Quadratic Reciprocity Part 2

Theorem : (12.4)

If p and q are odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Proof. Suppose that $p \equiv q \equiv 3 \mod 4$. Then $\frac{(p-1)(q-1)}{4}$ is odd and thus

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \quad \text{so} \quad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

Suppose that $p \equiv 1 \mod 4$ or $p \equiv 1 \mod 4$. Then, $\frac{(p-1)(q-1)}{4}$ is even and thus

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \quad \text{so} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

As in the proof of Gauss's Lemma, take the least residues modulo p of

$$q, \quad 2q, \quad 3q, \quad \ldots, \quad \frac{p-1}{2} \cdot q$$

Then, separate the least residues modulo p into two classes. Put the residues less than or equal to $\frac{p-1}{2}$ in one class and call them

$$r_1, \quad r_2, \quad \ldots, \quad r_k$$

Put the least residues greater than $\frac{p-1}{2}$ in another class and call them

$$s_1, \quad s_2, \quad \ldots, \quad s_g$$

The conclusion of Gauss's Lemma is that

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

To simplify notation later, define R and S as

$$R = r_1 + r_2 + \cdots + r_k, \quad S = s_1 + s_2 + \cdots + s_g$$

While proving Gauss's Lemma, we showed that the set of numbers

$$r_1, \quad r_2, \quad \ldots, \quad r_k, \quad p - s_1, \quad p - s_2, \quad \ldots, \quad p - s_g$$

Was simply a permutation of the set of numbers

$$1, \quad 2, \quad \ldots, \quad \frac{p-1}{2}$$

It follows that the two sums are equivalent

$$\begin{aligned} 1 + 2 + \cdots + \frac{p-1}{2} &= r_1 + r_2 + \cdots + r_k + p - s_1 + p - s_2 + \cdots + p - s_g \\ R + gp - S &= \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \\ R &= \frac{p^2-1}{8} + S - gp \end{aligned}$$

The least residue modulo p of jq for $j = 1, 2, \ldots, \frac{p-1}{2}$, is the remainder when we divide jq by p. We know the quotient is $\left[\frac{jq}{p}\right]$, so if we let t_j denote the least residue modulo p of jq, we have

$$jq = \left[\frac{jq}{p}\right] p + t_j$$

If we sum these equations over j, we have

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}} jq &= \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] p + \sum_{j=1}^{\frac{p-1}{2}} t_j \\ q\sum_{j=1}^{\frac{p-1}{2}} j &= p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] + \sum_{j=1}^{k} r_j + \sum_{j=1}^{g} s_j\end{aligned}$$

This gives us that

$$\begin{aligned}q \cdot \frac{p^2-1}{8} &= p \cdot S(p,q) + R + S \\ q \cdot \frac{p^2-1}{8} &= p \cdot S(p,q) + S + \frac{p^2-1}{8} + S - gp \\ (q-1) \cdot \frac{p^2-1}{8} &= p \cdot (S(p,q) - g) + 2S\end{aligned}$$

The left-hand side is even because $\frac{p^2-1}{8}$ is an integer and $q-1$ is even. The right side has $2S$ even, so it follows that $p(S(p,q)-g)$ is even. Therefore, $S(p,q)-g$ is even, and hence

$$\begin{aligned}(-1)^{S(p,q)-g} &= 1 \\ (-1)^{S(p,q)} &= (-1)^g\end{aligned}$$

Since $(-1)^g = \left(\frac{q}{p}\right)$, we get that

$$\left(\frac{p}{q}\right) = (-1)^{S(p,q)}$$

Now, we can repeat the argument with p and q interchanged to get

$$\left(\frac{p}{q}\right) = (-1)^{S(q,p)}$$

Multiplying together, we get that

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

Therefore, by Lemma 12.1, we have that

$$\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

□

Primality Testing: It is not know whether 2 is a primitive root of infinitely many primes.

Theorem : (12.3)

If p and $4p+1$ are both primes, then 2 is a primitive root modulo $4p+1$.

Proof. If $q = 4p+1$ is prime, then $\phi(q) = 4p$. Therefore, 2 has order 1, 2, p, $2p$, or $4p$, modulo q. By Euler's Criterion, we have that

$$2^{2p} \equiv 2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \mod q$$

However, p is odd, so $4p \equiv 4 \mod 8$, so $q \equiv 5 \mod 8$. From Theorem 11.6, 2 is a quadratic non-residue of primes congruent to 5 modulo 8. Therefore, we have that

$$2^{2p} \equiv -1 \mod q$$

Thus, the order of 2 can not be any of the divisors of $2p$. Therefore, the order of 2 is not 1, 2, p, or $2p$. Also, 2 does not have order 4 either since $2^4 \equiv 1 \mod q$ implies that $q \mid 15$, which is impossible. Thus, 2 has order $4p$ and is therefore a primitive root of $4p+1$. □

Other Extensions:

- Could you could multiple congruences simultaneously (Similar to the Chinese Remainder Theorem)?
- What about other residues (Cubic, Quartic)?

Theorem

If $p \equiv 2 \mod 3$, then all $x^3 \equiv a \mod p$ have solutions.

Proof. From Fermat's Little Theorem, we have that

$$x^p \equiv x \mod p \quad \Leftrightarrow \quad x^{p-1} \equiv 1 \mod p$$

Multiplying these gives

$$x^{2p-1} \equiv x \mod p$$

Since $p \equiv 2 \mod 3$, let $p = 3q+2$

$$x \equiv x^{2p-1} \equiv x^{2(3q+2)-1} \equiv x^{6q+3} \equiv \left(x^{2q+1}\right)^3 \mod p$$

Therefore, x is a cubic residue. □

What about for $p \equiv 1 \mod 3$? We would split it into 3 cosets (similar to how we split residues into 2 cosets for quadratics)