Problem Set 10, Due Wednesday, April 26

INSTRUCTIONS: Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

1. Find the value of the Jacobi symbol \( \left( \frac{1463}{5083} \right) \) by repeated use of the Quadratic Reciprocity Law. **Justify every step.** There will be no credit given for using either an exhaustive search, a computer algebra system, or a program.

2. Pythagorean triples.
   
   (a) Prove that the triple of numbers \((645, 818, 1037)\) is not a primitive Pythagorean triple (PPT).
   
   (b) One of the three numbers can be changed to make the resulting triple a PPT. Determine which number is wrong – and why it is wrong – and use the Theorem 13.1 to determine the corrected PPT.

3. Find a positive integer \(z\) that is the hypotenuse for four distinct PPT’s. (NOTE: Changing the signs of the numbers \(x, y\) and \(z\) does not count.)

4. Find the square-free congruent numbers (see Section 13.5) corresponding to the area of the primitive right triangle corresponding to these Pythagorean triples:
   
   (a) \((35, 12, 37)\)  
   (b) \((11, 60, 61)\)  
   (c) \((45, 28, 53)\)  
   (d) \((9, 40, 41)\).

Problem Set 9, Due Friday, April 7

INSTRUCTIONS: Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

Class on Wednesday April 5 will be devoted to the Quadratic Reciprocity Law and Gauss’s Lemma. The textbook identifies and describes both the Law and the Lemma.

1. Find the value of the Legendre symbol \( \left( \frac{83}{127} \right) \) by repeated use of the Quadratic Reciprocity Law. **Justify every step.** There will be no credit given for using either an exhaustive search, a computer algebra system, or a program.

2. Use Gauss’s Lemma with \(a = 6\) and \(p = 31\) to evaluate the Legendre symbol \( \left( \frac{6}{31} \right) \).

3. (a) Prove that if \(p \equiv -1 \pmod{8}\), then the integer \(2^{(p-1)/2} - 1\) is divisible by \(p\). Assume that if \(p\) is an odd prime, then \(2\) is a quadratic residue mod \(p\) if and only if \(p \equiv 1\) or \(7\) (mod 8).
(b) Use this fact to find a divisor \( d \) of \( M_{83} = 2^{83} - 1 \) such that \( 1 < d < M_{83} \).

**Problem Set 8, Due Wednesday, March 29**

**INSTRUCTIONS:** Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

1. Find – with proof – all positive integers \( n \) such that \( \phi(n) = 12 \).

2. Prove that if \( n \) is a positive integer, then \( \mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0 \).

3. Write a program to implement the Lucas-Lehmer Test (Rosen, Theorem 7.13) for primality of \( M_p = 2^p - 1 \), where \( p \) is a prime. Your output should include:
   
   (a) a list of the remainders \( \{r_1, r_2, \ldots, r_{p-1}\} \mod M_p \), and
   
   (b) a conclusion about the primality or compositeness of \( M_p \) and a reason for that conclusion.

   Use this test to determine the primes \( p \) between 60 and 130 for which \( M_p \) is prime. SHOW YOUR WORK.

4. Let \( q \) be a prime divisor of the Fermat number \( F_n = 2^{2^n} + 1 \). Prove that \( ord_q(2) = 2^{n+1} \).
   
   **(HINT:** This problem is not meant to be hard.)

**Problem Set 7, Due Monday, March 20**

**INSTRUCTIONS:** Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

1. Find the last digit of the decimal expansion of \( 437^{999999999} \).

2. Let \( n = 35 \). Construct a table comparing \( a^{35} \mod 35 \) with \( a^{35-\phi(35)} \mod 35 \) for \( a = 1, 2, \ldots, 35 \). What do you notice?

3. What you notice is true for all positive integers \( n \). Prove it.

4. Prove that if \( m \) and \( n \) are positive integers and \( m|n \), then \( \phi(m)|\phi(n) \).

5. A positive integer is called **3-special** if it can be written as a sum of two or more consecutive positive integers in exactly one way, namely as a sum of three consecutive positive integers. Thus, \( 12 = 3+4+5 \) is 3-special, but \( 15 = 4+5+6 = 1+2+3+4+5 \) is not 3-special. Characterize the 3-special numbers.

**Problem Set 6, Due Monday, March 13**

**INSTRUCTIONS:** Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.
1. We are looking for square divisors of consecutive numbers.

   (a) Find five consecutive integers \( x, x + 1, x + 2, x + 3, x + 4 \), each divisible by the square of an integer greater than 1.

   (b) Find six consecutive integers such that each integer is divisible by the square of a prime greater than five.

2. According to a local legend, a band of seven pirates have found a hoard of gold coins and are trying to share the coins equally among themselves. Alas, there are six coins left over, and in the ensuing fight, one pirate is slain. The remaining six pirates, still unable to share equally because two coins are left over, fight again — and another pirate lies dead. The remaining pirates attempt to share and share alike, except that one coin is left over. One more fight, one more dead pirate, and it is only now that an equal sharing is possible.

   What is the minimum number of coins which allows this to happen? You may assume, without proof, the Generalized Chinese Remainder Theorem, as stated in Exercise 19 of Section 4.3 of the textbook.

3. Let \( p = 6529 \), \( q = 6601 \), and \( r = 6673 \).

   (a) Perform the Fermat Primality Test on each of \( p \), \( q \), and \( r \) using the random bases \( a = 573 \), \( b = 605 \), and \( c = 633 \). In each of these cases, what does the test tell you? Give reasons.

