Chapter 4

4.4.04 We can write the set of all outcomes as

$$\Omega = \{\omega_0, \omega_1, \omega_2, \ldots, \omega_n, \ldots\}$$

where ω_n is the event in which the sequence of coin flips begins with n heads and then a tail. Define a random variable X to be the number of heads before the first tail, so $X(\omega_n) = n$. Since Ω is an infinite set, we will end up having to evaluate an infinite series to calculate the expected value. You may find one of the following formulas from Calc 2 to be helpful: for $|x| < 1$,

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x} \qquad \sum_{n=0}^{\infty} (n+1)x^n = \frac{1}{(1-x)^2} \qquad \sum_{n=0}^{\infty} n\,x^n = \frac{1}{(1-x)^2} - \frac{1}{1-x}$$

4.4.05 See the hint for 4.4.04.

4.4.08 This problem is similar to, but slightly different from 4.4.04. You will have the same set of outcomes Ω, but the appropriate random variable is now the number of flips up to and including the first tail. So $X(\omega_n) = n + 1$. Again, you will need to evaluate an infinite series to calculate the expected value; use one of the formulas in the hint for 4.4.04.

4.5.07 Compute the index of coincidence of the following two character streams:

```
nowilaymedowntosleep
nowimaymeetonthestep
```

4.5.08 Is this index of coincidence computed in 4.5.07 what you would expect for two random character streams of English? If not, is it higher or lower?

4.5.09 Encrypt the character streams in 4.5.07 with a simple shift cipher with key 3, and compute the index of coincidence of the resulting encrypted character streams.

4.5.10 Encrypt the character streams in 4.5.07 with using Vigenère cipher with key '`lullaby`', and compute the index of coincidence of the resulting encrypted character streams.

4.5.11 (a) Compute the index of coincidence of the following two character streams:

```
wheninthecourseofhumaneventsit
becomesnecessaryforonepeopleto
```

(b) Is this index of coincidence what you would expect for two random character streams of English? If not, is it higher or lower? (c) Encrypt the character streams with a simple shift cipher with key 7, and compute the index of coincidence of the resulting encrypted character streams. (d) Explain why the index of coincidence will not change after encrypting with a shift cipher, regardless of the key.

4.5.12 Use the Friedman attack to crack the Vigenère cipher for the ciphertext posted in the text file `friedman-ciphertext.txt` on Blackboard. You may use *Mathematica* or another computer program. I have posted a *Mathematica* notebook on Blackboard (`friedman-students.nb`) that walks you through the process; it includes commands for computing the index of coincidence, etc. Bonus points if you can figure out what the original plaintext is!

Chapter 6

6.3.1 Run the Euclidean algorithm backwards to find the inverse. (You do not need to use the matrix way of doing the computation.)

6.3.2 Run the Euclidean algorithm backwards to find the inverse. (You do not need to use the matrix way of doing the computation.)

Chapter 7

7.3.04 Verify that 2 is not a primitive root mod 17, but 3 is a primitive root mod 17.

7.5.03 With public information $b = 2$, $c = 58$, $p = 103$ for an ElGamal cipher with included header $b^r = 98$, use the private/secret key $\ell = 47$ (the discrete log of $c = 58$ base $b = 2$ modulo $p = 103$) to decrypt the ciphertext '79'.

7.5.04 An ElGammal cipher has public information $b = 82$, $c = 85$, and $p = 97$.

(a) Verify that the discrete log of 85 base 82 mod 97 is $\ell = 54$.

(b) Use the private key $\ell = 54$ to decrypt the ciphertext $y = 55$ with included header $b^r = 32$.

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 12

12.3.01 (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, which are squares modulo 17? modulo 19? modulo 323?

12.3.02 (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, which are squares modulo 5? modulo 7? modulo 35?

Chapter 13

13.1.07 Note: For this problem, you may use *Mathematica* or another computer programming language to generate tables of numbers of the form $b^{n-1} \,\%\, n$ and test for primality. Some helpful *Mathematica* commands are `Table`, `PowerMod`, and `PrimeQ`.

