In this lecture we shall prove the Law of Quadratic Reciprocity. We follow the treatment given in Hardy and Wright.

Let \( p \) and \( q \) be distinct odd primes, and let \( p_1 = \frac{1}{2}(p - 1) \) and \( q_1 = \frac{1}{2}(q - 1) \). Define

\[
S(q, p) = \sum_{i=1}^{p_1} \left[ \frac{iq}{p} \right]
\]

(1)

Note that \( \left[ \frac{iq}{p} \right] \) (the integer part of \( iq/p \)) can also be described as the quotient on division of \( iq \) by \( p \); thus, denoting the remainder by \( R_i \), we have \( 0 < R_i < p \) (since \( p \nmid iq \)) and

\[
iq = p \left[ \frac{iq}{p} \right] + R_i \quad \text{(for all } i \text{ from 1 to } p_1)\]

(2)

Using the terminology introduced in the discussion of Gauss's Lemma (in Lecture 21), the minimal residue of \( iq \) modulo \( p \) is the number congruent to \( iq \) (mod \( p \)) with smallest possible absolute value. If \( 0 < R_i < (p/2) \) then \( R_i \) is the minimal residue, but if \( (p/2) < R_i < p \) then the minimal residue is \( R_i - p \) (which lies between \(-p/2\) and 0). In this latter case the minimal residue is negative, and its absolute value is \( p - R_i \); in the former case the minimal residue is positive and its absolute value is \( R_i \). We proved last time that the absolute values of the minimal residues of \( q, 2q, \ldots, p_1q \) are \( 1, 2, \ldots, p_1 \) in some order, and so it follows that

\[
\sum_{R_i < \frac{p}{2}} R_i + \sum_{R_i > \frac{p}{2}} (p - R_i) = 1 + 2 + \cdots + p_1.
\]

(3)

If \( w \) denotes the number of terms in the second sum on the left hand side, then \( w \) is also the number of values of \( i \) for which the minimal residue is negative, and so by Gauss’s Lemma, \( \left( \frac{q}{p} \right) = (-1)^w \). Our immediate aim is to prove that \( \left( \frac{q}{p} \right) = (-1)^{S(q,p)} \) (with \( S(q,p) \) as defined in Eq. (1) above). Thus we must show that \( S(q,p) \equiv w \) (mod 2).

Writing \( N = 1 + 2 + \cdots + p_1 \), Eq. (3) gives

\[
\left( \sum_{R_i < \frac{p}{2}} R_i \right) - \left( \sum_{R_i > \frac{p}{2}} R_i \right) + wp = N.
\]

(4)

But \(-1 \equiv +1 \) (mod 2), and \( p \equiv 1 \) (mod 2); so reading Eq. (4) mod 2 gives

\[
\left( \sum_{R_i < \frac{p}{2}} R_i \right) + \left( \sum_{R_i > \frac{p}{2}} R_i \right) + w \equiv N \quad \text{(mod 2)}.
\]
The two sums on the left combine to give all the values of \( i \); so

\[
\left( \sum_{i=1}^{p_1} R_i \right) + w \equiv N \pmod{2}.
\] (5)

On the other hand, summing Eq. (2) from \( i = 1 \) to \( p_1 \) gives

\[
q + 2q + \cdots + p_1q = \left( \sum_{i=1}^{p_1} p \left\lfloor \frac{iq}{p} \right\rfloor \right) + \left( \sum_{i=1}^{p_1} R_i \right),
\]

or, equivalently,

\[
qN = pS(q, p) + \sum_{i=1}^{p_1} R_i,
\] (6)

since \( \sum_{i=1}^{p_1} p[iq/p] = p \sum_{i=1}^{p_1} [iq/p] = pS(q, p) \) by Eq. (1). Now reading Eq. (6) mod 2, using the fact that \( q \equiv p \equiv 1 \pmod{2} \), gives

\[
N \equiv S(q, p) + \sum_{i=1}^{p_1} R_i \pmod{2}.
\]

Combining this with (5) above we deduce that

\[
S(q, p) \equiv N - \sum_{i=1}^{p_1} R_i \equiv w \pmod{2},
\]

and hence \((-1)^{S(q,p)} = (-1)^w = \left( \frac{q}{p} \right) \), as required.

We now complete the proof of the Law of Quadratic Reciprocity by proving the following result.

**Proposition:** With the notation as above, \( S(q, p) + S(p, q) = p_1q_1 \).

The proof proceeds by counting in two different ways the number of points \((i, j)\) in the \(xy\)-plane such that the coordinates \(i\) and \(j\) are integers satisfying \(0 < i < (p/2)\) and \(0 < j < (q/2)\). The first way is trivial: there are obviously \(p_1q_1\) such points, since the number of possible values for \(i\) is \(p_1 = \lfloor p/2 \rfloor\) and the number of possible values for \(j\) is \(q_1 = \lfloor q/2 \rfloor\).

