CS 173, Fall 2014
Examlet 2, Part A

NETID:	
FIRST:	**LAST:**

Discussion: Thursday 2 3 4 5 Friday 9 10 11 12 1 2

Prove the following claim, using your best mathematical style and the following definition of congruence mod k: $a \equiv b \pmod{k}$ if and only if $a = b + nk$ for some integer n.

Claim: For all integers a, b, c, d, and k (k positive), if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ then $a^2 + c \equiv b^2 + d \pmod{k}$.

Solution:

Let a, b, c, d, and k be integers, with k positive. Suppose that $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$.

By the definition of congruence mod k, $a \equiv b \pmod{k}$ implies that $a = b + nk$ for some integer n. Similarly, $c \equiv d \pmod{k}$ implies that $c = d + mk$ for some integer m. Then we can calculate

$$a^2 + c = (b + nk)^2 + (d + mk) = b^2 + 2bnk + n^2k^2 + d + mk = b^2 + d + k(2bn + n^2k + m)$$

If we let $p = 2bn + n^2k + m$, then we have $a^2 + c = (b^2 + d) + kp$. Also, p must be an integer since b, n, k, and m are integers. So, by the definition of congruence mod k, $a^2 + c \equiv b^2 + d \pmod{k}$.

CS 173, Fall 2014
Examlet 2, Part A

NETID:

FIRST: **LAST:**

Discussion: Thursday 2 3 4 5 Friday 9 10 11 12 1 2

Prove the following claim, using your best mathematical style and the following definition of congruence mod k: $a \equiv b \pmod{k}$ if and only if $a - b = nk$ for some integer n.

> Claim: For all integers a, b, c, d, j and k (j and k positive), if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ and $j|k$, then $a + c \equiv b + d \pmod{j}$.

Solution:

Let a, b, c, d, j and k be integers, with j and k positive. Suppose that $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ and $j|k$.

By the definition of congruence mod k, $a \equiv b \pmod{k}$ implies that $a - b = nk$ for some integer n. Similarly $c \equiv d \pmod{k}$ implies that $c - d = mk$ for some integer m. By the definition of divides, $j|k$ implies that $k = pj$ for some integer p.

We can then calculate

$$(a + c) - (b + d) = (a - b) + (c - d) = nk + mk = (n + m)k = (n + m)pj$$

Notice that $(n + m)p$ is an integer, since n, m, and p are integers. So, by the definition of congruence mod k, $a + c \equiv b + d \pmod{j}$.

CS 173, Fall 2014
Examlet 2, Part A

NETID:

FIRST:	LAST:

Discussion: Thursday 2 3 4 5 Friday 9 10 11 12 1 2

Prove the following claim, using your best mathematical style and the following definition of congruence mod k: $x \equiv y \pmod{k}$ if and only if $x = y + nk$ for some integer n.

For all integers a, b, p, q and k (k positive), if $a \equiv b \pmod{2k}$ and $p \equiv q \pmod{k}$, then $a(p+1) \equiv b(q+1) \pmod{k}$.

Solution:

Let a, b, p, q and k be integers with k positive. Suppose $a \equiv b \pmod{2k}$ and $p \equiv q \pmod{k}$.

By the definition of congruence mod k, $a \equiv b \pmod{2k}$ implies that $a = b + n(2k)$ for some integer n. Similarly, $p \equiv q \pmod{k}$ implies that $p = q + mk$ for some integer m.

We can now calculate

$$
\begin{aligned}
a(p+1) &= (b+2nk)(q+mk+1) = b(q+mk+1) + 2nk(q+mk+1) \\
&= b(q+1) + bmk + 2nk(q+mk+1) = b(q+1) + k(bm + 2n(q+mk+1))
\end{aligned}
$$

Suppose we let $t = bm + 2n(q+mk+1)$. Then we have $a(p+1) = b(q+1) + kt$. t must be an integer, since m, b, n, q and k are all integers. So, by the definition of congruence mod k, $a(p+1) \equiv b(q+1) \pmod{k}$.

CS 173, Fall 2014
Examlet 2, Part A

NETID:

FIRST:	LAST:

Discussion: Thursday 2 3 4 5 Friday 9 10 11 12 1 2

Prove the following claim, using your best mathematical style and the following definition of congruence mod k: $x \equiv y \pmod{k}$ if and only if $x = y + nk$ for some integer n.

For all integers a, b, c, p and k (c positive), if $ap \equiv b \pmod{c}$ and $k \mid a$ and $k \mid c$, then $k \mid b$.

Solution:

Let a, b, c, p and k be integers, with c positive. Suppose that $ap \equiv b \pmod{c}$ and $k \mid a$ and $k \mid c$.

By the definition of congruence mod k, $ap \equiv b \pmod{c}$ implies that $ap = b + nc$ for some integer n. By the definition of divides, $k \mid a$ and $k \mid c$ imply that $a = ks$ and $c = kt$ for some integers s and t.

Since $ap = b + nc$, $b = ap - nc$. So then we have

$b = ap - nc = ksp - nkt = k(sp - nt)$

$sp - nt$ is an integer since s, p, n, and t are integers. So this implies that $k \mid b$.