1 Modular Arithmetic

Solve the following equations for $x$ and $y$ modulo the indicated modulus, or show that no solution exists. Show your work.

(a) $9x \equiv 1 \pmod{11}$.
(b) $10x + 23 \equiv 3 \pmod{31}$.
(c) $3x + 15 \equiv 4 \pmod{21}$.
(d) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

2 Baby Fermat

Assume that $a$ does have a multiplicative inverse $\pmod{m}$. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.
(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?
(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is $k$ in terms of $i$ and $j$?

3 Does It Exist?

Can you find a number that is a perfect square and is a multiple of 2 but not a multiple of 4? Either give such a number or prove that no such number exists.

4 Bijections

Let $n$ be an odd number. Let $f(x)$ be a function from $\{0, 1, \ldots, n-1\}$ to $\{0, 1, \ldots, n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.
(b) $f(x) = 5x \pmod{n}$. 

CS 70 Spring 2017 DIS 3b
(c) $n$ is prime and

$$f(x) = \begin{cases} 
0 & \text{if } x = 0, \\
\left( x^{-1} \mod n \right) & \text{if } x \neq 0.
\end{cases}$$

(d) $n$ is prime and $f(x) = x^2 \mod n$. 