# Handout for Section 9.3 (II)

① Read the discussion on page 188 and Example 9.5

② I gave a different (simplified) presentation of the proof of QRL than is that given in the book. But you should be able 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 $a$, $a = \pm 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$

so, $(a/p) = (\pm 1/p)(2/p)^{k_0}(p_1/p)^{k_1} \cdots (p_r/p)^{k_r}$

by multiplicativity of Legendre symbol.

So, we only need to know $(1/p)$ (known), $(-1/p)$ (known), $(2/p)$ (known), $\underbrace{(p_i/p)}$

apply QRL to replace this with $\pm(p/p_i)$, this has smaller denominator & can be replaced by $\pm(p'/p_i)$ where $p \equiv p' \pmod{p_i}$, & so on.

Let's do another example to see this process —

④ Does $x^2 \equiv 19 \pmod{283}$ have solutions?

$$(19/283) = (283/19)(-1)^{\frac{18}{2}\frac{282}{2}} = -(283/19)$$

$(\because 283 \equiv 17 \pmod{19})$, $= -(17/19) = -(19/17)(-1)^{\frac{16}{2}\frac{18}{2}} = -(19/17)$

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

$\therefore$ no solns.

⑤ A formula for $(3/p)$ :—

**Thm** $(3/p) = \begin{cases} +1, & \text{if } p \equiv \pm 1 \pmod{12} \\ -1, & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$

**Pf.** By QRL, since $3 \equiv 3 \pmod 4$, $(3/p) = \begin{cases} (p/3), & \text{if } p \equiv 1 \pmod 4 \\ -(p/3), & \text{if } p \equiv 3 \pmod 4 \end{cases}$

Now, $p \equiv 1$ or $2 \pmod 3$,
By previous theorems for $(2/p)$ & $(1/p)$,

$$(p/3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

Thus, $(3/p) \equiv 1$ iff $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$
i.e., $p \equiv 1 \pmod{12}$
or $p = 3 \pmod 4$ and $p \equiv 2 \pmod 3$
i.e., $p \equiv 11 \pmod{12}$ (by CRT)

(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, (maybe after the semester) read and attempt problems #16, 17, 18, 19 on page 192.