13.3.01 Show that 341 is a Fermat pseudoprime base 2, but not an Euler pseudoprime base 2. (You may use `PowerMod` for the exponentiation, 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 `PowerMod` for the exponentiation, 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 `PowerMod` for the exponentiation, 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 `PowerMod` for exponentiation, 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 `JacobiSymbol` command 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 `JacobiSymbol` command in *Mathematica*.) (c) Choose 10 'random' integers b with $1 < b < 560$, and run the test with them. What can you conclude?

13.6.01 Hint: First write $n - 1$, which is 1280, in the form $(2^r) \cdot m$, where m is odd. To do this, just factor out as many 2s as you can from 1280. The number of 2s you factored out is your r. (You should get $r = 8$.) After dividing 1280 by all the 2s, you will have an odd number: this is m. (You should get $m = 5$.) Next you compute b^m, b^{2m}, b^{4m}, etc., where b is your base; here $b = 41$. In theory, you may need to compute up to $b^{(n-1)/2}$, which is 41^{640}, but you will probably be able to stop computing powers before then. If $b^m = \pm 1 \bmod 1281$, you are done. If not, keep going. If $b^{2m} = -1 \bmod 1281$, you are done. Keep computing the powers of b^m until you get -1.

13.6.09 Consider $n = 2753$. Choose three 'random' integers b in the range $1 < b < 2752$, and run the Miller-Rabin Test with them. What can you conclude? Is your conclusion certain or just probable? If probable, what is the probability?

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?

14.3.05 Alice has two secrets $s_0 = 23$ and $s_1 = 32$. She will use oblivious transfer to reveal one of the secrets to another person, without herself knowing which secret has been revealed, so she publishes the following information publically: $p = 103$, $g = 2$, $c = 25$. (a) Bob wishes to know s_0 so he chooses his bit $i = 0$. He also chooses a random integer x in the range $1 < x < 102$: $x = 47$. Bob computes $b_0 = g^x \bmod p$ and $b_1 = c \cdot g^{-x} \bmod p$ and sends (b_0, b_1) to Alice, while keeping $i = 0$ and $x = 47$ secret. What are b_0 and b_1? (b) Alice checks that $b_0 b_1 = c \bmod p$. Check this yourself. (c) Alice chooses $y_0 = 61$ and $y_1 = 11$ and computes a_0, a_1, t_0, t_1, m_0 and m_1 as described in the text. Compute these numbers for yourself. What are they? (d) Alice sends a_0, a_1, m_0, and m_1 to Bob but keeps t_0 and t_1 secret. Bob acquires the secret s_0 by computing $a_0^x = t_0$ and $s_0 = m_0 - t_0$. Check that this works.

14.3.06 Alice has the same two secrets and the same public information as in the previous problem. (a) Bernie wishes to know s_1 so he chooses his bit $i = 1$. He also chooses a random integer x in the range $1 < x < 102$: $x = 47$. Bernie computes $b_1 = g^x \bmod p$ and $b_0 = c \cdot g^{-x} \bmod p$ and sends (b_0, b_1) to Alice, while keeping $i = 1$ and $x = 47$ secret. What are b_0 and b_1? (b) Alice checks that $b_0 b_1 = c \bmod p$. Check this yourself. (c) Alice chooses $y_0 = 55$ and $y_1 = 14$ and computes a_0, a_1, t_0, t_1, m_0 and m_1 as described in the text. Compute these numbers for yourself. What are they? (d) Alice sends a_0, a_1, m_0, and m_1 to Bernie but keeps t_0 and t_1 secret. Bernie acquires the secret s_1 by computing $a_1^x = t_1$ and $s_1 = m_1 - t_1$. Check that this works.

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.

14.4.01 Peter knows the factorization $n = 351\,613 = 587 \cdot 599$, but Vera does not. Vera chooses a random integer $x = 6001$, computes $z = x^4 \,\%n$, and sends z to Peter. (a) What is z? (b) Peter computes the principal square roots y_1 and y_2 of z modulo 587 and 599, respectively. What are y_1 and y_2? (c) Peter finds an integer y satisfying $y = y_1 \bmod 587$ and $y = y_2 \bmod 599$, with $0 < y < n$. What is y? (d) Vera checks that $y^2 = z$. Check this for yourself.

