Chapter 7

7.2.04 You may use technology to factor n.

7.2.05 You may use technology to factor n.

Chapter 9

9.5.09 The same algorithm works for matrix exponentiation. Initialize $X = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 5 \end{smallmatrix}\right)$, $E = 17$, $Y = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For this problem, perform the computations modulo 1001.

9.6.02 Before using the formula in the theorem, check to make sure the theorem applies: check that 19 is the right kind of prime and that 6 is a square mod 19 (using quadratic reciprocity.) After you use the formula to find the principal square root, check that your answer is actually a square root of 6 mod 19 (by squaring it), and check that your answer is itself a square (using quadratic reciprocity.)

9.6.03 Before using the formula in the theorem, check to make sure the theorem applies: check that 71 is the right kind of prime and that 2 is a square mod 71 (using quadratic reciprocity.) After you use the formula to find the principal square root, check that your answer is actually a square root of 2 mod 71 (by squaring it), and check that your answer is itself a square (using quadratic reciprocity.)

Chapter 10

10.8.10 Verify Euler's Criterion for squares mod p for the case $p = 11$, as follows. (a) Create an input-output table for the squaring function $x \mapsto x^2$ on the units modulo p. You may use technology. For example, entering

```
Table[PowerMod[x, 2, 11], {x, 1, 10}]
```

to WolframAlpha will create an input-output table for the function $x \mapsto x^2$ on the units mod 11. (b) Which units mod p are squares mod p? Which units mod p are non-squares mod p? (c) Create an input-output table for the function $y \mapsto y^{(p-1)/2}$ on the units mod p. (d) Which units satisfy $y^{(p-1)/2} = 1 \bmod p$? Are these the same as the units that are square mod p?

10.8.11 Verify Euler's Criterion for the case $p = 13$, using the procedure outlined in the previous exercise.

10.8.12 Let $n = 9$. (a) Create an input-output table for the squaring function $x \mapsto x^2$ on the units modulo n. (b) Which units mod n are squares mod n? Which units mod n are non-squares mod n? Make sure you only consider *units* mod n. (c) Create an input-output table for the function $y \mapsto y^{(n-1)/2}$ on the units mod n. (d) Which units satisfy $y^{(n-1)/2} = 1 \bmod n$? Are these the same as the units mod n that are square mod n? (e) Explain why this does not contradict Euler's Criterion.

10.8.13 Let $n = 15$. Find the units mod 15 that are squares mod 15, and determine whether computing $y^{(n-1)/2} \bmod n$ predicts the squares and non-squares. (Follow the outline given in the previous problem.)

Chapter 12

12.2.01 (a) Using your work for 10.8.10, make a table of values for $\left(\frac{b}{11}\right)_2$ for $b = 0, 1, \ldots, 14$. (b) Using your work for 10.8.11, make a table of values for $\left(\frac{b}{13}\right)_2$ for $b = 0, 1, 2, \ldots, 16$.

12.3.01 Let $n = 9$. (a) Use WolframAlpha to create an input-output table for the Jacobi symbol $y \mapsto \left(\frac{y}{n}\right)_2$ on the units mod n:

```
Table[JacobiSymbol[y, n], {y, 1, 8}]
```

(b) Which units satisfy $\left(\frac{y}{n}\right)_2 = 1$? Refer back to your work for 10.8.12. Are all of the units satisfying $\left(\frac{y}{n}\right)_2 = 1$ squares mod n? (c) Which units satisfy $\left(\frac{y}{n}\right)_2 = -1$? Are all of these units non-squares mod n?

12.3.02 Let $n = 15$. (a) Use WolframAlpha to create an input-output table for the Jacobi symbol $y \mapsto \left(\frac{y}{n}\right)_2$ on the units mod n. (b) Which units satisfy $\left(\frac{y}{n}\right)_2 = 1$? Refer back to your work for 10.8.13. Are all of the units satisfying $\left(\frac{y}{n}\right)_2 = 1$ squares mod n? (c) Which units satisfy $\left(\frac{y}{n}\right)_2 = -1$? Are all of these units non-squares mod n?

12.3.03 (a) Compute the following Legendre or Jacobi symbols by hand, using the fast expenentiation algorithm, Euler's criterion, and multiplicativity: $\left(\frac{2}{17}\right)_2$, $\left(\frac{2}{19}\right)_2$, $\left(\frac{3}{17}\right)_2$, $\left(\frac{3}{19}\right)_2$, $\left(\frac{6}{17}\right)_2$, $\left(\frac{6}{19}\right)_2$, $\left(\frac{6}{323}\right)_2$, $\left(\frac{24}{323}\right)_2$. (b) Of the numbers 2, 3, 6, and 24, can you determine which are squares mod 17? mod 19? mod 323?

12.3.04 (a) Compute the following Legendre or Jacobi symbols by hand: $\left(\frac{2}{5}\right)_2$, $\left(\frac{2}{7}\right)_2$, $\left(\frac{3}{5}\right)_2$, $\left(\frac{3}{7}\right)_2$, $\left(\frac{6}{5}\right)_2$, $\left(\frac{6}{7}\right)_2$, $\left(\frac{2}{35}\right)_2$, $\left(\frac{3}{35}\right)_2$, $\left(\frac{6}{35}\right)_2$, $\left(\frac{24}{35}\right)_2$. (b) Of the numbers 2, 3, 6, and 24, can you determine which are squares modulo 5? modulo 7? modulo 35?

