Group 1.

3.7.2

If p is prime, then $\{-(p-1)/2, \ldots -2, -1, 1, 2, \ldots (p-1)/2\}$ is a reduced residue system mod p.

To prove: (direct): We will establish this by checking the three requirements.

1. There are $\frac{p-1}{2}$ objects from $1, 2 \ldots \frac{p-1}{2}$, and another $\frac{p-1}{2}$ objects from $-\frac{(p-1)}{2} \ldots -2, -1$
So there are a total of $p-1 = \phi(p)$ objects in the system

2. since $(i, p) = 1$ for $i = 1, 2, \ldots p-1$ then
$(i, p) = 1$ for $i = 1, 2 \ldots \frac{p-1}{2}$.
Also, $(-1, p) = 1$
So by an exercise
$(-i, p) = 1$ for $i = 1, 2 \ldots \frac{(p-1)}{2}$

3. since $-1 \equiv p-1 \pmod{p}$, $-2 \equiv (p-2), \ldots$
$-\frac{(p-1)}{2} \equiv \frac{p+1}{2} \pmod{p}$
the list $\{-\left(\frac{p-1}{2}\right), \ldots -2, -1, 1, 2 \ldots \left(\frac{p-1}{2}\right)\}$ is congruent to $\{1, 2 \ldots p-1\}$ which is the canonical rrs.
Then no two members of the original system are congruent mod p.
Thus $\{-\left(\frac{p-1}{2}\right), \ldots -2, -1, 1, 2 \ldots, \frac{(p-1)}{2}\}$ is a reduced residue system.
Proved.

Group 4
Exercise 3.7.3

Fix n to be natural. If a is an integer with $(a,n)=(a-1,n)=1$, then $1+a+a^2+\dots+a^{\phi(n)-1} \equiv 0 \pmod{n}$

<u>Proof (Direct):</u>

Fix n in $\mathbb{N}$ and a in $\mathbb{Z}$ with $(a,n)=(a-1,n)=1$.

So, by Theorom 3.26 (Euler's Thm.), $a^{\phi(n)} \equiv 1 \pmod{n}$.

That, is, $n \mid (a^{\phi(n)}-1)$.

So $n \mid (a-1)(a^{\phi(n)-1}+\dots+a^2+a+1)$. But $n \nmid (a-1)$.

And $n \mid a^{\phi(n)-1}+\dots+a^2+a+1$.

Thus $1+a+a^2+\dots+a^{\phi(n)-1} \equiv 0 \pmod{n}$.

$\blacksquare$

Exercise 3.8.1 Group 3

Let $ax^2+bx+c \equiv 0 \pmod 2$ for a,b,c in $\mathbb{Z}$ and a is odd. For any $ax^2+bx+c \equiv 0 \pmod 2$, it can reduce to $a'x^2+b'x+c' \equiv 0 \pmod 2$. The four possible congruences that $ax^2+bx+c \equiv 0 \pmod 2$ can reduce to are:

① $x^2+x+1 \equiv 0 \pmod 2$

$$\left.\begin{array}{l} 0^2+0+1 \not\equiv 0 \pmod 2 \\ 1^2+1+1 \not\equiv 0 \pmod 2 \end{array}\right\} \text{ no solutions}$$

② $x^2+1 \equiv 0 \pmod 2$

$0^2+1 \not\equiv 0 \pmod 2$

$1^2+1 \equiv 0 \pmod 2 \rightarrow x=1$ is a solution

③ $x^2+x \equiv 0 \pmod 2$

$$\left.\begin{array}{l} 0^2+0 \equiv 0 \pmod 2 \rightarrow x=0 \\ 1^2+1 \equiv 0 \pmod 2 \rightarrow x=1 \end{array}\right\} \text{solutions}$$

④ $x^2 \equiv 0 \pmod 2$

$0^2 \equiv 0 \pmod 2 \rightarrow x=0$ is a solution

$1^2 \not\equiv 0 \pmod 2$

3.8.2

Proof: (direct) Fix d and p so that d is a q. res mod p.

Let $S = \{1, 2, \ldots, p-1\}$ with y and $p-y$ removed

where $y^2 \equiv d \bmod p$.

Fix c in S w/o y, $p-y$.

Consider $cX \equiv d \pmod{p}$.

Since $(c,p) = 1$ this equation has a soln, call it c'.

Note $c' \not\equiv 0 \pmod{p}$ [else $d \equiv 0 \pmod{p}$ and d is a q. r. $\divideontimes$]

Just suppose $c' \equiv y \pmod{p}$

So $cy \equiv d \equiv y^2 \pmod{p}$, and we know $(y,p) = 1$.

We can cancel giving $c \equiv y \pmod{p}$ $\divideontimes$.

So it must be that $c' \not\equiv y \pmod{p}$.

Just suppose $c' \equiv p-y \pmod{p}$.

We know $p-y \equiv -y \pmod{p}$.

So $c(-y) \equiv d \equiv (-y)^2 \pmod{p}$, and $(-y,p) = 1$.

So cancelling we have $c \equiv -y \equiv p-y \pmod{p}$ $\divideontimes$.

Just suppose $c \equiv c' \pmod{p}$.

Then $c^2 \equiv d \equiv y^2 \pmod{p}$.

So $c^2 - y^2 \equiv 0 \pmod{p}$ or $(c+y)(c-y) \equiv 0 \pmod{p}$.

Since p is prime, $p \mid (c+y)$ or $p \mid (c-y)$.

If $p \mid (c+y)$, then $c \equiv -y \equiv p-y \pmod{p}$ $\ast$.

If $p \mid (c-y)$, then $c \equiv y \pmod{p}$ $\ast$.

So it must be that $c \not\equiv c' \pmod{p}$.

Thus for any c in S w/o y, $p-y$, there is a c' in S w/o y, $p-y$ such that $c \not\equiv c' \pmod{p}$ and $c c' \equiv d \pmod{p}$.