§4.4 Inverse

Def: If \( x \in \mathbb{Z} \) satisfies \( ax \equiv 1 \pmod{m} \), we say \( x \) is an inverse of \( a \pmod{m} \).

Thm: If \( \gcd(a, m) = 1 \), \( m \in \mathbb{Z}^+ \), then \( a \) has an inverse \( \overline{x} \) modulo \( m \).

Furthermore,

Pf: \( \gcd(a, m) = 1 \Rightarrow \exists s, t \in \mathbb{Z} \) such that \( sa + tm = 1 \).

Since \( tm \equiv 0 \pmod{m} \),

Suppose \( \tilde{x} \) is another inverse of \( a \pmod{m} \), then \( \tilde{x} \equiv x \pmod{m} \).

Ex: Find the inverse of \( 3 \pmod{11} \).

Need to write \( \gcd(3, 11) \).
Euclid Alg. ⇒
⇒

\[ \frac{\text{wre}}{2} \]

\[ \frac{1}{=} \]

\[ \text{wre} \]

\[ 1 = \]
Announcements

Tuesday (Feb 13): In-class midterm, 12:40 - 2:00pm
No notes, books, calculators.

Your homework grades should be on Bcourses.

Exam will cover every topic we've covered in class up through §14.3.

Exam: ≈ 1/2
≈ 1/2
≈ 1/2

Questions will be similar to those we've done in class or on homework.

You should know:

Advice

•

•
(1) Mark each of the following questions true (T) or false (F). Provide a sentence or two justifying each answer.

(a) If $x \equiv y \pmod{m}$ then $ax \equiv ay \pmod{m}$.

(b) If $ax \equiv ay \pmod{m}$ then $x \equiv y \pmod{m}$.

(c) The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = \lfloor \frac{x}{2} \rfloor$ is surjective.

(d) The set of integers and the set of even integers have the same cardinality.

(e) The positive real numbers are countable.

(f) Let $\mathbb{R}$ be the domain, and let $P(x, y)$ be the statement $y^2 = x$. Determine the truth value of the following statement:
   $\forall x \exists y \ P(x, y)$.  

(2) Prove that if \( m \) is a positive integer of the form \( 4k + 3 \) for some non-negative integer \( k \), then \( m \) is not the sum of the squares of two integers.
(3) Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$. 
(4) Computation.
   - Write the number 466 in base 9.

   - What is the sum of the first $n$ entries of the sequence $1, 3, 9, 27, 81, \ldots$?

   - Calculate $(47^{100} + 25^4) \mod 23$.

   - What is the contrapositive of the statement “If my cell phone rings, I disturb the lecture.”
(5) Prove that if $p$ is prime, the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers $x$ such that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. 
(6) Show that if $a$ and $b$ are positive integers, then $ab = \gcd(a, b) \cdot \lcm(a, b)$. 