110.304 Midterm II
November 15, 2018 (75 minutes)

In this exam all variables are integers. Solutions mean integer solutions.

1. (25 points) True or False. Determine if the following statements are true. Explain your answers.
   (1). Let \( p \) be an odd prime number. Let \( g \) and \( h \) be primitive roots modulo \( p \). Then \( gh \) is a quadratic residue modulo \( p \).
   (2). Let \( p \) be an odd prime number. Let \( g \) be a primitive root modulo \( p \). Then \(-g\) is a primitive root modulo \( p \) if and only if \( p \equiv 1 \pmod{4} \).

2. (25 points) Show that there are infinitely many prime numbers \( p \) such that
   \[ x^4 + 1 \equiv (x^2 - ax + 1)(x^2 + ax + 1) \pmod{p}, \]
   for some \( a \).

3. (25 points) For any \( n > 1 \), define
   \[ f(n) = \sum_{1 \leq d \leq n, \gcd(d, n) = 1} d. \]
   If \( f(m) = f(n) \), show that \( m = n \).

4. (25 points) How many mutually incongruent solutions (or pair of solutions) do the following equations have? Explain your answers.
   (1). \( x^5 - x + 1 \equiv 0 \pmod{125} \).
   (2). \( 23x^2 - 29y^2 = 1 \).

Solutions on next page
Solutions:

1. (1). True. \( h \equiv g^r \) where \( r \) must be odd since otherwise \( h \) is quadratic residue, thus not a primitive root. Then \( gh \equiv g^{r+1} \) is a quadratic residue since \( r + 1 \) is even.

   (2). True. Note that \(-g \equiv g^{\frac{p+1}{2}} \cdot g \equiv g^{\frac{p+1}{2}} \pmod{p}\). It is a primitive root mod \( p \) if and only if \( \gcd\left(\frac{p+1}{2}, p-1\right) = 1 \). If \( p = 4k + 1 \), this is \( \gcd(2k + 1, 4k) = 1 \). If \( p = 4k + 3 \) then both numbers are even so they are not co-prime.

2. From the assumption, the coefficient of \( x^2 \) is \( 1 + 1 - a^2 \equiv 0 \pmod{p} \) which means \((\frac{2}{p}) = 1 \). So \( p \equiv 1 \pmod{8} \) or \( p \equiv 7 \pmod{8} \). If \( p \equiv 7 \pmod{8} \) this is the only possibility of factorization.

   To show there exists infinitely many prime number of \( 8k + 7 \): Assume there are only finitely many prime numbers that are congruent to \( 7 \) modulo \( 8 \). Call them \( p_1, \ldots, p_r \). Consider \( N = (p_1p_2 \ldots p_r)^2 - 2 \). Then \( N\equiv 7 \pmod{8} \).

   If \( p \mid N \) is a prime factor, then \( (p_1p_2 \ldots p_r)^2 \equiv 2 \pmod{p} \). Therefore \((\frac{2}{p}) = 1 \) which means \( p \equiv 1 \pmod{8} \) or \( p \equiv 7 \pmod{8} \). However \( N\equiv 7 \pmod{8} \). Therefore it has at least one prime factor \( q \) such that \( q \equiv 7 \pmod{8} \).

   By assumption, \( q \mid p_1p_2 \ldots p_r \) and \( q \mid N \). Thus \( q \mid 2 \) which is a contradiction

3. Note that \( \gcd(d, n) = 1 \) if and only if \( \gcd(n - d, n) = 1 \). So

\[
    f(n) = \sum_{1 \leq d \leq n} d = \frac{1}{2} \left[ \sum_{1 \leq d \leq n} d + \sum_{1 \leq d \leq n} (n - d) \right] = \frac{1}{2} n \varphi(n).
\]

Therefore we need to show that if \( n \varphi(n) = m \varphi(m) \), we have \( n = m \). Let \( n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \) and \( m = p_1^{\beta_1} \cdots p_r^{\beta_r} \). Here \( p_1 < p_2 < \cdots < p_r \) are prime numbers, and all \( \alpha_i \geq 0 \) and \( \beta_i \geq 0 \) (but not both 0). If \( \alpha_r = 0 \), then \( \beta_r > 0 \), so \( p_r \nmid n \varphi(n) \) but \( p_r \mid m \varphi(m) \), a contradiction. So \( \alpha_r > 0 \) and \( \beta_r > 0 \). Then \( n \varphi(n) = (\ldots)p_r^{2\alpha_r - 1}(p_r - 1) \) and \( m \varphi(m) = (\ldots)p_r^{2\beta_r - 1}(p_r - 1) \). Compare the exponents of \( p_r \), we have \( \alpha_r = \beta_r \). Now cancel the \( p_r^{2\alpha_r - 1} \) part and prove inductively that all \( \alpha_i = \beta_i \) for all \( i \). So \( n = m \).

4. (1). None. If \( a^5 - a + 1 \equiv 0 \pmod{125} \), then \( a^5 - a + 1 \equiv 0 \pmod{5} \). But by Fermat’s theorem \( a^5 \equiv a \pmod{5} \). So we have \( 1 \equiv 0 \pmod{5} \) which is a contradiction.

   (2). None. If \((a, b)\) is a solution, then \(-29b^2 = 1 - 23a^2 \equiv 1 \pmod{23} \). Therefore \((-29b)^2 \equiv -29 \pmod{23} \), which means \((-\frac{29}{23}) = 1 \). However \((-\frac{29}{23}) = (-\frac{6}{23}) = \left(\frac{1}{23}\right) \cdot \left(\frac{2}{23}\right) \cdot \left(\frac{3}{23}\right) = (-1) \cdot 1 \cdot 1 = -1 \). A contradiction. Therefore the equation has no solution. [Another way: consider modulo 4, then we have \( x^2 + y^2 \equiv -1 \pmod{4} \). Check directly this is impossible.]