1. (10 points) True or False. Determine if the following statements are true. Explain your answers.

1. Let $\mu(n)$ be the M"obius Function. Then the function \( \sum_{d \mid n} \mu(d) \) is multiplicative.

2. Let $p$ be prime. Assume that \( \left( \frac{a}{p} \right) = -1 \). Then $a$ is a primitive root modulo $p$.

2. (10 points) Find a set of mutually incongruent primitive roots modulo 50.

3. (10 point) Show that there are infinitely many prime numbers $p$ such that the equation $x^4 - 4 \equiv 0 \pmod{p}$ has no solution.

4. (10 points) Recall that Fibonacci numbers are defined as $F_1 = 1$, $F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 1$.

1. Let $n \geq 1$. Show that for any $k > 0$, we have $F_n \mid F_{kn}$.

2. Based on the result of (1), assume that $F_n$ is a prime number, what can you say about $n$?

5. (10 point) Let $p > 2$ be prime. How many mutually incongruent solutions do the following equations have? Explain your answers.

1. $x^p + 1 \equiv 0 \pmod{p^3}$.

2. $x^p + x + 1 \equiv 0 \pmod{p^3}$.

3. $x^p - x + 1 \equiv 0 \pmod{p^3}$.

6. (10 points) Find the smallest positive integer $n$ such that
\[ \sum_{e \mid n} \mu(e) d^2(e) > 2018. \]

7. (20 points) Let $p > 2$ be prime. Let $d$ the least positive quadratic non-residue modulo $p$.

1. Is it possible that $d = 6$ for some $p$?

2. Let $p$ be the prime number less than 100 with the largest possible $d$. Determine $p$ and $d$.

3. From the case of (2), find the least positive number $n$ such that $n$ is both a primitive root modulo $p$ and also a primitive root modulo $d$.

4. Consider the numbers $p$, $d$ and $pd$ from (2). Are any of these numbers sum of two squares? Sum of three squares? Sum of four squares? Explain your answers.

8. (10 points) Assume $p$ is a prime number and $p \equiv 7 \pmod{8}$. Show that
\[ \sum_{k=1}^{\frac{p-1}{2}} k \left( \frac{k}{p} \right) = 0. \]

9. (10 points) Find the number of pairs of consecutive integers $(a, a+1)$ in $[1, 100]$ such that exactly one number in the pair is a quadratic residue modulo 101.

Solutions on next page.
Solutions:

1. (1) True. Let \( n = n_1^2 \cdot m \) where \( m \) is square free. Then \( \sum_{d \mid n} \mu(d) = \sum_{d \mid n_1} \mu(d) \).
   By Theorem 6.5 this is 0 unless \( n_1 = 1 \) (in which case it is equal to 1). In other words it is 1 if \( n \) is square free, 0 if not. Or, say in another way, \( \sum_{d \mid n} \mu(d) = \mu^2(n) \). Now it is clear that this function is multiplicative.

(2) False. If \( a \) is a primitive root modulo \( p \), then \( \left( \frac{a}{p} \right) = -1 \). But the converse is not true. For example \( p = 7 \) and \( a = 6 \).

2. Note that \( \varphi(50) = 20 \) and \( \varphi(20) = 8 \). Direct computation to check that 3 is a primitive root modulo 5, and that \( 3^{5-1} \equiv 81 \equiv 6 \pmod{5^2} \). Therefore by Exercise #12 in §7.2, 3 is a primitive root modulo \( 5^2 \). Since 3 is odd, by Exercise #14 in §7.2, 3 is also a primitive root modulo 50 = \( 2 \cdot 5^2 \).

Then a set of mutually incongruent primitive roots modulo 50 can be \( 3^k \) where \( \gcd(k, 20) = 1 \), i.e., \( 3, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17} \), and \( 3^{19} \).

3. If \( x^4 - 4 \equiv 0 \pmod{p} \), then \( p \mid (x^2 + 2)(x^2 - 2) \). Thus either \( x^2 \equiv 2 \pmod{p} \) or \( x^2 \equiv -2 \pmod{p} \). For both to have no solution, we need \( \left( \frac{2}{p} \right) = -1 \) and \( \left( \frac{-2}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{2}{p} \right) = -1 \). This happens if and only if \( p \) is of the form \( 8k + 5 \).

Assume there are only finitely many prime numbers that are congruent to 5 modulo 8. Call them \( p_1, \ldots, p_r \). Consider \( N = (p_1 p_2 \ldots p_r)^2 + 4 \). Then \( N \equiv 5 \pmod{8} \). If \( p \mid N \) is a prime factor, then \( (p_1 p_2 \ldots p_r)^2 \equiv -4 \pmod{p} \). Therefore \( \left( \frac{-1}{p} \right) = 1 \) which means \( p \equiv 1 \pmod{8} \) or \( p \equiv 5 \pmod{8} \). However \( N \equiv 5 \pmod{8} \). Therefore it has at least one prime factor \( q \) such that \( q \equiv 5 \pmod{8} \). By assumption, \( q \mid p_1 p_2 \ldots p_r \) and \( q \mid N \). Thus \( q \mid 4 \), which is a contradiction.

