UNIVERSITY OF CALGARY

Faculty of Science
Department of Mathematics & Statistics

Homework #4 - MATH 271 - L01 & L02

Follow instructions available in the Assignment Policy document!

Question 1

a: Let a, b and c be integers. Prove that if $gcd(a, b) = 1$, $a \mid c$ and $b \mid c$, then $ab \mid c$.

b: Show that the assumption that $gcd(a, b) = 1$ in part (a) is necessary.

Question 2

a: Prove Theorem 10.4.3 part 4.

That is let a, b and n be integers with $n > 1$ and $a \equiv b(mod\ n)$. Prove by induction that $a^m \equiv b^m(mod\ n)$ for all integers $m \geq 1$.

(You may use the other parts of the Theorem in your proof).

b: Argue the following statement:

Let a, b, c , d and n be all non-negative integers with $n > 1$ and such that $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$. Then $a^c \equiv b^d(mod\ n)$.

Question 3

a: With justification, find an inverse for 3276 modulo 3025.

b: With justification, find an inverse for 3276 modulo 3026.

c: You have intercepted the encrypted message $C = 8$ which you know has been encrypted using the RSA cipher using the public key $pq = 1271$ and $e = 43$. With justification, what is the message M?