1 Exercises

1.1

Check that the theorem gives the right result in this case by applying Euler's Criterion and showing that $5^8 \equiv -1 \pmod{17}$.

$$\begin{aligned} 5 &\equiv 5 \pmod{17} \\ 5^2 &\equiv 8 \pmod{17} \\ 5^4 &\equiv 13 \pmod{17} \\ 5^8 &\equiv 16 \equiv -1 \pmod{17} \end{aligned}$$

1.2

Apply the theorem to determine whether $x^2 \equiv 7 \pmod{23}$.

$(23-1)/2 = 11$, so have to consider $7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77$, which $\pmod{23}$ are $7, 14, 21, 5, 12, 19, 3, 10, 17, 1$ 5 of these residues are greater than 11, and as 5 is odd, the congruence has no solutions.

1.3

Check the cases $p \equiv 5 \pmod 8$ and $p \equiv 7 \pmod 8$.

For $p \equiv 5$, $p = 8k+5$, so $(p+3)/4 = 2k+2$, and the largest integer smaller than this is $2k+1$, so $(2/p) = -1$. For $p \equiv 7$, $p = 8k+5$, so $(p+3)/4 = 2k+5$, and the largest integer smaller than this is $2k+4$, so $(2/p) = 1$.

1.4

Verify that the lemma is true for $p = 5$ and $q = 7$.

$$\sum_{k=1}^{(5-1)/2} \left[\frac{7k}{5}\right] + \sum_{k=1}^{(7-1)/2} \left[\frac{5k}{7}\right] =$$
$$\left[\frac{7}{5}\right] + \left[\frac{14}{5}\right] + \left[\frac{5}{7}\right] + \left[\frac{10}{7}\right] + \left[\frac{15}{7}\right] =$$
$$1+2+0+1+2 = 6$$
$$\frac{p-1}{2} \cdot \frac{q-1}{2} = 2 \cdot 3 = 6$$

2 Problems

2.1

Adapt the method used in the text to evaluate $(2/p)$ to evaluate $(3/p)$.

Need to figure out how many residues $\pmod p$ of $3, 6, 9, ..., 3(\frac{p-1}{2})$ are greater than $\frac{p-1}{2}$. Consider the last term, $3(\frac{p-1}{2})$. This term will be greater than p for $p > 3$, so will have to subtract some multiple of p to obtain its least residue. We can ignore $p \leq 3$ as it is trivial to calculate $(3/2) = (1/2) = 1$ and $(3/3) = (0/3) = 1$. As it turns out, $\frac{3}{2}(p-1) - p = \frac{p-3}{2}$, which is smaller than p. So one can obtain the least residues of integers in the sequence that are $\geq p$ by subtracting p from them. Furthermore, the least residues for these integers are $< \frac{p-1}{2}$. So, have to figure out how many integers in the sequence $3, 6, ..., 3(\frac{p-1}{2})$ fall between $\frac{p-1}{2}$ and p. If $3a$ is the smallest integer $\ni 3k > \frac{p-1}{2}$, then $k > \frac{p-1}{6}$. If $3k$ is the largest integer $\ni 3k < p$, then $k < \frac{p}{3}$, and since $p > 3$ and $3 \nmid p$, we know that this isn't an integer, so can consider $k \leq \frac{p-1}{3}$. In other words, we are looking for whether the total number of $k \ni \frac{p-1}{6} < k \leq \frac{p-1}{3}$ is odd or even. First consider $p \equiv 1 \pmod 6$. Then $\frac{p-1}{6} = \frac{6x+1-1}{6} = x$, and $\frac{p-1}{3} = 2x$. The number of $k \ni x < k \leq 2x$ is x, about which we cannot say whether it is even or odd. So, instead consider $p \equiv 1 \pmod{12}$. Then need $k \ni 2x < k \leq 4x$, of which there are $2x$, an even number. For $p \equiv 5 \pmod{12}$, need $k \ni 2x < k \leq 4x+1$, of which there are an odd number. For $p \equiv 7 \pmod{12}$, need $k \ni 2x+1 < k \leq 4x+2$, of which there are an odd number. For $p \equiv 11 \pmod{12}$, need $k \ni 2x+1 < k \leq 4x+3$, of which there are an even number. So $(3/p) = 1$ for $p \equiv 1, 11 \pmod{12}$ and $(3/p) = -1$ for $p \equiv 5, 7 \pmod{12}$.

