Record multiple choice answers below

(1) (A)  ☐  (C)  (D)  (E)  (F)
(2) (A)  (B)  ☐  (D)  (E)  (F)
(3) (A)  (B)  (C)  (D)  ☐  (F)
(4) (A)  (B)  (C)  (D)  (E)  ☐
(5) (A)  (B)  (C)  (D)  ☐  (F)
(6) ☐  (B)  (C)  (D)  (E)  (F)
(7) (A)  (B)  (C)  (D)  ☐  (F)
(8) (A)  ☐  (C)  (D)  (E)  (F)
(9) (A)  (B)  (C)  (D)  (E)  ☐
(10) ☐  (B)  (C)  (D)  (E)  (F)
Multiple Choice Section

Each question in this section is worth 5 points. You can write on these pages. Mark the answers on the right for your own use. Record the answers on page 1 for grading.

(1) 105 ≡ _____ (mod 13)
   (A) 6  (B) 7  (C) 5  (D) 9  (E) None of these.

\[ 105 \equiv 13 \times 8 + 1 \]

(2) \( \phi(407) = _____ \)
   (A) 280  (B) 416  (C) 360  (D) 400  (E) 450  (F) None of these.

\[ 407 = 11 \times 37 \]
\[ \phi(407) = \phi(11) \phi(37) = 10 \times 36 = 360 \]

(3) If \( a \equiv 2 \) (mod 6) and \( b \equiv 3 \) (mod 6), then \( 11a - 4b \equiv _____ \) (mod 6).
   (A) 0  (B) 1  (C) 2  (D) 3  (E) 4  (F) None of these.

\[ 11a - 4b \equiv 11 \times 2 - 4 \times 3 \equiv 10 \equiv 4 \pmod{6} \]

(4) If \( a \equiv -2 \) (mod 7), then \( a^{2017} \equiv _____ \) (mod 7)
   (A) 0  (B) 1  (C) 2  (D) 3  (E) 4  (F) None of these.

Since 7 \( \nmid a \), By Fermat's Thm,
\[ a^{6} \equiv 1 \pmod{7} \]

So \[ a^{2017} = a^{2016+1} = 6 \times 336 + 1 \equiv a \equiv 5 \pmod{7} \]
(5) Which of the following is NOT a **complete residue system** modulo 7?

(A) \{0, 1, 2, 3, 4, 5, 6\}  
(B) \{5, 6, 7, 8, 9, 10, 11\}  
(C) \{6, 10, 15, 20, 25, 30\}  
(D) \{-15, -13, -5, 7, 10, 18, 26\}  
(E) \{2, 4, 8, 16, 32, 64, 128\}  
(F) none of these.

\[ 2 \equiv 16 \pmod{7} \]

(6) Which of the following is NOT a **reduced residue system** modulo 8?

(A) \{1, 1, 11^2, 11^3\}  
(B) \{1, 3, 5, 7\}  
(C) \{-15, -5, 5, 15\}  
(D) \{3, 9, 15, 21\}  
(E) \{-3, -1, 1, 3\}  
(F) none of these.

\[ 1 \equiv 11^2 \pmod{8} \]

(7) The exponent of 7 in the canonical representation of 50! is 

(A) 4  
(B) 5  
(C) 6  
(D) 7  
(E) 8  
(F) none of these.

\[ \left[ \frac{50}{7} \right] + \left[ \frac{50}{7^2} \right] = 7 + 1 = 8 \]
(8) Which of the following is not a primitive Pythagorean triple?

(A) (7, 24, 25)  (B) (13, 84, 87)  (C) (33, 56, 65)  (D) (20, 21, 29)  (E) (28, 45, 53)  (F) none of these.

\[ 1^2 + 6^2 = 8^2 \]

(9) Which of the following statement is **FALSE**?

(A) If \( a \) is coprime with \( b \), then \( a^3 \) is coprime with \( b^2 \).

(B) If \( ac \equiv bc \pmod{mc} \), then \( a \equiv b \pmod{m} \).

(C) If \( p \) is an odd prime, then \( 2^{p-1} \equiv 1 \pmod{p} \).

(D) If \( 2^n - 1 \) is a prime, then \( 2^{n-1}(2^n - 1) \) is a perfect number.

(E) If \( 2^n - 1 \) is a prime, then \( p \) is also a prime.

