1. (10 points) True or False. Determine if the following statement are true. If true, give a proof. If false, give a counter-example.

(1). Let \( p \) be prime. Then the equation \( x^p + x \equiv 304 \pmod{p^p} \) has solution.

(2). Let \( n = 2^{2k+1} \) where \( k > 0 \). Then \( n \) cannot be written as a sum of squares of four positive integers.

2. (10 points) Find 3 mutually incongruent primitive roots modulo 98.

3. (10 points) Show that there exists infinitely many prime numbers \( p \) such that both \( x^2 + 1 \equiv 0 \pmod{p} \) and \( x^2 + 2 \equiv 0 \pmod{p} \) have solutions.

4. (10 points) Does the equation \( x^4 + 69x^2 - 21 \equiv 0 \pmod{73} \) have any solution? Explain your answer.

5. (10 points) Recall that Fibonacci numbers are defined as \( F_1 = 1, F_2 = 1 \) and \( F_{n+1} = F_n + F_{n-1} \) for all \( n \geq 2 \). Show that for all \( n \geq 2 \), we have \( F_{n+5} > 10F_n \).

6. (10 points) Let \( n = 360 \). Find the minimal \( \alpha > 0 \) such that

\[
\sum_{\substack{d|n^\alpha \\text{d} > 0}} \frac{\phi(d)}{d}
\]

is an integer.

7. (10 points) Find all solutions of \( x^2 + y^2 = (110 \cdot 304)^2 \) where \( xy \neq 0 \).

8. (10 points) Let \( n > 1 \) be odd. Show that

\[
n \text{ has no primitive roots if and only if } \prod_{\substack{d|n \\text{d} > 0}} d^{\mu(d)} = 1.
\]

9. (10 points) Let \( p > 3 \) be prime. Do the following equations have solutions? Explain your answers.

(1). \( 2x^2 - 3y^2 \equiv 2019 \pmod{p} \).

(2). \( x^{2020} \equiv g \pmod{p} \) where \( g \) is a primitive root modulo \( p \).

10. (10 points) Let \( p \equiv 3 \pmod{8} \) be prime. Let \( N(p) \) be the number of consecutive pairs of quadratic residues modulo \( p \) in the interval \([1, p-1]\). Let \( \nu(p) \) be the number of consecutive triples of quadratic residues modulo \( p \) in the interval \([1, p-1]\). Show that \( N(p) = 2\nu(p) \).

Solutions on next page.
Solutions:

1. (1). True. First look at the equation \( x^p + x - 304 \equiv 0 \) (mod \( p \)). By Fermat’s Theorem \( x^p \equiv x \) (mod \( p \)). So the equation is \( 2x - 304 \equiv 0 \) (mod \( p \)) which has a unique solution \( m \equiv 152 \) (mod \( p \)). Now \( (x^p + x - 304)' = px^{p-1} + 1 \), so \( p \not| (x^p + x - 1)' \) for any \( x \). Therefore by Exercise 3 and 4 in §5.4, there exists a unique \( r \) (mod \( p \)) such that \( m + pr \) is a solution of \( x^p + x - 304 \equiv 0 \) (mod \( p^2 \)). Keep doing the process to show that the solution exists and is unique (up to congruence modulo \( p^2 \)).

(2). True. If \( 2^{2k+1} = a_2^2 + b_2^2 + c_2^2 + d_2^2 \) where \( abcd \not= 0 \), then \( a, b, c, d \) are all even. Otherwise \( a^2 + b^2 + c^2 + d^2 \) is either \( 4m + 2 \) or \( 8m + 4 \), but \( 8|2^{2k+1} \). Now consider \( (\frac{a}{2})^2 + (\frac{b}{2})^2 + (\frac{c}{2})^2 + (\frac{d}{2})^2 = 2^{2(k-1)}-1 \), use induction to see there is no such solution.

2. Direct computation to check that \( 3 \) is a primitive root modulo \( 7 \), and that \( 3^{7-1} \not= 1 \) (mod \( 7^2 \)). Therefore by Exercise #12 in §7.2, \( 3 \) is a primitive root modulo \( 7^2 \). Since \( 3 \) is odd, by Exercise #14 in §7.2, \( 3 \) is also a primitive root modulo \( 98 = 2 \cdot 7^2 \). To get three mutually incongruent primitive roots, we can use \( 3, 3^3 \) and \( 3^{11} \) (note \( \phi(98) = 42 \)).

