Homework 5

Due: Wednesday, March 14

All homeworks are due at 12:55 PM in the CS22 bin on the CIT second floor, next to the Fishbowl.

Include our cover sheet or equivalent, write your Banner ID (but not your name or your CS login) on each page of your homework, label all work with the problem number, and staple the entire handin before submitting.

Be sure to fully explain your reasoning and show all work for full credit. Consult the style guide for more information.

Problem 1

Suppose \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \). Let \( n \in \mathbb{Z}^+ \). Prove the following statements:

a. \( ac \equiv bd \pmod{m} \).

b. \( a^n \equiv b^n \pmod{m} \).

Hint: Try induction on \( n \).

For parts c and d, determine if there is an integer solution for \( x \). Justify your answers.

c. \( 12x \equiv 6 \pmod{24} \)

d. \( 7x \equiv 3 \pmod{20} \)

Problem 2

a. Find the \( \gcd \) of 630 and 825 using the Euclidean Algorithm. Show your work!

b. Express the \( \gcd \) in part a as a linear combination of 630 and 825 by backtracking through the Euclidean Algorithm. Show your work!

c. Find a solution to the congruence:

\[
630x \equiv 30 \pmod{825}, \ x \in \mathbb{Z}.
\]

b. Find the \( \gcd \) of 4199 and 14674 using the Euclidean Algorithm. Show your work!
e. Express the gcd in part d as a linear combination of 4199 and 14674 by backtracking through the Euclidean Algorithm.

f. Using your linear combination in part e, give a multiplicative inverse of 14674 when working in \((\text{mod } 4199)\). Similarly, give a multiplicative inverse of 4199 when working in \((\text{mod } 14674)\).

**Problem 3**

Black Hat and Beret Guy are playing a *very fun* game. The game starts with two distinct, positive integers \(a\) and \(b\) written on a blackboard. On a given player’s turn, they write a new positive integer on the board that is the difference of two integers already present on the board. If they cannot do so, they lose.

For example: suppose that 12 and 15 are on the board initially. Black Hat plays first and writes 3, which is \(15 - 12\). Then Beret Guy writes 9 = 12 − 3. Then Black Hat plays 6 = 15 − 9. Beret Guy cannot write any new integers, so he loses.

a. Prove that every number on the board at the end of the game is a multiple of \(\gcd(a, b)\).

b. Prove that every positive multiple of \(\gcd(a, b)\) up to \(\max(a, b)\) is on the board at the end of the game.

c. Given that Black Hat can choose to go first or second, describe a strategy that allows Black Hat to win every time. Explain why your strategy is correct.

**Problem 4**

Beret and Cueball want to establish a secure communication channel to thwart the persistent eavesdropping of Black Hat. Beret wants to use a cryptosystem that is both simple and effective and has decided to use the RSA cryptosystem as a result. He publishes the product of primes \(n = 1963\) and the public key \(k = 49\).

a. Black Hat wants to send nonsense along the communication channel to troll everyone. Encrypt his favorite word, XKCD, by encrypting each letter seperately by using the encoding of \(A = 1, B = 2, \ldots, Z = 26\). Your answer should be a sequence of numbers.

b. In a moment of weakness, Beret has revealed his decryption exponent, 1249, to Black Hat! Decrypt the most recent series of messages sent by Cueball:

\[(868, 1529, 1, 1125, 386, 1163)\]
Note: Beret and Cueball were using the same encoding as used in part a for encoding letters. As such, your answer should be a sequence of letters that Cueball originally encoded.

c. Suppose Black Hat has found two integers $x$ and $y$ such that $x^2 \equiv y^2 \pmod{n}$, but $x \not\equiv \pm y \pmod{n}$. Explain how he can find $(p, q)$.

d. Beret has regained his senses and chosen the new encryption exponent 101. But Black Hat has duped him once again and stolen the corresponding decryption exponent, 1301. Use the two pairs of encryption and decryption exponents to factor $n$. 