(F) If \( p \) is a prime, then \( 2p + 1 \) is also a prime.

\[ T \triangleq 7 \quad 2p+1 = 15 \sim \text{(composite)} \]

(10) This question is about the primality tests of Fermat and Miller. Which one of the following statements is **TRUE**?

(A) There are infinitely many Carmichael numbers.

(B) There exists a number \( n \) which passes Miller’s test to every base coprime with \( n \).

(C) Pseudoprimes to base \( a \) are also strong pseudoprimes to base \( a \).

(D) If a number \( n \) passes Miller’s test to some base \( a \), then \( n \) must be a prime.

(E) If \( n \) passes Fermat’s test to some base \( a \), then \( n \) also passes Miller’s test to base \( a \).

(F) none of these.
"Show work" for full credit problems

1 (15 pts) What is the remainder when 1234321 is divided by 17?

Note that \[ 1234 \equiv 17 \times 72 + 10 \]

So \[ 1234^{4321} \equiv 10^{9321} \pmod{17} \]

By Fermat's thm. \[ 10^{16} \equiv 1 \pmod{17} \]

So \[ 10^{9321} = 10^{16 	imes 580 + 1} = (10^{16})^{580} \cdot 10 \equiv 10 \pmod{17} \]

Hence the remainder is 10.

2 (15 pts) Show that 124 is a pseudoprime to base 5.

124 = 31 \times 2^2 is not a prime.

All we need to check is that \[ 5^{123} \equiv 1 \pmod{124} \]

But note that \[ 5^3 = 125 \equiv 1 \pmod{124} \]

So \[ 5^{123} = 5^3 \cdot 41 = (5^3)^4 \cdot 1 \equiv 1 \pmod{124} \]

Thus 124 is a pseudoprime to base 5.
3 (15 pts) Show that the numbers $5, 5^2, 5^3, 5^4, 5^5, 5^6$ form a reduced residue system modulo 7.

Since $\phi(7) = 7 - 1 = 6$, the set has the right number of elements. Also since $(5, 7) = 1$, it follows that all the numbers $5, 5^2, 5^3, \ldots, 5^6$ are coprime with 7. Moreover we check that modulo 7:

$5 \equiv 5, \quad 5 \cdot 2 \equiv 4, \quad 5 \cdot 3 \equiv 6, \quad 5 \cdot 4 \equiv 2, \quad 5 \cdot 5 \equiv 3, \quad 5 \cdot 6 \equiv 1.$

So they form a reduced residue system.

4 (5 pts) Show that $7x^3 + 2 = y^3$ has no solution in integers. Assume $x, y \in \mathbb{Z}$.

Since $0^3 \equiv 0 \pmod{7}, \quad 1^3 \equiv 1 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}, \quad 3^3 \equiv 6 \pmod{7}$

$4^3 \equiv 1 \pmod{7}, \quad 5^3 \equiv 6 \pmod{7}, \quad 6^3 \equiv 6 \pmod{7}$

It follows that $x^3 \equiv 0, 1, 6 \pmod{7}$ and $y^3 \equiv 0, 1, 6 \pmod{7}$.

Then $7x^3 + 2 \equiv 2 \pmod{7}$

So for all $x, y \in \mathbb{Z}$, we have

$7x^3 + 2 \equiv y^3 \pmod{7}$

Contradiction. So there does not exist solution in integers.
Record multiple choice answers below

(1) (A) (B) (C) (D) (E) (F)
(2) ( ) (B) (C) (D) (E) (F)
(3) (A) (B) (C) (D) (E) (F)
(4) (A) (B) (C) (D) (E) (F)
(5) (A) (B) (C) (D) (E) (F)
(6) (A) (B) (C) (D) (E) (F)
(7) (A) (B) (C) (D) (E) (F)
(8) (A) (B) (C) (D) (E) (F)
(9) (A) (B) (C) (D) (E) (F)
(10) (A) (B) (C) (D) (E) (F)
Multiple Choice Section

Each question in this section is worth 5 points. You can write on these pages. Mark the answers on the right for your own use. Record the answers on page 1 for grading.