14.4.02 Vera wishes to cheat and use Peter as a square root oracle, in order to find the factorization of $n = 351\,613$. Vera chooses three random integers x_1, x_2, x_3, computes their **squares** w_1, w_2, w_3 modulo n and sends them to Peter. Peter returns square roots y_1, y_2, y_3 of w_1, w_2, w_3 modulo n. (a) What are the chances that Vera can factor n using this information? (b) Given that Vera's choices, $x_1 = 6\,001$, $x_2 = 54\,321$, and $x_3 = 100\,001$, return $y_1 = 345\,612$, $y_2 = 297\,292$, and $y_3 = 331\,279$ from Peter, can Vera factor n? If so, which pair(s) (x_i, y_i) allow her to factor n?

Chapter 16

16.4.03 Simply find the period of the LFSR given in problem 16.4.03 in the textbook; assume that all computations are modulo 2.

16.4.04 Simply find the period of the LFSR given in problem 16.4.04 in the textbook; assume that all computations are modulo 2.

16.4.05 Simply find the period of the LFSR given in problem 16.4.05 in the textbook; assume that all computations are modulo 2.

16.6.01 Let p be a prime congruent to 3 modulo 4 and S be the set of squares in $(\mathbb{Z}/p)^\times$. Show that the squaring map $x \mapsto x^2$ is a bijection of S to itself.

16.6.02 Let $p = 3$, $q = 7$, $n = pq$. (a) Find the set S of squares in $(\mathbb{Z}/n)^\times$. (b) Write out the bijection $S \to S$ given by $x \mapsto x^2$ explicitly, e.g. via a table. (c) What is the maximal period of a sequence with recursion relation: $s_{i+1} = s_i^2 \,\%\, n$, given that the seed s_0 is in $(\mathbb{Z}/n)^\times$? (d) Find all "bad seeds" in $(\mathbb{Z}/n)^\times$, i.e. all elements x_{bad} in $(\mathbb{Z}/n)^\times$ such that if $s_0 = x_{\text{bad}}$, $s_{i+1} = s_i$ for all $i \geq 1$.

16.6.03 Let $p = 3$, $q = 11$, $n = pq$. (a) Find the set S of squares in $(\mathbb{Z}/n)^\times$. (b) Write out the bijection $S \to S$ given by $x \mapsto x^2$ explicitly, e.g. via a table. (c) What is the maximal period of a sequence with recursion relation: $s_{i+1} = s_i^2 \,\%\, n$, given that the seed s_0 is in $(\mathbb{Z}/n)^\times$? (d) Find all "bad seeds" in $(\mathbb{Z}/n)^\times$, i.e. all elements x_{bad} in $(\mathbb{Z}/n)^\times$ such that if $s_0 = x_{\text{bad}}$, $s_{i+1} = s_i$ for all $i \geq 1$.

16.6.04 Let $p = 7$, $q = 11$, $n = pq$. (a) Find the set S of squares in $(\mathbb{Z}/n)^\times$. (b) Write out the bijection $S \to S$ given by $x \mapsto x^2$ explicitly, e.g. via a table. (c) What is the maximal period of a sequence with recursion relation: $s_{i+1} = s_i^2 \,\%\, n$, given that the seed s_0 is in $(\mathbb{Z}/n)^\times$? (d) Find all "bad seeds" in $(\mathbb{Z}/n)^\times$, i.e. all elements x_{bad} in $(\mathbb{Z}/n)^\times$ such that if $s_0 = x_{\text{bad}}$, $s_{i+1} = s_i$ for all $i \geq 1$.

Chapter 18

18.1.04 Use Pollard's rho method to find a factor of 2059.

18.3.04 Use Proth's Corollary to prove that 577 is prime.

18.4.01 Suppose x is a large real number. Consider the interval $\mathcal{I} = [x - 50, x + 50)$. (a) How many integers are there in the interval $\mathcal{I}$? (b) Use the Prime Number Theorem (twice) to estimate the number of primes in the interval $\mathcal{I}$. (c) Estimate the probability that a "random" integer in $\mathcal{I}$ is prime. For $x = 10^9$, calculate this estimate explicitly, and compare to $1/\ln(x)$. (d) Challenge: Use L'Hopital's rule to show that the probability of a "random" integer in $\mathcal{I}$ being prime is $\sim 1/\ln(x)$ as $x \to \infty$.

