Week 11 Summary

Lecture 20

Let \( p \) be an odd prime, and define (as in Lecture 19)

\[
S_p = \{ t \in \mathbb{Z}_p^* \mid t \text{ has a square root in } \mathbb{Z}_p \},
\]

\[
N_p = \{ t \in \mathbb{Z}_p^* \mid t \text{ does not have a square root in } \mathbb{Z}_p \}.
\]

**Proposition:** \( S_p \) and \( N_p \) both have exactly \((p - 1)/2\) elements.

Indeed, since \( x^2 \equiv y^2 \pmod{p} \) if and only if \( x \equiv \pm y \pmod{p} \), it follows that \( 1^2, 2^2, \ldots, ((p - 1)/2)^2 \) are all distinct modulo \( p \); furthermore, since each nonzero element of \( \mathbb{Z}_p \) can be written in the form \( \pm j \) with \( j \in \{1, 2, \ldots, (p - 1)/2\} \) it is clear that these are all the nonzero squares in \( \mathbb{Z}_p \). So \( S_p \) has exactly \((p - 1)/2\) elements, and as there are \((p - 1)/2\) remaining nonzero elements of \( \mathbb{Z}_p \) it follows that \( N_p \) also has \((p - 1)/2\) elements.

We have shown that primitive roots exist for all primes; so let \( t \) be a primitive root modulo \( p \). Then \( t, t^2, \ldots, t^{p-1} \) are all the elements of \( \mathbb{Z}_p^* \). Of these, the ones with even exponent are obviously squares (since \( t^2j = (t^j)^2 \)); so \( t^2, t^4, \ldots, t^{p-1} \in S_p \).

(Note that \( p - 1 \) is even.) This gives \((p - 1)/2\) elements of \( S_p \); so it is all the elements of \( S_p \). The powers of \( t \) with odd exponent, namely \( t, t^3, \ldots, t^{p-2} \), are thus the elements of \( N_p \). (Note that the rule that \( t^j \) is in \( S_p \) if \( j \) is even and \( N_p \) if \( j \) is odd applies also for \( j \) outside the range \( 1 \leq j \leq p - 1 \), since \( t^i = t^j \) if and only if \( i \equiv j \pmod{p - 1} \), and \( i \equiv j \pmod{p - 1} \) implies \( i \equiv j \pmod{2} \) since \( p - 1 \) is even.)

**Proposition:**

1. If \( x, y \in S_p \) then \( xy \in S_p \).
2. If \( x, y \in N_p \) then \( xy \in S_p \).
3. If \( x \in S_p \) and \( y \in N_p \) then \( xy \in N_p \).

This is clear, since \( t^iT^j = t^{i+j} \), and \( i + j \) is even if \( i, j \) are both even or both odd, and odd if \( i \) is even and \( j \) is odd.

For each integer \( a \) and odd prime \( p \) we define the Legendre symbol \((\frac{a}{p})\) as follows:

\[
(\frac{a}{p}) = \begin{cases} 
1 & \text{if } a \text{ is a nonzero square modulo } p, \\
-1 & \text{if } a \text{ is a nonzero non-square modulo } p, \\
0 & \text{if } a \text{ is zero modulo } p.
\end{cases}
\]

Observe the following properties.

(i) \((\frac{a}{p}) = (\frac{b}{p})\) if \( a \equiv b \pmod{p} \).

(ii) \((\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})\) for all \( a, b \in \mathbb{Z} \).

The first of these is immediate from the definition, and the second is little more than a restatement of the previous proposition.
*Proposition: \( \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p} \). 

This is clear if \( p \mid a \), both sides being zero modulo \( p \). For the case \( p \nmid a \), recall that if \( t \) is a primitive root modulo \( p \) then \( t^{(p-1)/2} \equiv -1 \pmod{p} \); so if \( a \) is an odd power of \( t \) then \( a^{(p-1)/2} \) is an odd power of \(-1 \pmod{p} \), and if \( a \) is an even power of \( t \) then \( a^{(p-1)/2} \) is an even power of \(-1 \).

