UNIVERSITY OF WESTERN ONTARIO

Computer Science 2214a, Fall 2013 - 2014
Discrete Structures for Computing

ASSIGNMENT 3
Given: Wednesday, Oct.30, Due: Wednesday, Nov.6, 6:00pm

1. Prove that if n is an integer that is not a multiple of 3, then

$$n^2 \equiv 1 (\text{mod } 3).$$

Provide detailed justifications of your answer.

2. *(a)* Use the Euclidean Algorithm to find gcd(580, 50).

(b) Given that gcd(662, 414) = 2, use the algorithm described in class to write 2 as a linear combination of 662 and 414.

Provide detailed justifications of your answers.

3. *(a)* Use the algorithms described in class to convert $(11101)_2$ to base 16 and convert $(6253)_8$ to base 2.

(b) Use the algorithms described in class to find the sum and product of the base 2 numbers $(10\ 1011)_2$ and $(110\ 1011)_2$. Express your answers as numbers in base 2.

Provide detailed justifications of your answers.

4. *(a)* Decrypt the message "AHFXVHFBGZ" that was encrypted using the shift cipher $f(x) = (x + 19)$ **mod** 26.

(b) What is the decryption function for an affine cipher if the encryption function is $f(x) = (3x + 7)$ **mod** 26?

Provide detailed justifications of your answers.

5. Use the Principle of Mathematical Induction to show that

$$1 + 4 + 7 + 10 + ... + (3n - 2) = n(3n - 1)/2,$$

for all $n \geq 1$. Provide detailed justifications of your answer.