2.2

Show that 3 is a quadratic nonresidue of all primes of the form $4^n + 1$.

Let $p = 4^n + 1$. Want to show $(3/p) = -1$. Since $p \equiv 1 \pmod 4$, know $(3/p) = (p/3)$. Also know that $4^n = 3 * 4^{n-1} + 4^{n-1}$. Know that for $n = 1$, $4^n \equiv 1 \pmod 3$. Assume this holds for n up to r. Examine $4^{r+1} = 3 * 4^r + 4^r$. Since the property holds up to r, we know $3 * 4^r + 4^r \equiv 1 \pmod 3$. We have proved by induction that $4^n + 1 \equiv 2 \pmod 3$. So $(p/3) = (2/3)$, and since $3 \equiv 3 \pmod 8$, $(p/3) = (2/3) = -1$. Combining with $(3/p) = (p/3)$, have $(3/p) = -1$ and 3 a nonresidue of p.

2.3

Show that 3 is a quadratic nonresidue of all Mersenne primes greater than 3.

A Mersenne prime can be written $p = 2^n - 1$. Know from the previous exercise that $4^n \equiv 1 \pmod 3$, which means that for even n, $2^n \equiv 1 \pmod 3$. Odd n can be written $2k+1$, so $2^n = 2 * 4^k \equiv 2 * 1 \equiv 2 \pmod 3$. Regardless of whether $2^n - 1 \equiv 0$ or 1, $(p/3) = 1$. Also observe that $p \equiv 3 \pmod 4$, and obviously $3 \equiv 3 \pmod 4$, so $(3/p) = -(p/3) = -1$.

2.4

(a) Prove that if $p \equiv 7 \pmod 8$, then $p | (2^{(p-1)/2} - 1)$.
(b) Find a factor of $2^{83} - 1$.

(a) By Euler's criterion, $(2/p) \equiv 2^{(p-1)/2} \pmod p$. Also know that if $p \equiv 7 \pmod 8$, then $(2/p) = 1$. So $(2^{(p-1)/2} - 1) \equiv 0 \pmod p$, or, stated differently, $p | (2^{(p-1)/2} - 1)$.
(b) Notice that $2 * 83 + 1 = 167$ is a prime, and $167 \equiv 7 \pmod 8$, so we can use the result from above to conclude that 167 is such a factor.

2.5

(a) If p and $q = 10p + 3$ are odd primes, show that $(p/q) = (3/p)$.
(b) If p and $q = 10p + 1$ are odd primes, show that $(p/q) = (-1/p)$.

(a) Know that $q \equiv 3 \pmod p$, so $(q/p) = (3/p)$. If $p \equiv 3 \pmod 4$, then $10p + 3 = 40k + 33 \equiv 1 \pmod 4$. So p and q can't both be $\equiv 3 \pmod 4$, thus $(q/p) = (p/q) = (3/p)$.
(b) Know that $(-1/p) = 1$ if $p \equiv 1 \pmod 4$, and $(-1/p) = -1$ if $p \equiv 3 \pmod 4$. Also know that $q \equiv 1 \pmod p$, so $(q/p) = 1$. If $p \equiv 1 \pmod 4$, then $(p/q) = (q/p) = 1 = (-1/p)$. If $p \equiv 3 \pmod 4$, then $10p + 1 \equiv 3 \pmod 4$, and $(p/q) = -(q/p) = -1 = (-1/p)$.

