$ and suppose $a_n | b_n$ for some $n > 1$. Then, n is odd (otherwise $a_n \equiv 0$ mod 3). So, $a_n \equiv 1$ mod 3 and $\equiv -1$ mod 4.
In other words, $a_n \equiv 7$ mod 12. Thus, a_n has a prime divisor $p \equiv \pm 5$ mod 12. Now, $3^n \equiv 1$ mod p implies $\left(\frac{3}{p}\right) = 1$ as n is odd.
QRL gives $\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$ or -1 according as to whether $p \equiv 1$ mod 4 or 3 mod 4.
But, $\left(\frac{p}{3}\right) = 1$ or -1 according as to whether $p \equiv -5$ or 5 mod 12. This is a contradiction.

3. We can verify that $1/47$ has decimal expansion with period 46. Can we generalize this? Let n be a positive integer such that both $20n+3, 40n+7$ are primes. We prove that the decimal expansion of $\frac{1}{40n+7}$ has period $40n + 6$.
Note that the period of the decimal expansion of $1/p$ is the order of 10 mod p. By quadratic reciprocity law, 10 is a (non-zero) square modulo a prime p if and only if p is of the form $40m \pm 1, 40m \pm 3, 40m \pm 9$ or $40m \pm 13$. Indeed, 2 is a square mod p iff $p = 8k \pm 1$ and 5 is a square mod p iff $p = 5u \pm 1$. Thus, in our case of $p = 40n + 7$, the order of 10 is d which is a divisor of $p-1$ and is not equal to the odd prime $(p-1)/2$ (because 10 is a non-square mod p means $10^{(p-1)/2} \equiv -1$ mod p). Hence, the order must be $p - 1$ (it

cannot be 2 because $p > 11$)

4. Let p be a prime such that every quadratic non-residue mod p is a primitive root mod p. Then, $p = 2^{2^n} + 1$ for some $n \geq 0$. In other words, $p = 3$ or a Fermat prime.
Indeed, $p = 3$ satisfies this; assume $p \neq 3$. Consider a possible odd divisor d of $p - 1$. Consider an element a of order $(p-1)/d$ in the cyclic group $\mathbb{Z}_p^*$. Note that $a^{(p-1)/2} \equiv -1 \bmod p$; otherwise, the order $(p-1)/d$ of a would divide $(p-1)/2$, an impossibility. Thus, a is a quadratic non-residue mod p. Hence, it would have to be a primitive root; that is, the order $(p-1)/d$ equals $p - 1$. Therefore, $d = 1$. So, $p - 1$ is a power of 2 and is a prime which implies it is a Fermat prime.

1 Problems on QRL from NZM

The following problems are from the exercises following section 3.2 of NZM.

Exercise 17, section 3.2. If $19a^2 \equiv b^2 \bmod 7$ for some integers a, b, we claim that this congruence must hold modulo 7^2.
Indeed, if $(7, a) = 1$, then we would have $19 \equiv (a^{-1}b)^2 \bmod 7$ which means $\left(\frac{19}{7}\right) = 1$. This is clearly checked to not hold. Hence $7|a$. Hence $7|b$ also. So, we have $19a^2 \equiv b^2 \bmod 7^2$.

Exercise 20, section 3.2. If x, y are integers, we shall show that $\frac{x^2-2}{2y^2+3}$ cannot be an integer.
Indeed, the denominator is an odd number which is either 3 or 5 mod 8. Hence, it must have some prime divisor $p \equiv \pm 3 \bmod 8$. But such a prime cannot divide the numerator as, otherwise, 2 would be a quadratic residue mod p.

Exercise 22, section 3.2. If p is an odd prime not dividing ab, we show that the number of solutions for x, y satisfying $ax^2 + by^2 \equiv 1 \bmod p$ is $p - \left(\frac{-ab}{p}\right)$.
For any solution x, y we have, mod p,

$$a^2x^2 \equiv a - aby^2 = (-ab)(y^2 - b^{-1}).$$

That is, $\left(\frac{-ab(y^2-b^{-1})}{p}\right) = 1$.

We digress to observe a few things. First, note that $x^2 \equiv d \bmod p$ has $1 + \left(\frac{d}{p}\right)$ solutions.

We claim that $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right)$ *equals* $p-1$ *or* -1 *according as to whether* p *divides* a *or not.*

We may assume p does not divide a; else, it is clear.

By the above exercise, the number of solutions of $x^2 \equiv y^2 + a \bmod p$ is $1+\left(\frac{y^2+a}{p}\right)$. Therefore, varying y also, it follows that the number of solutions in x, y of $x^2 - y^2 \equiv a \bmod p$ is

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right) = p + \sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right).$$

On the other hand, the number of solutions of $x^2 - y^2 \equiv a$ is exactly $p-1$ since this congruence is equivalent to $uv \equiv a$ where $u = x+y, v = x-y$, and since $(a,p) = 1$, each $v \neq 0$ has exactly one u. Comparison of the two expressions for the number of solutions proves $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right)$ equals -1 when $(a,p) = 1$.

We already counted the number of solutions (as y varies) as the expression

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{-ab}{p}\right)\left(\frac{y^2-b^{-1}}{p}\right)\right).$$

As the above count implies that $\sum_{y=0}^{p-1} \left(\frac{y^2-b^{-1}}{p}\right) = -1$ (since $-b^{-1}$ is coprime to p), we get the expression asserted.

Exercise 23, section 3.2. If a, b are positive integers, then we claim

$$\sum_{r=1}^{[a/2]} [rb/a] + \sum_{s=1}^{[b/2]} [sa/b] = [a/2][b/2] - [GCD(a,b)/2].$$

This is exactly similar to Eisenstein's proof of QRL we discussed that used counting lattice points excepting that we have two integers a, b that may not be primes.

Look at the line $ay = bx$ and we first look at all the lattice points (x, y) with $1 \leq x \leq a/2$ and $1 \leq y \leq b/2$. These are clearly $[a/2][b/2]$ in number.

Among them exactly $[GCD(a,b)/2]$ lie on the line. The other lattice points we counted are either below or above the line. Clearly, these are the two sums on the LHS of our assertion.