(1) $113 \equiv \underline{\phantom{10}} \pmod{13}$
(A) 6  (B) 1  (C) 7  (D) 5  (E) 3  (F) none of these.

$$113 = 13 \times 8 + 9.$$ 

(2) $\varphi(319) = \underline{\phantom{10}}$
(A) 280  (B) 416  (C) 360  (D) 400  (E) 450  (F) none of these.

$$319 = 11 \times 29$$

$$\varphi(319) = ((11-1) \times (29-1)) = 10 \times 28 = 280$$

(3) If $a \equiv 2 \pmod{7}$ and $b \equiv 3 \pmod{7}$, then $11a - 4b \equiv \underline{\phantom{10}} \pmod{7}$.
(A) 0  (B) 1  (C) 2  (D) 3  (E) 4  (F) none of these.

$$11a - 4b \equiv 11 \times 2 - 4 \times 3 \equiv 10 \equiv 3 \pmod{7}$$

(4) If $a \equiv -7 \pmod{9}$, then $a^{2017} \equiv \underline{\phantom{10}} \pmod{9}$
(A) 0  (B) 1  (C) 2  (D) 3  (E) 4  (F) none of these.

$$\varphi(a) = 9 \times \frac{2}{3} = 6.$$ By Euler's theorem, $a^6 \equiv 1 \pmod{9}$

So $a^{2017} \equiv a^{2016+1} \equiv a^1 \equiv a \equiv 2 \pmod{9}$
(5) Which of the following is **NOT** a *complete residue system* modulo 7?

(A) \{0, 1, 2, 3, 4, 5, 6\}  
(B) \{5, 6, 7, 8, 9, 10, 11\}  
(C) \{2, 4, 8, 16, 32, 64, 128\}  
(D) \{-15, -13, -5, 7, 10, 18, 26\}  
(E) \{0, 5, 10, 15, 20, 25, 30\}  
(F) none of these.

\[2 \equiv 16 \pmod{7}\]

(6) Which of the following is **NOT** a *reduced residue system* modulo 8?

(A) \{3, 9, 15, 21\}  
(B) \{1, 3, 5, 7\}  
(C) \{-15, -5, 15\}  
(D) \{1, 11, 11^2, 11^3\}  
(E) \{-3, -1, 1, 3\}  
(F) none of these.

\[1 \equiv 11^2 \pmod{8}\]

(7) The exponent of 5 in the canonical representation of 50! is ______.

(A) 10  
(B) 11  
(C) 12  
(D) 13  
(E) 14  
(F) none of these.

\[\left\lfloor \frac{50}{5} \right\rfloor + \left\lfloor \frac{50}{5^2} \right\rfloor = 10 + 2 = 12\]
(8) Which of the following is not a primitive Pythagorean triple?

(A) (7, 24, 25)  (B) (33, 56, 65)  (C) (13, 84, 87)  (D) (20, 21, 29)  (E) (28, 45, 53)  (F) none of these.

\[ \frac{3^2}{2} + 84^2 = 85^2 \]

(9) Which of the following statement is **FALSE**?

(A) If \( a \) is coprime with \( b \), then \( a^3 \) is coprime with \( b^2 \).

(B) If \( ab \equiv bc \pmod{mc} \), then \( a \equiv b \pmod{m} \).

(C) If \( p \) is a prime, then \( 2p + 1 \) is also a prime.

(D) If \( 2^n - 1 \) is a prime, then \( 2^{n-1}(2^n - 1) \) is a perfect number.

(E) If \( 2^p - 1 \) is a prime, then \( p \) is also a prime.

(F) If \( a \equiv b \pmod{m_1} \), \( a \equiv b \pmod{m_2} \) and \( (m_1, m_2) = 1 \), then \( a \equiv b \pmod{m_1 \cdot m_2} \).

\[
\text{Take } \quad p = 7, \quad 2p+1 = 15 \text{ is composite.}
\]

(10) This question is about the primality tests of Fermat and Miller. Which one of the following statements is **TRUE**?

(A) If \( n \) passes Fermat’s test to some base \( a \), then \( n \) also passes Miller’s test to base \( a \).

(B) There exists number \( n \) which passes Miller’s test to every base coprime with \( n \).

(C) Pseudoprimes to base \( a \) are also strong pseudoprimes to base \( a \).

(D) If a number \( n \) passes Miller’s test to some base \( a \), then \( n \) must be a prime.

(E) There are infinitely many Carmichael numbers.

(F) none of these.
"Show work" for full credit problems

1 (15 pts) Show that the numbers $5, 5^2, 5^3, 5^4, 5^5, 5^6$ form a reduced residue system modulo 7.

See Version A

2 (15 pts) What is the remainder when $1234^{121}$ is divided by 17?

See Version A
3 (15 pts) Show that 124 is a pseudoprime to base 5.

4 (5 pts) Show that $7x^3 + 2 = y^3$ has no solution in integers.