18.4.02 Let p_1' be an integer, and suppose $p_1 = 2kp_1' + 1$ for some positive integer k. Show that p_1' divides $p_1 - 1$.

18.4.03 Let p_1 and p_2 be odd integers and suppose t satisfies $t = 1 \bmod p_1$ and $t = -1 \bmod 4p_2$. Show that (a) p_1 divides $t - 1$, (b) p_2 divides $t + 1$, and (c) $t \equiv 3 \bmod 4$.

18.4.04 Suppose $p = t + 4kp_1p_2$, where t, p_1, and p_2 are as in the previous exercise and k is a positive integer. Show that (a) p_1 divides $p - 1$, (b) p_2 divides $p + 1$, and (c) $p \equiv 3 \bmod 4$.

18.4.05 Suppose x is a large real number. Consider the interval $\mathcal{I} = [x - 50, x + 50)$. (a) Estimate the number of primes congruent to 1 mod 10 in the interval $\mathcal{I}$ using the fact that $\pi_{10,1}(t) \sim t/(\phi(10)\ln(t))$ as $t \to \infty$. (b) Estimate the probability that a "random" integer in $\mathcal{I}$ is a prime congruent to 1 mod 10. For $x = 10^9$, calculate this estimate explicitly, and compare to $1/(\phi(10)\ln(x))$. (c) Find all primes congruent to 1 mod 10 in $\mathcal{I}$. (You could create a table in *Mathematica* and use the `PrimeQ` command, for example.)

18.5.01 Provide a primality certificate for $N = 1\,000\,000\,009$. (Hint: the only primes dividing $N - 1 = 1\,000\,000\,008$ less than $B = 100$ are 2, 3, and 7.)

18.5.02 Provide a primality certificate for $N = 1\,000\,000\,021$. (Hint: using B=30 suffices.)

Chapter 19

19.2.01 Given that 100 is a square root of $b = 4$ modulo 833, find a proper factor of 833 by hand.

19.2.02 Factor 105 by hand. Use Sun Ze's Theorem to find all square roots of $b = 4$ modulo 105.

19.2.03 Factor 525 by hand. Use Sun Ze's Theorem to find all square roots of $b = 16$ modulo 525.

19.2.04 Given that $x = 4\,642$, $y = 5\,371$, $z = 8\,176$ are square roots of $b = 188$ modulo $n = 10\,013$, find a proper factor of n by hand.

19.1.01 Use Gaussian elimination to find a dependency relation among the vectors $v_1 = (1, 2)$, $v_2 = (1, 0)$, $v_3 = (3, 2)$ in $\mathbb{R}^2$.

19.1.02 Use Gaussian elimination to find a dependency relation among the vectors $v_1 = (0, 1, 1, 0)$, $v_2 = (1, 0, 0, 1)$, $v_3 = (1, 1, 1, 0)$, $v_4 = (1, 0, 1, 0)$, and $v_5 = (0, 1, 0, 1)$ in $\mathbb{F}_2^4$, where $\mathbb{F}_2 = \mathbb{Z}/2$ is the finite field with two elements.

19.3.01 Use Dixon's Algorithm to factor (a) $n = 3127$ with factor base $\{2, 3\}$ and lucky choice $a = 56$, and (b) $n = 3149$ with factor base $\{2, 3, 5\}$ and lucky choice $a = 57$.