   (b) Perform Miller’s Test (also known as the Miller-Rabin Test and the Strong Pseudoprime Test) on each of \( p \), \( q \), and \( r \) using the random bases \( a = 573 \), \( b = 605 \), and \( c = 633 \). What do the results of these tests tell you about \( p \), \( q \), and \( r \)? Give reasons.

AT MOST ONE MORE TO FOLLOW.
1. Let \( X = \{6n + 1 : n \in \mathbb{Z}, n \geq 0\} \).

   (a) Prove that \( X \) is closed under multiplication.

   (b) An \( X \)-prime is an element \( p \in X \) that cannot be written as a product \( p = ab \) of elements \( a, b \in X \) such that \( a > 1 \) and \( b > 1 \). \( n \in X \) is an \( X \)-composite if \( n > 1 \) and \( n \) is not an \( X \) prime. Find all \( X \) composites between 1 and 200.

   (c) Prove that \( X \) does not have unique factorization of elements into primes by finding an element \( n \) of \( X \) that has at least two distinct factorizations of \( n \) into products of \( X \)-primes – that is, \( n = ab = cd \) where \( a, b, c, \) and \( d \) are \( X \)-primes and \( \{a, b\} \neq \{c, d\} \).

2. Find, with proof, all primes in \( \mathbb{Z} \) of the form \( 2^{2n} + 5 \).

3. Prove that \( \log_2 3 \) is irrational.

4. At a fancy restaurant, the total cost of a jambalaya dinner is $11 and the total cost of a fried chicken dinner is $8. What conclusions can you make if the total bill is each of the following amounts?

   (a) $96
   (b) $777
   (c) $69

Problem Set 3, Due Monday, February 6

INSTRUCTIONS: Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

1. The Euclidean algorithm is not the only way to find GCD’s. Here is a procedure for finding the GCD of two positive integers \( u \) and \( v \) that uses only subtractions, divisions by 2, and parity checks. Here is how it works. Given \( u, v \) positive integers, apply the following procedure recursively to \( (u, v) \), reversing the roles of \( u \) and \( v \) where necessary:

   \[
   (u, v) = \begin{cases} 
   u, & \text{if } u = v; \\
   2(u/2, v/2), & \text{if } u \text{ and } v \text{ are both even}; \\
   (u/2, v), & \text{if } u \text{ is even and } v \text{ is odd}; \\
   (u - v, v), & \text{if } u \text{ and } v \text{ are both odd and } u > v. 
   \end{cases}
   \]

   (a) Find \((4212, 16636)\) using this algorithm. Show all of the steps.

   (b) Prove that this algorithm always produces the GCD of the given positive integers.

2. Let \( a \) and \( b \) be positive integers and let \( c \) be an integer greater than 1. Prove that \( (c^a - 1, c^b - 1) = c^{(a,b)} - 1 \).
3. Let \( a = 10166 \) and \( b = 1111 \).

(a) Use the Euclidean Algorithm (the “Pulverizer”) to find the greatest common divisor \( g \) of 10166 and 1111. Show every step.

(b) Use the Extended Euclidean algorithm (the “Dragon”) to find integers \( m \) and \( n \) such that \( g = 10166m + 1111n \). Show every step.

4. In the mid-nineteenth century, the French mathematician A. de Polignac (pronounced “PAW-lean-yock”) made a remarkable observation: It seems that every odd number greater than one can be written as a sum of a power of two and a prime. Thus,

\[
3 = 2^0 + 1, \quad 5 = 2^1 + 3, \quad 7 = 2^2 + 3, \ldots, \quad 53 = 2^4 + 37, \ldots, \quad 999999 = 2^{16} + 944463, \ldots
\]

He claimed to have checked this for all odd numbers up to three million! Can you prove de Polignac’s conjecture?

**Problem Set 2, Due Monday, January 30**

INSTRUCTIONS: Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

1. Show that no number of the form \( 1 + n^3 \) is a prime, except for \( 2 = 1 + 1^3 \).

2. Find a sequence of the form \((a, a + d, a + 2d, a + 3d, \ldots, a + (n - 1)d)\) of length at least six in which \( a \) is a number of three or more digits and every number in the sequence is a prime.

3. Use induction to prove that \( n^5 - n \) is divisible by 5 for every positive integer \( n \). Is this true if 5 is replaced by 6? by 7?

4. Recall that a positive integer is called special if it can be written as a sum of two or more consecutive positive integers. Describe, with proof, the set of positive integers that are not special. (HINT: Generate a list. Based on that list, make a guess. Then prove it.)

**Problem Set 1, Due Monday, January 23**

INSTRUCTIONS: Show all work. Part credit for unjustified correct answers. No credit for unjustified wrong answers. If a program was used, hand in well-documented source code or computer algebra system code along with the output.

1. Rosen, Exercises 1.3 # 20

2. Rosen, Exercises 1.4 # 6

3. A positive integer is called special if it can be written as a sum of two or more consecutive positive integers. For example, \( 15 = 7 + 8, \quad 36 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8, \)
   and \( 348 = 40 + 41 + 42 + 43 + 44 + 45 + 46 + 47 \). Describe, with proof, the set of positive integers that are not special. (HINT: Generate a list. Based on that list, make a guess. Then prove it.)