2.6

(a) Which primes can divide $n^2 + 1$ for some n?
(b) Which odd primes can divide $n^2 + n$ for some n?
(c) Which odd primes can divide $n^2 + 2n + 2$ for some n?

(a) $p | n^2 + 1$ can be rewritten $n^2 \equiv -1 \pmod p$. We know -1 is only a quadratic residue when $p \equiv 1 \pmod 4$.
(b) Notice that for $n = p - 1$, $n^2 + n = p^2 - 2p + 1 + p - 1 \equiv 0 \pmod p$. So, every p can divide $n^2 + n$ for $n = p - 1$.
(c) $n^2 + 2n + 2 = (n+1)^2 + 1$. So again have $(n+1)^2 = x^2 \equiv -1 \pmod p$, with -1 a quadratic residue when $p \equiv 1 \pmod 4$.

2.7

(a) Show that if $p \equiv 3 \pmod 4$ and a is a quadratic residue $\pmod p$, then $p - a$ is a quadratic nonresidue $\pmod p$.
(b) What if $p \equiv 1 \pmod 4$?

(a) Know that $(a/p) = 1$, and we're trying to determine $(p - a/p)$. Since $p - a \equiv -a \pmod p$, can rewrite this as $(-a/p) = 2(-1/p)(a/p) = (-1/p)$. Since $p \equiv 3 \pmod 4$, know $(-1/p) = -1$, and thus $p - a$ is a nonresidue.
(b) If $p \equiv 1$, then $(-1/p) = 1$, and $p - a$ is a quadratic residue.

2.8

If $p > 3$, show that p divides the sum of its quadratic residues that are also least residues.

Notice that all quadratic residues of a prime p that are least residues must be $\equiv r^2 \pmod p$ for some $r < p$. Conversely, $r^2 \pmod p$ for all $0 < r < p$ are quadratic residues that are least residues. Furthermore, we know that for a given $r^2 \equiv (-r)^2 \equiv (p-r)^2 \pmod p$, so we can exclude the duplicate $(p - r)^2$, which are those for $r > (p - 1)/2$. In other words, if $a_1, ..., a_k$ are all the quadratic residues that are also least residues, we know that $a_1 + ... + a_k \equiv 1^2 + 2^2 + ... + ((p-1)/2)^2 \pmod p$. There is a formula for the sum of a sequence of squares: $1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$. So, with $n = (p-1)/2$, we know that the sum of squares is equal to $p \cdot \frac{p^2-1}{24}$, and this must be an integer. Since p divides this sum, then p divides the sum of the sequence of squares up to $(p - 1)/2$, and since this is equivalent to the sum of quadratic residues $\pmod p$, p must divide that sum of quadratic residues as well.

2.9

If p is an odd prime, evaluate

$$(1 \cdot 2/p) + (2 \cdot 3/p) + ... + ((p - 2)(p - 1)/p)$$

TODO

2.10

Show that if $p \equiv 1 \pmod 4$, then $x^2 \equiv -1 \pmod p$ has a solution given by the least residue $\pmod p$ of $(\frac{p-1}{2})!$. Since $p \equiv 1 \pmod 4$, can write $p = 4k + 1$ and $(p - 1)/2 = 4k/2 = 2k$ is even. So, $(-1)^{(p-1)/2} = 1$. Expand $((\frac{p-1}{2})!)^2$:

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2} - 1\right) \cdots 1 =$$
$$1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(p - \left(\frac{p-1}{2} + 1\right)\right) \cdots \left(p - \left(\frac{p-1}{2} + \frac{p-1}{2} - 1\right)\right) \equiv$$
$$(-1)^{(p-1)/2} \cdot 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2} + 1\right) \cdots (p - 1) \equiv (p - 1)! \pmod p$$

We know from Wilson's theorem that $(p - 1)! \equiv -1 \pmod p$, so $((p - 1)/2)!$ is a solution of the quadratic congruence.