MATH 271 – Summer 2016
Solutions to practice problems – Week 6
University of Calgary
Mark Girard

1. Let a, b, m be integers such that $m > 1$. Assume that $a \equiv b \pmod{m}$. Using only the definition of mod and the definition of divisibility, prove that $a^2 \equiv b^2 \pmod{m}$.

   Solution. *Proof.* Since $a \equiv b \pmod{m}$, then $m \mid (a - b)$ by definition. This means that there exists an integer k so that $a - b = km$. Thus $a = km + b$. (We want to show that $a^2 - b^2$ is divisible by m.) Now

   $$\begin{aligned} a^2 = (km + b)^2 &= k^2m^2 + 2kmb + b^2 \\ &= m(mk^2 + 2kb) + b^2 \end{aligned}$$

   and thus $a^2 - b^2 = m(mk^2 + 2kb)$, where $mk^2 + 2kb$ is an integer. Hence $a^2 - b^2$ is divisible by m and thus $a^2 \equiv b^2 \pmod{m}$. □

2. Reduce each of the following modulo n.

   (a) $7 \cdot 9$ for $n = 2, 4, 5, 8, 11$.

   Solution. .

   - For $n = 2$, we have $7 \equiv 1 \pmod{2}$ and $9 \equiv 1 \pmod{2}$. Thus $7 \cdot 9 \equiv 1 \cdot 1 \equiv 1 \pmod{2}$.
   - For $n = 4$, we have $7 \equiv 3 \pmod{4}$ and $9 \equiv 1 \pmod{4}$. Thus $7 \cdot 9 \equiv 3 \cdot 1 \equiv 3 \pmod{4}$.
   - For $n = 5$, we have $7 \equiv 2 \pmod{5}$ and $9 \equiv 4 \pmod{5}$. Thus $7 \cdot 9 \equiv 2 \cdot 4 \equiv 8 \equiv 3 \pmod{5}$.
   - For $n = 8$, we have $7 \equiv 7 \pmod{8}$ and $9 \equiv 1 \pmod{8}$. Thus $7 \cdot 9 \equiv 7 \cdot 1 \equiv 7 \pmod{8}$.
   - For $n = 11$, note that $7 \cdot 9 = 63 = 55 + 8$. Thus $63 \equiv 8 \pmod{11}$. Alternatively, note that $7 \equiv -4 \pmod{11}$ and $9 \equiv -2 \pmod{11}$. Thus $7 \cdot 9 \equiv (-4)(-2) \equiv 8 \pmod{11}$.

   (b) $15 \cdot 23$ for $n = 2, 4, 5, 8, 11$.

   Solution. .

   - For $n = 2$, we have $15 \equiv 1 \pmod{2}$ and $23 \equiv 1 \pmod{2}$. Thus $15 \cdot 23 \equiv 1 \cdot 1 \equiv 1 \pmod{2}$.
   - For $n = 4$, we have $15 \equiv 3 \pmod{4}$ and $23 \equiv 3 \pmod{4}$. Thus $15 \cdot 23 \equiv 3 \cdot 3 \equiv 9 \equiv 1 \pmod{4}$.
   - For $n = 5$, we have $15 \equiv 0 \pmod{5}$ and $23 \equiv 3 \pmod{5}$. Thus $15 \cdot 23 \equiv 0 \cdot 3 \equiv 0 \pmod{5}$.
   - For $n = 8$, we have $15 \equiv -1 \pmod{8}$ and $23 \equiv -1 \pmod{8}$. Thus $15 \cdot 23 \equiv (-1)(-1) \equiv 1 \pmod{8}$.
   - For $n = 11$, we have $15 \equiv 4 \pmod{11}$ and $23 \equiv 1 \pmod{11}$. Thus $15 \cdot 23 \equiv 4 \cdot 1 \equiv 4 \pmod{11}$.

   (c) $(-12) \cdot 17$ for $n = 2, 4, 5, 8, 11$.

   Solution. .

   - For $n = 2$, we have $-12 \equiv 0 \pmod{2}$ and $17 \equiv 1 \pmod{2}$. Thus $(-12) \cdot 17 \equiv 0 \cdot 1 \equiv 0 \pmod{2}$.
   - For $n = 4$, we have $(-12) \equiv 0 \pmod{4}$ and $17 \equiv 1 \pmod{4}$. Thus $(-12) \cdot 17 \equiv 0 \cdot 1 \equiv 0 \pmod{4}$.
   - For $n = 5$, we have $(-12) \equiv 3 \pmod{5}$ and $17 \equiv 2 \pmod{5}$. Thus $(-12) \cdot 17 \equiv 3 \cdot 2 \equiv 6 \equiv 1 \pmod{5}$.
   - For $n = 8$, we have $(-12) \equiv 4 \pmod{8}$ and $17 \equiv 1 \pmod{8}$. Thus $(-12) \cdot 17 \equiv 4 \cdot 1 \equiv 4 \pmod{8}$.
   - For $n = 11$, we have $(-12) \equiv -1 \pmod{11}$ and $17 \equiv -5 \pmod{11}$. Thus $(-12) \cdot 17 \equiv (-1) \cdot (-5) \equiv 5 \pmod{11}$.

