Problem 1

Show that if $a \equiv b \pmod{n}$ then $a \equiv b \pmod{k}$ for any k which is a divisor of n.

Since $a \equiv b \pmod{n}$, $n|(a-b)$, and $a - b = nm$ for some $m \in \mathbb{Z}$. Since $k|n$, $n = ki$ for some $i \in \mathbb{Z}$. Therefore, $a - b = kim$, and $k|a-b$. Thus, $a \equiv b \pmod{k}$.

Problem 2

Show that the square of any odd number is congruent to 1, modulo 8.

Every odd number can be represented as $2k+1$ for some $k \in \mathbb{Z}$. Squaring gives us

$$\begin{aligned}(2k+1)^2 &= 4k^2 + 4k + 1\\ &= 4k(k+1) + 1\end{aligned}$$

If k is even, then $8|4k$. If k is odd, then $8|4(k+1)$. In either case, $8|(4k(k+1))$. Therefore, $(2k+1)^2 \equiv 4k^2 + 4k + 1 \equiv 4k(k+1) + 1 \equiv 0 + 1 \equiv 1 \pmod{8}$.

Problem 3

Given that $a^{10} \equiv 74 \pmod{650}$, find $(a, 650)$.

$650 = 2 \cdot 5^2 \cdot 13$. From problem 1, we can create 3 equivalent congruences: $a^{10} \equiv 74 \equiv 0 \pmod{2}$, $a^{10} \equiv 74 \equiv 4 \pmod{5}$, and $a^{10} \equiv 74 \equiv 9 \pmod{13}$. The first congruence implies that a is even and the other two imply that $5 \not| a$ and $13 \not| a$. Thus, $(a, 650) = 2$.

Problem 4

For $n = 1, 2, \ldots, 15$ calculate $(n-1)! \pmod{n}$. Do you state a pattern? State a conjecture.

n	$(n-1)! \pmod{n}$
1	0
2	1
3	2
4	2
5	4
6	0
7	6
8	0
9	0
10	0
11	10
12	0
13	12
14	0
15	0

For all $n = 1, 2, \ldots, 15$, except $n = 4$, $(n-1) \equiv -1 \pmod{n}$ if n is prime. If n is composite, then $(n-1)! \equiv 0 \pmod{n}$.

Conjecture 1

For all $n \in \mathbb{N}$, if n is prime, then $(n-1)! \equiv -1 \pmod{n}$.

Problem 5

Find each reciprocal

a. $7^{-1} \pmod{39}$

b. $15^{-1} \pmod{111}$

c. $12^{-1} \pmod{1331}$

a. $28 \pmod{39}$

b. $(15, 111) = 3$, so no inverse exists

c. $111 \pmod{1331}$

Problem 6

Solve each linear congruence:

a. $7x \equiv 22 \pmod{39}$

b. $15y \equiv 86 \pmod{111}$

c. $15z \equiv 87 \pmod{111}$

d. $12w \equiv 1234 \pmod{1331}$

a. As we found in 5a, the inverse of 7 modulo 39 is 28. Therefore, $x \equiv 28 \cdot 22 \equiv 616 \equiv 31 \pmod{39}$.

b. $(15, 111) = 3$, but $3 \nmid 86$, so there are no solutions.

c. $(15, 87, 111) = 3$, so we'll divide by that: $5z \equiv 29 \pmod{37}$. The inverse of 5 modulo 37 is 15, so $z \equiv 15 \cdot 29 \equiv 435 \equiv 28 \pmod{37}$.

d. $1234 \equiv -97 \pmod{1331}$. As we found in 5c, the inverse of 12 modulo 1331 is 111. Therefore, $w \equiv 111 \cdot (-97) \equiv -10767 \equiv 1212 \pmod{1331}$.

Problem 7

By casting out 9's and 11's find the missing digits a and b in the multiplication problem $38761 \times 29a37 = 11293b9257$.

We know modulus is multiplicative, so we can cast out 9's and 11's to find a and b.

$$\begin{aligned}(3+8+7+6+1)\times(2+9+a+3+7) &\equiv (1+1+2+9+3+b+9+2+5+7) \pmod{9}\\ 7(3+a) &\equiv 3+b \pmod{9}\\ 21+7a &\equiv 3+b \pmod{9}\\ 7a-b &\equiv 0 \pmod{9}\end{aligned}$$

$$\begin{aligned}(3-8+7-6+1)\times(2-9+a-3+7) &\equiv (1-1+2-9+3-b+9-2+5-7) \pmod{11}\\ 8(8+a) &\equiv 1-b \pmod{11}\\ 64+8a &\equiv 1-b \pmod{11}\\ 7+8a+b &\equiv 0 \pmod{11}\end{aligned}$$

With these two congruences, we can attempt to find solutions for a and b knowing that $0 \leq a, b \leq 9$.

Through some trial and error, we quickly find that $a = 1$ and $b = 7$.

Problem 8

Let $a^x \equiv a^y \equiv 1 \pmod{n}$. Prove that $a^{(x,y)} \equiv 1 \pmod{n}$.

By Bezout's theorem, there exists a linear combination of x and y that equals (x, y). Let $cx+dy = (x, y)$ for some $c, d \in \mathbb{Z}$. Since modulus is multiplicative we have that $a^{x \cdot c} \equiv a^{y \cdot d} \equiv 1 \pmod{n}$. Therefore, $a^{(x,y)} \equiv a^{cx+dy} \equiv a^{cx}a^{dy} \equiv 1 \pmod{n}$.

Problem 9

Among real numbers $x^2 = 1$ if and only if $x = \pm 1$. This is not always true in modular arithemtic. Show that it *is* true for prime moduli: if $x^2 \equiv 1 \pmod{p}$ where p is prime, then $x \equiv \pm 1 \pmod{p}$.

Let's do some rearranging.

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \\ x^2 - 1 &\equiv 0 \pmod{p} \\ (x-1)(x+1) &\equiv 0 \pmod{p} \end{aligned}$$

Thus, there exists a $k \in \mathbb{Z}$, such that $(x-1)(x+1) = kp$. As we have previously shown, this indicates that $p|x-1$ or $p|x+1$. So, either $x + 1 \equiv 0 \pmod{p} \Rightarrow x \equiv -1 \pmod{p}$ or $x - 1 \equiv 0 \pmod{p} \Rightarrow x \equiv 1 \pmod{p}$. Thus, we have shown that if $x^2 \equiv 1 \pmod{p}$ and p is prime, then $x \equiv \pm 1 \pmod{p}$.