In the case \( a = -1 \) the proposition tells us that \(-1 \) is a square modulo \( p \) if \( (p-1)/2 \) is even and a non-square modulo \( p \) if \( p \) is odd. That is, \(-1 \) is a square if \( p \equiv 1 \pmod{4} \) and a non-square if \( p \equiv 3 \pmod{4} \). We had already proved this in Lecture 14.

We shall derive two more rules which, when combined with the ones we have already, will make it easy to calculate \( \left( \frac{a}{p} \right) \) in all cases. The first of these is as follows:

\[
\left( \frac{2}{p} \right) = 1 \quad \text{if and only if} \quad p \equiv \pm 1 \pmod{8}.
\]

Thus \( \left( \frac{2}{17} \right) = 1 \) and \( \left( \frac{2}{31} \right) = 1 \), but \( \left( \frac{2}{13} \right) = -1 \) and \( \left( \frac{2}{19} \right) = -1 \). The other key fact is the famous Law of Quadratic Reciprocity: if \( p \) and \( q \) are odd primes, then

\[
\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \quad \text{if} \quad p \equiv 1 \pmod{4} \quad \text{or} \quad q \equiv 1 \pmod{4} \quad \text{(or both)},
\]

\[
\left( \frac{p}{q} \right) = -\left( \frac{q}{p} \right) \quad \text{if} \quad p \equiv q \equiv 3 \pmod{4}.
\]

As an example, we show how to use our rules to determine whether or not 38 is a square modulo 197. The first step in the calculation of \( \left( \frac{n}{p} \right) \) is always to factorize \( n \) and apply \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \) to reduce the problem to calculation of \( \left( \frac{q}{p} \right) \) for prime values of \( q \). Then either apply the formula for \( \left( \frac{2}{p} \right) \) or use quadratic reciprocity to reduce the problem to an equivalent problem with smaller numbers. Thus

\[
\left( \frac{38}{197} \right) = \left( \frac{2}{197} \right) \left( \frac{19}{197} \right) = - \left( \frac{19}{197} \right)
\]

since \( 197 \equiv 3 \pmod{8} \) gives \( \left( \frac{2}{197} \right) = -1 \). Since \( 197 \equiv 1 \pmod{4} \), quadratic reciprocity gives \( \left( \frac{19}{197} \right) = \left( \frac{197}{19} \right) = \left( \frac{7}{19} \right) \) (since \( 197 \equiv 7 \pmod{19} \)). Continuing in this way we find that

\[
\left( \frac{38}{197} \right) = - \left( \frac{7}{19} \right) = \left( \frac{19}{7} \right) = \left( \frac{5}{7} \right) = \left( \frac{2}{5} \right) = -1
\]

(where we used first \( 19 \equiv 7 \equiv 3 \pmod{4} \), then \( 19 \equiv 5 \pmod{7} \), then \( 5 \equiv 1 \pmod{4} \), then \( 7 \equiv 2 \pmod{5} \), and finally \( 5 \equiv -3 \pmod{8} \)). Thus 38 is not a square modulo 197.
Lecture 21

Let \( p \) be an odd prime, and write \( p_1 = (p-1)/2 \). For each integer \( a \) there exists an integer \( b \) in the range \( -p_1 \leq b \leq p_1 \) such that \( b \equiv a \pmod{p} \). We call \( b \) the minimal residue of \( a \).

Fix \( a \in \mathbb{Z} \) such that \( p \nmid a \), and consider the numbers \( a, 2a, \ldots, p_1a \). For each \( i \) from 1 to \( p_1 \), let \( b_i \) be the minimal residue of \( ia \). Then \( |b_i| \in \{1, 2, \ldots, p_1\} \) for each \( i \).

*Proposition:* The numbers \(|b_1|, |b_2|, \ldots, |b_{p_1}|\) are the numbers 1, 2, \ldots, \( p_1 \) in some order.