3. For both to have solutions, we need \( (\frac{-1}{p}) = 1 \) and \( (\frac{2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = 1 \). So \( (\frac{2}{p}) = 1 \). This happens if and only if \( p \equiv 1 \) (mod \( 8 \)).

Assume there are only finitely many prime numbers that are congruent to \( 1 \) modulo \( 8 \). Call them \( p_1, \ldots, p_r \). Consider \( N = (2p_1p_2 \cdots p_r)^4 + 1 \). Then \( N \equiv 1 \) (mod \( 8 \)). If \( p | N \) is a prime factor and \( p \) is not one of \( p_i \)’s above, then \( ((2p_1p_2 \cdots p_r)^2) \equiv -1 \) (mod \( p \)). Therefore \( (\frac{-1}{p}) = 1 \) which means \( p \equiv 1 \) (mod \( 4 \)). But now \( \frac{p-1}{4} \) is an integer and \( (\frac{-1}{p}) \equiv ((2p_1p_2 \cdots p_r)^4)^{\frac{p-1}{4}} \equiv (2p_1p_2 \cdots p_r)^{p-1} \equiv 1 \) (mod \( p \)) by Fermat’s theorem. If \( \frac{p-1}{4} \) is odd, then \( -1 \equiv 1 \) (mod \( p \)), which is a contradiction since \( p \) is odd. Therefore \( \frac{p-1}{4} \) is even which means \( p \equiv 1 \) (mod \( 8 \)). By assumption, \( p = p_i \) for some \( 1 \leq i \leq r \). A contradiction.

4. The equation is the same as \( x^4 - 4x^2 - 21 \equiv (x^2 + 3)(x^2 - 7) \equiv 0 \) (mod \( 73 \)). It has solution if either \( (\frac{2}{73}) = 1 \) or \( (\frac{7}{73}) = 1 \). Check directly that \( (\frac{7}{73}) = 1 \). So it has a solution. (In fact, \( x = 17 \) is a solution.)

5. Use induction. Check directly it is true for \( n = 2 \) and \( n = 3 \). Now assume the statement is true for all numbers up to \( n \), then \( F_{n+1} + 1 = F_{n+1} + F_{n+1} > 10F_n + 10F_{n-1} = 10F_{n+1} \) (the next to last step is by induction).

6. The function \( \frac{\phi(d)}{d} \) is multiplicative. Therefore \( \sum_{d | n} \frac{\phi(d)}{d} \) is also multiplicative. If \( n = p^r \) where \( p \) is prime, then

\[
\sum_{d \mid n} \frac{\phi(d)}{d} \phi(p) + \cdots + \frac{\phi(p^r)}{p^r} = 1 + r \cdot \frac{p-1}{p} \cdot \frac{p}{p} = \frac{p + (p-1)r}{p}.
\]

Therefore if \( n^\alpha = 360^\alpha = 2^3 \cdot 3 \cdot 5^\alpha \), then

\[
\sum_{d \mid n^\alpha} \frac{\phi(d)}{d} = \frac{2 + 3\alpha}{2} \cdot \frac{3 + 4\alpha}{3} \cdot \frac{5 + 4\alpha}{5}.
\]

For this to an integer, check that the smallest possible \( \alpha \) is 6.

7. \( (110 \cdot 304)^2 = 2^{10} \cdot 5^2 \cdot 11^2 \cdot 19^2 \). If \( (x, y) \) is a solution then both \( x \) and \( y \) are even. Consider \( (\frac{x}{n}, \frac{y}{n}) \) and check again, and so on, we see that \( 32 | x \) and \( 32 | y \). Also \( x^2 + y^2 \equiv 0 \) (mod 11). If the solution is not trivial (modulo 11) then we will get \( (\frac{x}{11}) = 1 \) which is not true. So \( 11 \mid x \) and \( 11 \mid y \). Similar argument shows that \( 19 \mid x \) and \( 19 \mid y \). Let \( n = 19 \cdot 11 \cdot 19 \), then \( n \mid x \) and \( n \mid y \). Let \( w = \frac{x}{n} \) and \( t = \frac{y}{n} \), then \( w^2 + t^2 = 5^2 \). Now you can find all the solutions.
8. Since \( n \) is odd, write \( n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r} \) where \( p_i \) are distinct odd prime numbers. Then \( n \) has no primitive root if and only if \( r \geq 2 \).