Now we count these points according to whether they lie above or below the line with equation \(y = (q/p)x\). (Note that none of the points lie on this line, since \( j = (q/p)i \) with \( i, j \in \mathbb{Z} \) would imply that \( p|i \), which is impossible for \(0 < i < (p/2)\).) For a fixed integer \(i\) in the range \(0 < i < (p/2)\), the point \((i, j)\) lies below the line \(y = (q/p)x\) if and only if \(j < (q/p)i\). So the number of points satisfying our requirements (for this fixed \(i\)) is the number of integers \(j\) in the
range \(0 < j < (iq/p)\). This equals \([iq/p]\), and as \(i\) varies the total number of points obtained is \(\sum_{i=1}^{p_1} [iq/p] = S(q, p)\).

Writing the equation of the line as \(x = (p/q)y\) we see that, for a fixed value of \(j\), the point \((i, j)\) lies above the line if \(0 < i < (p/q)j\). This gives \([jp/q]\) points, and as \(j\) runs from 1 to \(q_1\), the total number of points obtained is \(\sum_{j=1}^{q_1} [jp/q] = S(p, q)\). Hence \(S(q, p) + S(p, q) = p_1q_1\), as required.

Since \(\left(\frac{q}{p}\right) = (-1)^{S(q,p)}\) and (symmetrically) \(\left(\frac{p}{q}\right) = (-1)^{S(p,q)}\), it follows from the Proposition that

\[
\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{p_1q_1} = \begin{cases} -1 & \text{if both } p_1 \text{ and } q_1 \text{ are odd,} \\ +1 & \text{otherwise.} \end{cases}
\]

Since \(p_1\) is odd if \(p \equiv 3 \pmod{4}\) and even if \(p \equiv 1 \pmod{4}\), and similarly \(q_1\) is odd or even as \(q \equiv 3 \pmod{4}\) or \(q \equiv 1 \pmod{4}\), we conclude that \(\left(\frac{q}{p}\right) = -(\frac{p}{q})\) if \(p\) and \(q\) are both congruent to 3 (mod 4), and \(\left(\frac{q}{p}\right) = (\frac{p}{q})\) if either \(p\) or \(q\) is congruent to 1 (mod 4). This is the Law of Quadratic Reciprocity.

**Lecture 23**

As an example of the use of the Law of Quadratic Reciprocity, let us see how to determine whether or not 407 is a square modulo 113. (The number 113 is prime.) The first step is to reduce 407 mod 113: we find that 407 = 3 × 113 + 68. So

\[
\left(\frac{68}{113}\right) = \left(\frac{2^2 \times 17}{113}\right) = \left(\frac{2}{113}\right)^2 \left(\frac{17}{113}\right) = \left(\frac{17}{113}\right)
\]

since \(\left(\frac{2}{113}\right) = \pm 1\). Now 17 ≡ 1 (mod 4); so without even worrying about the mod 4 congruence class of 113 we can say that \(\left(\frac{17}{113}\right) = \left(\frac{113}{17}\right)\). Now 113 ≡ 11 (mod 17); so

\[
\left(\frac{407}{113}\right) = \left(\frac{113}{11}\right) = \left(\frac{11}{11}\right) = \left(\frac{17}{11}\right)
\]

by another application of quadratic reciprocity. Now 17 ≡ 6 (mod 11); so

\[
\left(\frac{407}{113}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2 \times 3}{11}\right) = \left(\frac{2}{11}\right) \left(\frac{3}{11}\right) = \left(\frac{2}{11}\right) \left(\frac{3}{11}\right).
\]

Now \(\left(\frac{2}{11}\right) = -1\) since 11 ≡ 3 (mod 4), and \(\left(\frac{3}{11}\right) = -(\frac{11}{3})\) since 11 and 3 are both congruent to 3 (mod 4). Thus

\[
\left(\frac{407}{113}\right) = \left(\frac{2}{11}\right) \left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1.
\]

So 407 is a non-square modulo 113.
A real (or complex) valued function \( f \) defined on the positive integers is said to be “multiplicative” if \( f(ab) = f(a)f(b) \) whenever \( \gcd(a, b) = 1 \). We have already observed that the Euler phi function \( \varphi \) has this property. Another example is the function \( f \) defined by the rule that \( f(n) \) is the number of positive divisors of \( n \). For example, the number 4 has three positive divisors, namely 1, 2 and 4. So \( f(4) = 3 \).

