CS 173, Spring 2015
Examlet 2, Part A

NETID:

FIRST: **LAST:**

Discussion: Monday 9 10 11 12 1 2 3 4 5

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, Spring 2015
Examlet 2, Part A

NETID:

FIRST:	**LAST:**

Discussion: **Monday** **9** **10** **11** **12** **1** **2** **3** **4** **5**

Recall that gcd m, n is the largest integer that divides both m and n. Use this definition, the definition of divides, and your best mathematical style to prove the following claim by contrapositive.

For all integers p and q, if $p + 6q = 23$ then $\gcd(p, q) \neq 7$.

Begin by explicitly stating the contrapositive of the claim:

Solution: For all integers p and q, if $\gcd(p, q) = 7$, then $p + 6q \neq 23$.

Now prove the contrapositive:

Solution: Let p and q be integers and suppose that $\gcd(p, q) = 7$. Then $7 \mid p$ and $7 \mid q$ by the definition of gcd. By the definition of divides, this implies that $p = 7m$ and $q = 7n$, for some integers m and n.

So $p + 6q = 7m + 6(7n) = 7(m + 6n)$. This mean that $p + 6q$ is divisible by 7. Since we know that 23 isn't divisible by 7, $p + 6q$ can't be equal to 23.

CS 173, Spring 2015
Examlet 2, Part A

NETID:

FIRST:	**LAST:**

Discussion: **Monday 9 10 11 12 1 2 3 4 5**

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, Spring 2015
Examlet 2, Part A

NETID:

FIRST: **LAST:**

Discussion: **Monday 9 10 11 12 1 2 3 4 5**

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 $k \mid b$.

CS 173, Spring 2015
Examlet 2, Part A

NETID:

FIRST:	**LAST:**

Discussion: **Monday** **9** **10** **11** **12** **1** **2** **3** **4** **5**

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 x, y, p, q and m, with $m > 0$, if $x \equiv p \pmod{m}$ and $y \equiv q \pmod{m}$, then $x^2 + xy \equiv p^2 + pq \pmod{m}$.

Solution: Let x, y, p, q and m be integers, with $m > 0$. Suppose that $x \equiv p \pmod{m}$ and $y \equiv q \pmod{m}$.

By the definition of congruence mod k, this means that $x = p + am$ and $y = q + bm$, for some integers a and b. Then we can calculate

$$\begin{aligned} x^2 + xy &= (p+am)^2 + (p+am)(q+bm) \\ &= (p+am)(p+am+q+bm) \\ &= (p+am)(p+q) + (p+am)(am+bm) \\ &= (p+am)(p+q) + m(p+am)(a+b) \end{aligned}$$

Let $t = (p+am)(a+b)$. Then we have

$$\begin{aligned} x^2 + xy &= (p+am)(p+q) + mt \\ &= p(p+q) + am(p+q) + mt = p^2 + pq + m(ap+aq+t) \end{aligned}$$

$(ap + aq + t)$ is an integer because a, b, m, p, q are all integers. So $x^2 + xy \equiv p^2 + pq \pmod{m}$.

CS 173, Spring 2015
Examlet 2, Part A

NETID:

FIRST: **LAST:**

Discussion: Monday 9 10 11 12 1 2 3 4 5

Recall that a real number p is rational if there are integers m and n (n non-zero) such that $p = \frac{m}{n}$. Use this definition and your best mathematical style to prove the following claim by contrapositive.

> For all real numbers x and y, if x is not rational, then $2x + 3y$ is not rational or y is not rational.

Begin by explicitly stating the contrapositive of the claim:

Solution: For all real numbers x and y, if $2x + 3y$ is rational and y is rational, then x is rational.

Now prove the contrapositive:

Solution: Let x and y be real numbers. Suppose that $2x + 3y$ is rational and y is rational. Then $2x + 3y = \frac{a}{b}$ and $y = \frac{m}{n}$, where a, b, m, n are integers, b and n non-zero.

Then $2x + 3\frac{m}{n} = \frac{a}{b}$

So $2x = \frac{a}{b} - \frac{3m}{n} = \frac{an-3bm}{bn}$

So $x = \frac{an-3bm}{2bn}$

$an - 3bm$ and $2bn$ are both integers because a, b, m, n are integers. Also $2bn$ is non-zero because b and n are non-zero. So x is rational.