4. (1) Let \( A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \). Then \( A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \). Now

\[
\begin{pmatrix} F_{kn+1} & F_{kn} \\ F_{kn} & F_{kmn-1} \end{pmatrix} = A^{kn} = A^{(k-1)n} \cdot A^n = \begin{pmatrix} F_{(k-1)n+1} & F_{(k-1)n} \\ F_{(k-1)n} & F_{(k-1)n-1} \end{pmatrix} \cdot \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.
\]

Compare the (1,2)-entry on both sides we get \( F_{kn} = F_{(k-1)n+1} \cdot F_n + F_{(k-1)n} \cdot F_{n-1} \). Now use induction (use the hypothesis \( F_n \mid F_{(k-1)n} \) to show \( F_n \mid F_{kn} \)) to finish the proof.

(2) If \( n \) has any odd factor, then clearly by (1) \( n \) must be (an odd) prime. If \( n = 2^k \), the only possibility is \( n = 4 \) (\( F_4 = 2 \)).

5. (1) If \( x^p + 1 \equiv 0 \pmod{p^3} \), then \( x^p + 1 \equiv 0 \pmod{p} \). By Fermat’s Theorem we have \( x+1 \equiv 0 \pmod{p} \), so \( x = -1 + kp \) for some \( k \). Now \( (-1 + kp)^p = (-1)^p + p(-1)^{p-1}(kp) + \ldots \equiv -1 + kp^2 \pmod{p^3} \). So it satisfies \( x^p + 1 \equiv 0 \pmod{p^3} \) if and only if \( p^3 \mid kp^2 \), which means \( p \mid k \). But now all numbers \(-1 + rp^2 \ (r = 0, 1, \ldots, p - 1) \) are mutually incongruent modulo \( p^3 \), and check they are all solutions of \( x^p + 1 \equiv 0 \pmod{p^3} \). So the equation has \( p \) mutually incongruent solutions.

(2) First look at the equation \( x^p + x - 1 \equiv 0 \pmod{p} \). By Fermat’s Theorem \( x^p \equiv x \pmod{p} \). So the equation is \( 2x - 1 \equiv 0 \pmod{p} \) which has a unique solution \( m \equiv \frac{p+1}{2} \pmod{p} \). Now \( (x^p + x - 1)' = px^{p-1}+1 \), so \( p \mid (x^p + x - 1)' \mid x = m \). Therefore by Exercise 3 and 4 in §5.4, there exists a unique \( r \pmod{p} \) such that \( m + pr \) is a solution of \( x^p + x - 1 \equiv 0 \pmod{p^3} \). Do the process one more time to show that the solution exists and is unique (up to congruence modulo \( p^3 \)).

(3) None. If \( a^p - a + 1 \equiv 0 \pmod{p^3} \), then \( a^p - a + 1 \equiv 0 \pmod{p} \). But by Fermat’s theorem \( a^p \equiv a \pmod{p} \). So we have \( 1 \equiv 0 \pmod{p} \) which is a contradiction.
6. The function \( \mu(n) \cdot d^2(n) \) is multiplicative. Therefore \( \sum_{e \mid n} \mu(e) d^2(e) \) is also multiplicative. If \( n = p^k \) where \( p \) is prime, then \( \sum_{e \mid n} \mu(e) d^2(e) = \mu(1) \cdot d^2(1) + \mu(p) \cdot d^2(p) = 1 + (-1) \cdot 2^2 = -3 \). Therefore if \( n = p_1^{k_1} \cdots p_r^{k_r} \), then \( \sum_{e \mid n} \mu(e) d^2(e) = (-3)^r \). For this to be greater than 2018 (3^6 < 2018 < 3^7), the smallest \( r \) is 8 (when \( r = 7 \) the sum is negative). So the smallest \( n \) is \( 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9699690 \).

7. (1) No. If \( d = ab \), then \(-1 = \left( \frac{d}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \) so \( \left( \frac{a}{p} \right) = -1 \) or \( \left( \frac{b}{p} \right) = -1 \). So by assumption \( d \) must be prime.

   (2). Check all primes less than 100 with \( \left( \frac{2}{p} \right) = \left( \frac{3}{p} \right) = 1 \). Then \( p \equiv \pm 1 \pmod{24} \). So \( p = 23, 47, 71, 73 \) or 97. Among those, all have \( \left( \frac{2}{p} \right) = -1 \) (in other words, \( d = 5 \)) except 71. So \( p = 71 \) and check in this case \( d = 7 \).

