Handout for Section 9.3 (II)

1. Read the discussion on page 188 and Example 9.5 (simplified).

2. I gave a different presentation of the proof of QRL than is in the book. But you should be able to read and understand the proof given in the book by making a composite out of the proof of Theorem 9.9 and the proof of the lemma on page 183.

3. In general, to find \((a/p)\), look at the prime factorization of \(a\), \(a = \pm \prod p_i^{k_i}\).

So, \((a/p) = (\pm 1/p) (2/p)^{k_2} (3/p)^{k_3} \cdots (p_i/p)^{k_i}\)

by multiplicativity of Legendre symbol.

So we only need to know \((1/p) (\text{prime})\), \((-1/p) (\text{prime})\), \((2/p) (\text{prime})\), \((3/p) (\text{prime})\), \((p_i/p)\)

Apply QRL to replace this with \(\pm (p/p_i)\), this has smaller denominator \(a\) can be replaced by \(\pm (p'/p_i)\), where \(p \equiv p' \pmod{p_i}\), \(\forall \text{ etc.}\).

Let's do another example to see this process—

4. Does \(x^2 \equiv 19 \pmod{283}\) have solutions?

\((19/283) = (283/19) (-1)^{283-19} = -(283/19)\)

\((19 \equiv 17 \pmod{19})\), \(- (17/19) = -(19/17) (-1)^{17-19} = -(19/17)\)

\((19 \equiv 2 \pmod{17})\), \(- (2/17) = -(1) = -1\)

So no solutions.

5. A formula for \((3/p)\): —
Theorem: \( \frac{3}{p} = \begin{cases} 
+1 & \text{if } p \equiv \pm 1 \pmod{12} \\
-1 & \text{if } p \equiv \pm 5 \pmod{12}
\end{cases} \)

Proof: By QR, \( \frac{3}{p} = \begin{cases} 
\sqrt{p/3} & \text{if } p \equiv 1 \pmod{4} \\
-(p/3) & \text{if } p \equiv 3 \pmod{4}
\end{cases} \)

Since \( 3 \equiv 3 \pmod{4} \),

Now, \( p \equiv 1 \pmod{2} \) or \( 3 \).

By previous theorem, for \( \frac{2}{p} \) and \( \frac{1}{p} \),

\[ \frac{p/3} = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{3} \\
-1 & \text{if } p \equiv 2 \pmod{3}
\end{cases} \]

Thus, \( \frac{3}{p} \equiv 1 \) if

\[ p \equiv 1 \pmod{4} \text{ and } p \equiv 1 \pmod{3} \]

i.e., \( p \equiv 1 \pmod{12} \)

or \( p \equiv 3 \pmod{4} \) and \( p \equiv \bar{2} \pmod{3} \)

i.e., \( p \equiv 11 \pmod{12} \) (by CRT)

\[ \Box \]

6. Read example 9.6 on page 189

- Make sure you understand it!

Note the use of CRT.

7. Solve problem #14 on page 191

\( x \equiv 9, 16, 19, 26 \pmod{35} \) are the solutions.

8. When you have time later, read and attempt problems #16, 17, 18, 19 on page 192.