To prove this it suffices to show that \(|b_i| \neq |b_j|\) for \( i \neq j \). But if \(|b_i| = |b_j|\) then \( ia \equiv b_i = \pm b_j \equiv \pm ja \pmod{p} \), giving \( i \equiv \pm j \pmod{p} \). Since \( i, j \in \{1, 2, \ldots, p_1\} \), this implies that \( i = j \).

We are now able to derive a key result, discovered by Gauss.

*Gauss’s Lemma:* With the notation as above, let \( w \) be the number of \( b_i \) that are negative. Then \( \left( \frac{a}{p} \right) = (-1)^w \).

Indeed, \( \prod_{i=1}^{p_1} b_i = (-1)^w \prod_{i=1}^{p_1} |b_i| \), which by the preceding proposition equals \( (-1)^w p_1! \). Modulo \( p \) we have \( \prod_{i=1}^{p_1} b_i \equiv \prod_{i=1}^{p_1} ia = a^{p_1} p_1! \), and so cancelling \( p_1! \) gives \( (-1)^w \equiv a^{p_1} \pmod{p} \). But \( a^{p_1} \equiv \left( \frac{a}{p} \right)_p \), as was shown in Lecture 20.

Gauss’s Lemma makes it easy to evaluate \( \left( \frac{2}{p} \right) \): we simply need to determine how many of the numbers 2, 4, \ldots, \( 2p_1 \) have negative minimal residues. Now if \( 1 \leq i < p/4 \) then \( 2 \leq 2i < p/2 \), and so \( 2i \) is its own minimal residue. On the other hand, for \( p/4 < i \leq p_1 \) we have \( p/2 < 2i \leq p-1 \), and for each of these values of \( 2i \) the minimal residue is \( 2i - p \), and is negative. So the number of negative minimal residues is the number of integers \( i \) in the range \( p/4 < i \leq p_1 \), which is \( p_1 - [p/4] \). If \( p \) has the form \( 8k + 1 \) then \( p_1 = 4k \) and \( [p/4] = [2k + (1/4)] = 2k \), and so \( p_1 = [p/4] = 2k \), which is even. Similarly, if \( p = 8k - 1 \) then \( p_1 - [p/4] = (4k - 1) - (2k - 1) \), which is even, while if \( p = 8k \pm 3 \) then similar calculations show that \( p_1 - [p/4] \) is odd.

In fact, for any specified value of \( a \) we can use this same method to find out which primes \( p \) give \( \left( \frac{a}{p} \right) = 1 \) and which give \( \left( \frac{a}{p} \right) = -1 \). For example, consider the case \( a = -3 \). If \( 1 \leq i < p/6 \) then \( -3 \geq -3i > -p/2 \), the minimal residue of \(-3i\) is \(-3i\) itself, and is negative. This gives \( [p/6] \) negative minimal residues. For \( p/6 < i < p/3 \) we have \(-p/2 > -3i > -p\), and the minimal residue of \(-3i\) is \( p - 3i \), which is positive. Finally, for \( p/3 < i < p/2 \) we have \(-p > -3i > -3p/2\), again the minimal residue is \( p - 3i \), which is negative for these values of \( i \). This gives a further \([p/2] - [p/3] \) negative minimal residues. If \( p = 6k + 1 \) then the number of negative minimal residues is \( [p/6] + [p/2] - [p/3] = k + 3k - 2k \), which is even, and so \( \left( \frac{a}{p} \right) = 1 \). If \( p = 6k - 1 \) then \( [p/6] + [p/2] - [p/3] = (k - 1) + (3k - 1) - (2k - 1) \) is odd, and so \( \left( \frac{a}{p} \right) = -1 \).

We conclude that \(-3\) is a square modulo any prime that is congruent to 1 modulo 6, and a non-square modulo any prime congruent to \(-1\) modulo 6.

\[ \text{–3–} \]