19.3.02 Use Dixon's Algorithm to factor $n = 803$ with factor base $\{2, 3, 5\}$ and $a_1 = 41$, $a_2 = 43$, $a_3 = 51$, $a_4 = 82$, as follows. (a) Compute $b_i = a_i^2 \,\%\, n$ for $1 \le i \le 4$. Verify that each b_i is 5-smooth, and write out the prime factorization of each b_i in the form $b_i = 2^{e_{i1}} \cdot 3^{e_{i2}} \cdot 5^{e_{i3}}$. (b) Compute the vectors $v_i = (e_{i1} \,\%\, 2, e_{i2} \,\%\, 2, e_{i3} \,\%\, 2)$ for each $1 \le i \le 4$. (c) Use Gaussian elimination to find coefficients $c_1, c_2, c_3, c_4 \in \mathbb{F}_2$ in a dependency relation $c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4 = 0$. (d) Compute $x = a_1^{c_1}\, a_2^{c_2}\, a_3^{c_3}\, a_4^{c_4}$ and let y be the square root (in $\mathbb{Z}$) of $b_1^{c_1}\, b_2^{c_2}\, b_3^{c_3}\, b_4^{c_4}$. (This is a perfect square, as you can see by looking at the exponents of the prime factors.) (e) Compute $\gcd(x \pm y, n)$ to find proper factors of n.

19.3.03 Use Dixon's Algorithm to factor $n = 923$ with factor base $\{2, 3, 5\}$ and $a_1 = 44$, $a_2 = 46$, $a_3 = 53$, $a_4 = 57$. (Follow the outline given in the previous problem.)

19.4.01 Let $n = 2773$. (a) Find $m = \text{floor}(\sqrt{n})$. (b) For all a the range $m + 1 \le a \le 2m$, find $b = a^2 \,\%\, n$, and find the prime factorization of b. (You may find the *Mathematica* commands `Table`, `TableForm`, and `FactorInteger` helpful, though you're certainly welcome to use other commands or even other programing languages.) (c) How many of the b's found in the previous part are smooth with respect to the factor base $\{2, 3\}$? with respect to $\{2, 3, 5\}$? $\{2, 3, 5, 7\}$? $\{2, 3, 5, 7, 11\}$? (d) What factor base is an appropriate size to guarantee that, using the values from (b), we will be able to find a dependency relation among the exponent-reduced-mod-2 vectors? (e) Construct three pairs (x, y) such that $x^2 = y^2 \bmod n$ but $x \ne \pm y \bmod n$, given the values for a and b you have found.

19.4.02 Let $n = 4343$. (a) Find $m = \text{floor}(\sqrt{n})$. (b) For all a the range $m + 1 \le a \le m + 40$, find $b = a^2 \,\%\, n$, and find the prime factorization of b. (c) How large a factor base is needed to find five b's that are smooth with respect to that factor base? Is the factor base small enough to *ensure* that a dependency relation must exist among the exponent-reduced-mod-2 vectors? (d) If we extend the range to $m + 1 \le a \le 2m$, how many b's are there that are smooth with respect to the factor base you found in the previous part? (e) Construct two pairs (x, y) such that $x^2 = y^2 \bmod n$ but $x \ne \pm y \bmod n$, given the values for a and b you have found.

19.4.03 Let $n = 2881$. (a) Find $m = \text{floor}(\sqrt{n})$. (b) For all a the range $m + 1 \le a \le 2m$, find $b = a^2 \,\%\, n$, and find the prime factorization of b. (c) On what attempt do we "get lucky" and find a b that is a perfect square in $\mathbb{Z}$? (d) How many attempts are needed to generate a list of $(t + 1)$ b values that are p_t smooth? (You need to specify an appropriate factor base $\{2, 3, \ldots, p_t\}$ to answer this.)

19.5.01 Let $n = 4343$. (a) Find the first 10 continued fractions rational approximations $r_i = p_i/q_i$ for $\sqrt{n}$, as outlined in the reading questions for 19.5. (b) Construct a list of pairs (a, b) with (potential) values for a being the numerators p_i of the rational approximations r_i found in (a) and (potential) values for b being given by $p_i^2 - q_i^2 n$. (Note that this guarantees that $b = a^2 \bmod n$.) Keep only those pairs (a, b) for which b is smooth with respect to the factor basis $\{-1, 2, 5, \ldots, 17\}$. (c) How many pairs do you have? Compare this to the number of such pairs you found in ten attempts in 19.4.02.