CS22 Practice Exam 2: Number Theory (Fall 2026)

ANSWER KEY ANSWER KEY ANSWER KEY ANSWER KEY

Please read these directions carefully before you begin!

For this section, there are 5 total pages (including this cover sheet) and 4 questions.

Before the Exam

- At the start of the exam, you should have one exam for each section you are doing.
- Please sit with a gap between you and the people on either side (as much as you're able).
- No electronic devices are allowed. Please turn off and put away your phone.
- Write your name and Brown ID number on this cover sheet, and write your Brown ID in the top right of every page. To do this, just flip up the top right corner of each page; do not open the exam or look at the questions. This will help us grade anonymously.
- Do not start the exam until the time starts.

During the Exam

- This is a *closed-book* exam. You may not use any external resources.
- Your work should be yours and yours alone. Please do not look at other people's exams!
- You may do the sections in any order and split the exam time among them as you like.
- As a rough guide, plan to spend about one minute per point.
- We will only grade what is written on the front of the pages. You may use the backs of the pages as scratch paper. However we will not grade answers written on the backs of pages.
- If you run out of space on the front of the page, please ask for extra scratch paper and continue your answer on the front of the scratch paper. If you do this, when you turn in your exam, you must let us know so that we can staple your scratch paper into your exam.
- If you have a question, raise your hand and we will come to you.
- If you need extra scratch paper, raise your hand; do not use your own.
- To use the bathroom, raise your hand first and leave your phone on your desk.

After the Exam

- This exam is for you alone. Do not share it or your solutions with anyone.
- Solutions will be graded on correctness and clarity. Partial correctness will get partial credit.

Good luck!

Student name: _____

Brown ID: _____

ANSWER KEY ANSWER KEY ANSWER KEY ANSWER KEY

1. (4 points) For each item below, select exactly one option. Below, recall that $x \mid y$ means x divides y, $\text{rem}(y, x)$ is the remainder of y divided by x, $\gcd(x, y)$ is the greatest common divisor of x and y and ϕ is the totient function.

   i. If $x \mid y$ then $\text{rem}(y, x)$ is

   $\surd$ 0 ◯ x ◯ y ◯ Undefined

   ii. For any integer $x \geq 0$ we have $\gcd(x, 0)$ is

   ◯ 0 $\surd$ x ◯ $x/2$ ◯ Undefined

   iii. If p is prime then a multiplicative inverse of $a \in (0, p)$ mod p is

   ◯ a $\surd$ a^{p-2} ◯ a^{p-1} ◯ a^p

   iv. (Noting that $21 = 7 \cdot 3$) we have $\phi(21)$ is

   ◯ 21 ◯ 20 ◯ 2 $\surd$ 12

2. (4 points) Select exactly one option for each item.

   i. The set of integers which satisfy $x - 2 \equiv 1 \mod 4$ is

   $\surd$ $\{x : \mathbf{rem}(x, 4) = 3\}$ ◯ $\{\ldots, 1, 5, 9, \ldots\}$ ◯ $\{3\}$ ◯ $\{x : \text{rem}(3, x) = 4\}$

   ii. 0 has a multiplicative inverse mod 2.
   ◯ True $\surd$ **False**

   iii. The following gives all intermediate values of variables when running Euclid's algorithm for computing $\gcd(36, 15) = 3$ (with blanks X and Y).

Step	a	b
1	15	36
2	6	**X**
3	**Y**	6
4	0	3

   What goes in the table for X and Y?
   ◯ $X = 36, Y = 0$ ◯ $X = 6, Y = 0$ $\surd$ $X = 15$**,** $Y = 3$ ◯ $X = 0, Y = 0$

   iv. For any integer $n \geq 2$ we have $\phi(n) \geq 1$.
   $\surd$ **True** ◯ False

3. (7 points) Find all x such that $2^{52}x \equiv 3 \mod 5$. (**Hint**: Note that $52 = 4 \cdot 13$).

Solution: Since 5 is prime, by Fermat's Little Theorem we have that $2^4 \equiv 1 \mod 5$. Substituting this we get

$$\begin{aligned} 2^{52}x &\equiv 3 \mod 5 \\ &\text{iff} \\ (2^4)^{13}x &\equiv 3 \mod 5 \\ &\text{iff} \\ x &\equiv 3 \mod 5 \end{aligned}$$

so the x satisfying the above are $\{\ldots 3, 8, 13, \ldots\}$.

4. (10 points) Prove that for all integers a, b, n, m, if $a \equiv b \mod n$ and $m \mid n$ then $a \equiv b \mod m$. You may assume that $x \equiv y \mod z$ iff $z \mid (x - y)$ for any integers x, y, z.

Solution: Fix arbitrary a, b, n and suppose $a \equiv b \mod n$ and $m \mid n$.

Since $a \equiv b \mod n$ we know $n \mid (a - b)$ so there is an integer k such that $nk = a - b$. Similarly, since $m \mid n$, there is another integer k' such that $mk' = n$.

Combining these, we get $a - b = m(kk')$ so $m \mid (a - b)$ and so $a \equiv b \mod m$.