Similarly, there are two positive divisors of 3, namely 1 and 3; so \( f(3) = 2 \). Since \( \gcd(4, 3) = 1 \) it is easy to see that every positive divisor of 12 = 4 \times 3 is uniquely expressible in the form \( xy \) with \( x \) a positive divisor of 4 and \( y \) a positive divisor of 3. So \( f(12) = f(4)f(3) = 6 \), as is readily checked.

Similarly, let \( \sigma : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \) be the function defined by the rule that \( \sigma(n) \) is the sum of the positive divisors of \( n \). If \( \gcd(a, b) = 1 \) then \( d = xy \) establishes a one to one correspondence between positive integers \( d \) such that \( d|ab \) and pairs \((x, y)\) of positive integers \( x|a \) and \( y|b \); hence

\[
\sigma(ab) = \sum_{d|ab} d = \sum_{x|a} \sum_{y|b} xy = \left( \sum_{x|a} x \right) \left( \sum_{y|b} y \right) = \sigma(a)\sigma(b).
\]

Thus \( \sigma \) is multiplicative.

A positive integer \( n \) is said to be “perfect” if it is the sum of its proper positive divisors (the positive divisors other than \( n \) itself). For example, 28 is perfect, since \( 1 + 2 + 4 + 7 + 14 = 28 \). In terms of the function \( \sigma \) defined above, \( n \) is perfect if \( \sigma(n) = 2n \). It is known that an even number \( n \) is perfect if and only if there exists a prime \( p \) such that \( 2^p - 1 \) is also prime, and \( n = 2^{p-1}(2^p - 1) \). (We shall prove this below.) It is not known if there are any odd perfect numbers.

Numbers of the form \( 2^p - 1 \), where \( p \) is prime, are called “Mersenne numbers”. Since \( 2^{ab} - 1 = (2^a - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \) it is clear that \( 2^K - 1 \) cannot be prime unless \( K \) is prime. For example, since \( 3|15 \) and \( 5|15 \) it follows that \( 2^3 - 1 | 2^{15} - 1 \) and \( 2^5 - 1 | 2^{15} - 1 \). However, a little experimentation suggests that there is a tendency for \( 2^p - 1 \) to be prime when \( p \) is. Thus, \( 2^2 - 1 = 3 \) is prime, \( 2^3 - 1 = 7 \) is prime, \( 2^5 - 1 = 31 \) is prime, and \( 2^7 - 1 = 127 \) is prime. In general, suppose that \( p \) is prime and that \( r \) is a prime divisor of \( 2^p - 1 \). Then \( 2^p \equiv 1 \pmod{r} \), and so \( \text{ord}_r(2) | p \). Since the only divisors of \( p \) are \( p \) and \( 1 \), and since \( \text{ord}_r(2) \) is certainly not \( 1 \), it follows that \( \text{ord}_r(2) = p \). However, the Euler-Fermat Theorem tells us that \( \text{ord}_r(2) | r - 1 \). So \( r - 1 \) is a multiple of \( p \). Thus we have shown that all prime factors of \( 2^p - 1 \) must be congruent to 1 modulo \( p \).

Thus, for example, the prime factors of \( 2^{11} - 1 = 2047 \) must be congruent to 1 modulo 11. The first few numbers congruent to 1 modulo 11 are 1, 12, 23, 34, 45, 56, 67, 78, 89, \ldots\ For each prime \( r \) in this list we can easily check whether or not it is a factor of 2047; we immediately find that 2047 = 23 \times 89. So it is certainly not true that all Mersenne numbers are prime; however, testing primality of a Mersenne number involves significantly less computation than testing primality of an arbitrary number of a similar size. The largest prime known is in fact a Mersenne number.
Here is the proof that all even perfect numbers have the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime. Suppose that $n$ is an even perfect number, and write $n = 2^k m$, where $m$ is odd. Since $n$ is perfect,

$$2^{k+1} m = 2n = \sigma(n) = \sigma(2^k m) = \sigma(2^k) \sigma(m) = (2^{k+1} - 1) \sigma(m)$$

where we have used the multiplicative property of $\sigma$ and the trivial fact that $\sigma(2^k) = 1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$ (proved by summing this geometric series). So $\sigma(m)/m = 2^{k+1}/(2^{k+1} - 1)$, and since the fraction on the right hand side is clearly in its lowest terms, it follows that $m = (2^{k+1} - 1)r$ and $\sigma(m) = 2^{k+1}r$ for some positive integer $r$. Now $m$ has at least the divisors $r$ and $(2^{k+1} - 1)r$, the sum of which is $2^{k+1}r$. Since this is already equal to $\sigma(m)$ it follows that $m$ has no further divisors. Thus $r = 1$ (or else 1 would be another divisor) and $2^{k+1} - 1$ is prime (or else it would contribute further divisors of $m$). (In fact a number that has only two divisors in total has to be prime.) So $m$ is a Mersenne prime, as claimed.