If \( r = 1 \), then \( n = p^a \). It is easy to compute that

\[
\prod_{d \mid n} d^{\mu(d)} = 1^{\mu(1)} \cdot p^{\mu(p)} = \frac{1}{p} \neq 1 .
\]

Now let \( r \geq 2 \). Note that any \( d \) with 2 or high power for any \( p_i \) will have \( d^{\mu(d)} = d^0 = 1 \), so does not matter in the product. Therefore let \( m = p_1 p_2 \cdots p_r \), then

\[
\prod_{d \mid n} d^{\mu(d)} = \prod_{d \mid m} d^{\mu(d)} .
\]

Now let \( p \mid m \) and write \( m = p \cdot m_1 \), then \( p \nmid m_1 \) and \( m_1 > 1 \). Note that if \( p \nmid k \) then \( \mu(pk) = -\mu(k) \). From this we observe that the exponential of \( p \) in the product \( \prod_{d \mid m} d^{\mu(d)} \) is

\[
- \sum_{d \mid m_1} \mu(d) = (-1) \cdot 0 = 0
\]

by Theorem 6.5 since \( m_1 > 1 \). Therefore \( \prod_{d \mid m} d^{\mu(d)} = p_1^0 \cdot p_2^0 \cdots p_r^0 = 1 \).

9. (1). Yes. This is a special case of the example in class that the equation \( ax^2 + by^2 \equiv n \) \((\text{mod} \ p)\) always has solutions if \( p \nmid \text{ab} \). Or to prove directly: multiply \( \frac{1}{p}x^2 \) on both sides, we see that to solve the original equation, it is equivalent to solve

\[
x^2 \equiv \frac{3(1 - p)}{2} y^2 + \frac{2019(1 - p)}{2} \pmod{p} .
\]

Check that \( \frac{3(1-p)}{2} y_1^2 + \frac{2019(1-p)}{2} \equiv \frac{3(1-p)}{2} y_2^2 + \frac{2019(1-p)}{2} \pmod{p} \) if and only if \( y_1 \equiv \pm y_2 \pmod{p} \). Therefore when \( y \) goes through all values modulo \( p \), there are \( \frac{p-1}{2} + 1 = \frac{p+1}{2} \) values of \( \frac{3(1-p)}{2} y^2 + \frac{2019(1-p)}{2} \). Since there are only \( \frac{p+1}{2} \) quadratic non-residues modulo \( p \), there must exist \( y \) such that \( \frac{3(1-p)}{2} y^2 + \frac{2019(1-p)}{2} \) is a quadratic residue.

(2). No. Note that \( p - 1 \) is even. If \( a^{2020} \equiv g \pmod{p} \), then

\[
g^{\frac{p-1}{2}} \equiv (a^{2020})^{\frac{p-1}{2}} \equiv (a^{p-1})^{1010} \equiv 1 \pmod{p}
\]

which is a contradiction since \( g \) is a primitive root modulo \( p \).

10. Let \( p = 8k + 3 \). We know \( \left( -\frac{1}{p} \right) = -1, \left( \frac{2}{p} \right) = -1 \) and \( \left( \frac{2}{p} \right) = 1 \). From Theorem 10.1 in §10.1, we have

\[
N(p) = \frac{1}{4} (p - 4 - \left( -\frac{1}{p} \right)) = \frac{1}{4} (8k + 3 - 4 + 1) = 2k .
\]

On the other hand, from Theorem 10.4 in §10.2 and use Theorem 10.3, we have

\[
\nu(p) = \frac{1}{8} \sum_{n=1}^{p-3} \left( 1 + \left( \frac{n}{p} \right) \right) \cdot \left( 1 + \left( \frac{n+1}{p} \right) \right) \cdot \left( 1 + \left( \frac{n+2}{p} \right) \right)
\]

\[
= \frac{1}{8} (p - 3) - \frac{1}{8} \left( \left( \frac{-2}{p} \right) - \left( -\frac{1}{p} \right) \right) - \frac{1}{8} \left( \left( \frac{-1}{p} \right) - \left( -\frac{1}{p} \right) \right) - \frac{1}{8} \left( \left( \frac{1}{p} \right) - \left( 0 \right) \right) - \frac{1}{8} \left( \left( \frac{1}{p} \right) - \left( 1 \right) \right) + \frac{1}{8} S(1)
\]

\[
= \frac{1}{8} (8k + 3 - 3 + 0 + 0 + 0 + 0 + 0 + 0) + \frac{1}{8} S(1)
\]

\[
= k + \frac{1}{8} S(1)
\]

Since \( p \equiv 3 \pmod{4} \), from the proof of Theorem 10.4 we have \( S(1) = 0 \). Therefore \( \nu(p) = k \) and so \( N(p) = 2 \nu(p) \).