12.3.05 Identify each of the following quadratic symbols as a Legendre or Jacobi symbol and then compute it by hand: $\left(\frac{2}{31}\right)_2$, $\left(\frac{5}{31}\right)_2$, $\left(\frac{10}{93}\right)_2$. What (if anything) can you conclude about whether 2, 5, or 10 are squares modulo 31 or 93?

Chapter 13

13.1.07 You need not verify that there are no smaller Fermat pseudoprimes, but do verify that each of the listed numbers *is* a Fermat pseudoprime that is not prime. (You may use WolframAlpha for the exponentiation mod n and for the primality testing.) And do determine which of the listed false primes are detected by Fermat's test base 3 or base 5.

13.3.01 Show that 341 is a Fermat pseudoprime base 2, but not an Euler pseudoprime base 2. (You may use WolframAlpha for the exponentiation mod n, but use quadratic reciprocity to compute the Jacobi symbol.)

13.3.02 Show that 91 is a Fermat pseudoprime base 3, but not an Euler pseudoprime base 3. (You may use WolframAlpha for the exponentiation mod n, but use quadratic reciprocity to compute the Jacobi symbol.)

13.3.03 Show that 1387 is a Fermat pseudoprime base 2, but not an Euler pseudoprime base 2. (You may use WolframAlpha for the exponentiation mod n, but use quadratic reciprocity to compute the Jacobi symbol.)

13.3.04 Show that 1729 is an Euler pseudoprime base $b = 2$, $b = 3$, and $b = 5$. (You may use WolframAlpha for the exponentiation mod n, but use quadratic reciprocity to compute the Jacobi symbols.)

13.4.02 (a) How likely do we suppose it is that 1729 is truly prime, given that it passes the Solovay-Strassen Test with bases $b = 2$, $b = 3$, and $b = 5$? (See 13.3.04.) (b) Choose three 'random' integers b with $1 < b < 1728$, and run the Solovay-Strassen Test with them. (You may use the WolframAlpha to compute the Jacobi symbols, if you want.) What can you conclude?

13.4.03 (a) How many numbers b in the range $0 < b < 560$ should we use with the Solovay-Strassen Test to conclude with probability 80% that 561 is prime? (b) Run the test with $b = 35$, 281, and 463. (You may use the WolframAlpha to calculate Jacobi symbols.) (c) Choose 10 'random' integers b with $1 < b < 560$, and run the test with them. What can you conclude?

Chapter 14

14.3.01 Alice has a secret: the factorization of $n = 21$ (which we pretend not to know.) Bob chooses $x = 10$. (a) Check that $z = x^2 \bmod 21$ is 16. (b) After sending $z = 16$ to Alice, Bob receives $y = 17$ from Alice. Show that Bob can find the factorization of 21 by computing $\gcd(n, x - y)$ and $\gcd(n, x + y)$, using the Euclidean algorithm.

14.3.02 Alice has a secret: the factorization of $21 = 3 \cdot 7$. (Don't tell!) Bob chooses an integer x in the range $1 < x < 21$, computes $z = x^2 \bmod 21 = 16$, and sends z to Alice. (a) Alice computes the principal square roots w_1 and w_2 of 16 modulo the primes $p = 3$ and $q = 7$, respectively, using the formulas $w_1 = z^{(p+1)/4} \bmod p$ and $w_2 = z^{(q+1)/4} \bmod q$. What are w_1 and w_2? (b) Alice chooses $y_1 = -w_1$ and $y_2 = w_2$ and computes y (reduced modulo 21) such that $y = y_1 \bmod p$ and $y = y_2 \bmod q$ using Sun Ze's Theorem. What is y?

14.3.03 Alice has a secret: the factorization of $n = 327\,653$. Bob chooses $x = 200\,005$. (a) Bob sends $z = x^2 \bmod n$ to Alice. What is z? (b) Bob receives $y = 312\,140$ from Alice. Compute $\gcd(n, x - y)$ and $\gcd(n, x + y)$, using the Euclidean algorithm. Have you found the factorization of n?

14.3.04 Alice has a secret: $n = 330\,481 = 563 \cdot 587$. Bob chooses an integer x in the range $1 < x < 330\,481$ and computes $z = x^2 \bmod n = 175\,422$. (a) Alice computes the principal square roots w_1 and w_2 of z modulo the primes $p = 563$ and $q = 587$, respectively. What are w_1 and w_2? (b) Alice chooses $y_1 = w_1$ and $y_2 = -w_2$ and computes y (reduced modulo n) such that $y = y_1 \bmod p$ and $y = y_2 \bmod q$ using Sun Ze's Theorem. What is y?

14.3.07 Alice has a secret: the factorization of $n = 450\,097 = 659 \cdot 683$. Bob chooses $x = 1\,000$. (a) Bob sends $z = x^2 \bmod n$ to Alice. What is z? (b) Alice computes principal square roots w_1 and w_2 of z modulo $p = 659$ and $q = 683$ respectively. She chooses $y_1 = \pm w_1$ and $y_2 = \pm w_2$. List the four possible choices for (y_1, y_2), and in each case find y (reduced modulo n) such that $y = y_1 \bmod p$ and $y = y_2 \bmod q$ using Sun Ze's Theorem. (c) Which choices will reveal the secret to Bob? Justify your answer by showing how Bob can recover the secret in each case that it is possible.