   (3). Note that for \( d = 7 \), a mutually incongruent set of primitive roots are 3 and 5. Both satisfy \( \left( \frac{n}{71} \right) = 1 \). So we need to look at the numbers \( 7k + 3 \) or \( 7k + 5 \) with \( k > 0 \). The first among such numbers that satisfies \( \left( \frac{n}{71} \right) = -1 \) is \( n = 17 \). Note that this does not guarantee that 17 is a primitive root modulo 71 (See Problem 1 part 2). However this shows (by Theorem 9.2) the order of 17 modulo 71 (which must divide \( \varphi(71) = 70 \)) is not 35 nor any factor of 35 (so cannot be 1, 5 or 7), and cannot be 2 since 17 \( \equiv \pm 1 \pmod{71} \). So we only need to check if the order can be 10 (which is equivalent to 17^5 \( \equiv -1 \pmod{71} \)), or if the order can be 14 (which is equivalent to 17^7 \( \equiv -1 \pmod{71} \)). Here indeed 17^5 \( \equiv -1 \) (as 17^2 = 289 \( \equiv 5 \), so 17^5 \( \equiv 5^2 \cdot 17 = 425 = 71 \cdot 6 - 1 \equiv -1 \pmod{71} \)). So 17 is not a primitive root modulo 71. The next \( n \) satisfies \( \left( \frac{n}{71} \right) = -1 \) is 26, but 26^7 \( \equiv -1 \pmod{71} \). It turns out the next such number \( n = 31 \) is a primitive root for both 7 and 71. (You get full credit for this part if you check the case for \( n = 17 \).)

   (4). None of the numbers is a sum of two squares by Theorem 11.1. The numbers \( p = 71 \) and \( d = 7 \) are of the form \( 8k + 7 \) so they cannot be sum of three squares. However \( pd = 497 \) can be written as sum of three squares. For example 497 = \( 2^2 + 3^2 + 22^2 \). Finally any positive number is a sum of four squares.

8. Let \( p = 2n + 1 \). Since \( p \equiv 7 \pmod{8} \), we have \( \left( \frac{2}{p} \right) = 1 \) and \( \left( \frac{-1}{p} \right) = -1 \). Now

\[
\sum_{k=1}^{2n} k \left( \frac{k}{p} \right) = \sum_{k=1}^{n} k \left( \frac{k}{p} \right) + \sum_{k=n+1}^{2n} k \left( \frac{k}{p} \right) \\
= \sum_{k=1}^{n} k \left( \frac{k}{p} \right) + \sum_{k=1}^{n} (p - k) \left( \frac{p - k}{p} \right) \\
= \sum_{k=1}^{n} k \left( \frac{k}{p} \right) \cdot (1 - \left( \frac{-1}{p} \right)) + p \sum_{k=1}^{n} \left( \frac{k}{p} \right) \cdot \left( \frac{-1}{p} \right) \\
= 2 \sum_{k=1}^{n} k \left( \frac{k}{p} \right) - p \sum_{k=1}^{n} \left( \frac{k}{p} \right).
\]
On the other hand
\[
\sum_{k=1}^{2n} k \left( \frac{k}{p} \right) = \sum_{k \text{ even}} k \left( \frac{k}{p} \right) + \sum_{k \text{ odd}} k \left( \frac{k}{p} \right)
\]
\[
= \sum_{k=1}^{n} 2k \left( \frac{2k}{p} \right) + \sum_{k=1}^{n} (p - 2k) \left( \frac{p - 2k}{p} \right)
\]
\[
= \sum_{k=1}^{n} 2k \left( \frac{k}{p} \right) \left( \frac{2}{p} \right) \cdot \left( 1 - \left( \frac{-1}{p} \right) \right) + p \sum_{k=1}^{n} \left( \frac{k}{p} \right) \cdot \left( \frac{-1}{p} \right) \cdot \left( \frac{2}{p} \right)
\]
\[
= 4 \sum_{k=1}^{n} k \left( \frac{k}{p} \right) - p \sum_{k=1}^{n} \left( \frac{k}{p} \right).
\]
Subtract these two lines we get
\[
\sum_{k=1}^{n} k \left( \frac{k}{p} \right) = 0.
\]

9. Note that \( \sum_{n=1}^{p-2} \left( \frac{n(n+1)}{p} \right) = \sum_{n=0}^{p-1} \left( \frac{n(n+1)}{p} \right) = -1 \) by Theorem 10.3, we have
\[
N(p) = \frac{1}{p} \sum_{n=1}^{p-2} \left( 1 - \left( \frac{n}{p} \right) \right) \cdot \left( 1 + \left( \frac{n+1}{p} \right) \right) + \frac{1}{p} \sum_{n=1}^{p-2} \left( 1 + \left( \frac{n}{p} \right) \right) \cdot \left( 1 - \left( \frac{n+1}{p} \right) \right)
\]
\[
= \frac{1}{4} \sum_{n=1}^{p-2} \left( 2 - 2 \left( \frac{n(n+1)}{p} \right) \right)
\]
\[
= \frac{1}{4} \sum_{n=1}^{p-2} \left( 2 - \frac{n(n+1)}{p} \right)
\]
\[
= \frac{1}{2}(p - 2) - \frac{1}{2} \sum_{n=1}^{p-2} \left( \frac{n(n+1)}{p} \right)
\]
\[
= \frac{1}{2}(p - 2) - \frac{1}{2}(-1)
\]
\[
= \frac{1}{2}(p - 1).
\]
For \( p = 101 \), this is equal to 50, as expected.