Chapter 2

Section 2.3: #13 Follow the hint in the back of the text.

#23 Start by proving that gcd($a, p^k$) ≠ 1 if and only if $p|a$. Then count for how many $a = 1, 2, \ldots, p^k$ this is the case.

Section 2.5: #8 First, use the Euclidean algorithm to show that gcd(144, 233) = 1. This tells you that 144 does have an inverse modulo 233. Next, find integers $x$ and $y$ such that $x \cdot 144 + y \cdot 233 = 1$. (You can do this as shown in Example 1, or use the method presented in class.) Finally, explain why $x$ is the inverse of 144 modulo 233, i.e. why $x \cdot 144 \equiv 1 \mod 233$.

#12 Find an inverse $c$ of 2 mod 17 (i.e. $c \cdot 2 \equiv 1 \mod 17$) like in Problem 8. Then multiply both sides of $2x \equiv 7 \mod 17$ by $c$.

#13 Recall the following fact we proved in class: If $a$ divides $b \cdot c$, then $a/gcd(a, b)$ divides $c$. Use this fact with $a, b, c$ replaced by $m, c,$ and $a - b$, respectively.

#14 (a) $2 \cdot 6 \equiv 3 \cdot 4 \equiv 7 \cdot 8 \equiv 5 \cdot 9 \equiv 1 \mod 11$. (b) Re-group the product $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$ as $(2 \cdot 6) \cdot (3 \cdot 4) \cdot (7 \cdot 8) \cdot (5 \cdot 9) \cdot (1 \cdot 10)$ and notice that $10 \equiv -1 \mod 11$.

#16 (a) By Problem 15, the only two positive integers less than $p$ which are their own inverses mod $p$ are 1 and $p - 1 (\equiv -1) \mod p$. All the others can be paired up with their inverses just like in Problem 14. (b) Proceed as in Problem 14(b).

#22 You need to solve the system

$$x \equiv 0 \mod 5$$
$$x \equiv 1 \mod 3$$

One would usually solve this system with the formula of the Chinese remainder theorem. However, since the numbers are so small one can quickly see that $x = 10$ is a solution. By the Chinese remainder theorem, all solutions are then given by $10 \mod 15$. 
#25  (a) Since by Fermat’s little theorem $5^6 \equiv 1 \mod 7$, then $5^{2003} \equiv 5^{333\cdot 6+5} \equiv 5^5 \equiv 3 \mod 7$. Similarly, $5^{2003} \equiv 4 \mod 11$ and $5^{2003} \equiv 8 \mod 13$. (b) So, you need to solve the congruences

$$
\begin{align*}
  x &\equiv 3 \mod 7 \\
  x &\equiv 4 \mod 11 \\
  x &\equiv 8 \mod 13
\end{align*}
$$

Use the formula of the Chinese remainder theorem as in Example 6. The answer is 983.

#36 The answer is 2299, 1317, 2117. Make sure you use 00 for A, 01 for B, etc. Otherwise you will have a different encrypted message. Show your work!

#40 For a definition of quadratic residue, read the paragraph before Problem #38. Take the list of positive integers less than $p$ and square them all, $\mod p$. By Problem #39, every square in this list appears exactly twice.

#42 First read the definition of the Legendre symbol above Problem #41. You might want to do Problem #39 and #40, to put this symbol into context.

(i) If $a$ is a quadratic residue mod $p$, i.e. if $a \equiv x^2 \mod p$ for some $x \in \mathbb{Z}$, then by Fermat’s little theorem:

$$
a^{\left(\frac{p-1}{2}\right)} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \mod p.
$$

(Note that $p$ does not divide $x$, since $p$ does not divide $a$.)

(ii) If $a$ is not a quadratic residue mod $p$, then $\left(\frac{a}{p}\right) \equiv -1 \mod p$, by the very definition of the Legendre symbol. So, we need to prove that $a^{(p-1)/2} \equiv -1 \mod p$, too. Since $\gcd(i, p) = 1$ for every $i \in \{1, 2, \ldots, p-1\}$, then for every $i \in \{1, 2, \ldots, p-1\}$ there is a (unique) $j \in \{1, 2, \ldots, p-1\}$, with $i \cdot j \equiv a \mod p$. Since we are assuming that $a$ is not a perfect square mod $p$, we always have $i \not\equiv j \mod p$. So, when we multiply all numbers from 1 through $p-1$, always two factors pair up to give an $a$. Hence, $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a^{(p-1)/2} \mod p$. The result follows now from Willson’s Theorem (Problem #16).