(d) $(-12) \cdot (-7)$ for $n = 2, 4, 5, 8, 11$.

Solution. .

- For $n = 2$, we have $-12 \equiv 0 \pmod 2$ and $-7 \equiv 1 \pmod 2$. Thus $(-12) \cdot (-7) \equiv 0 \cdot 1 \equiv 0 \pmod 2$.
- For $n = 4$, we have $(-12) \equiv 0 \pmod 4$ and $-7 \equiv 1 \pmod 4$. Thus $(-12) \cdot (-7) \equiv 0 \cdot 1 \equiv 0 \pmod 4$.
- For $n = 5$, we have $(-12) \equiv 3 \pmod 5$ and $(-7) \equiv 3 \pmod 5$. Thus $(-12) \cdot (-7) \equiv 3 \cdot 3 \equiv 9 \equiv 4 \pmod 5$.
- For $n = 8$, we have $(-12) \equiv 4 \pmod 8$ and $(-7) \equiv 1 \pmod 8$. Thus $(-12) \cdot (-7) \equiv 4 \cdot 1 \equiv 4 \pmod 8$.
- For $n = 11$, we have $(-12) \equiv -1 \pmod{11}$. Thus $(-12) \cdot (-7) \equiv (-1) \cdot (-7) \equiv 7 \pmod{11}$.

3. Solve each of the following congruences for x.

(a) $x + 17 \equiv 31 \pmod 5$

Solution. .
Subtracting 17 from both sides, we have $x \equiv 14 \pmod 5$. But $14 \equiv 4 \pmod 5$, so $x = 4$.

(b) $x + 27 \equiv -10 \pmod{13}$

Solution. .
Subtracting 27 from both sides, we have $x \equiv -37 \pmod{13}$. But $-37 \equiv 2 \pmod{13}$, so $x = 2$.

(c) $2x + 5 \equiv 3 \pmod 7$

Solution. .
Subtracting 5 from both sides, we have $2x \equiv -2 \pmod 7$. Note that 4 is an inverse of 2 modulo 7. That is, $4 \cdot 2 \equiv 1 \pmod 7$. Multiplying both sides by 4 gives us

$$4 \cdot 2x \equiv 4 \cdot (-2) \pmod 7$$

or $1 \cdot x \equiv -8 \pmod 7$ and $-8 \equiv 6 \pmod 7$. Hence $x = 6$.
Alternatively, we note that $\gcd(2, 7) = 1$, so we can cancel the 2 on both sides of

$$2x \equiv -1(2) \pmod 7$$

which gives us $x \equiv -1 \equiv 6 \pmod 7$.

(d) $2x + 5 \equiv -3 \pmod{11}$

Solution. .
Subtracting 5 from both sides, we have $2x \equiv -8 \pmod{11}$ or $2x \equiv 3 \pmod{11}$. Note that 6 is an inverse of 2 modulo 11. That is, $6 \cdot 2 \equiv 1 \pmod{11}$. Multiplying both sides by 6 gives us

$$6 \cdot 2x \equiv 6 \cdot 3 \pmod{11}$$

or $x \equiv 18 \pmod{11}$ and $18 \equiv 7 \pmod{11}$. Hence $x = 7$.

Alternatively, we note that $\gcd(2, 11) = 1$, so we can cancel the 2 on both sides of

$$2x \equiv -8 \pmod{11}$$

which gives us $x \equiv -4 \equiv 7 \pmod{11}$.

(e) $4x + 7 \equiv 1 \pmod 9$

Solution. .
Subtracting 7 from both sides, we have $4x \equiv -6 \pmod 9$ or $4x \equiv 3 \pmod 9$. Note that $2 \cdot 4 = 8$ and $8 \equiv -1 \pmod 9$. Multiplying both sides by 2 gives us

$$2 \cdot 4x \equiv 2 \cdot 3 \pmod 9$$

or $(-1)x \equiv 6 \pmod 9$ and $x \equiv -6 \pmod 9$. But $-6 \equiv 3 \pmod 9$. Thus $x = 3$. (Alternatively, note that -2 is an inverse of 4 modulo 9, since $-2 \cdot 4 = -8 = 1 - 9$. Multiplying both sides by -2 gives you $x \equiv -6 \pmod 9$ and $-6 \equiv 3 \pmod 9$.)

(f) $15x + 12 \equiv -11 \pmod{49}$

Solution. .
Subtracting 12 from both sides, we have $15x \equiv -23 \pmod{49}$ or $15x \equiv 26 \pmod{49}$. Also note that $15x \equiv 75 \pmod{49}$ since $26 \equiv 75 \pmod{49}$. Note that $75 = 15 \cdot 5$. Also note that $\gcd(15, 49) = 1$, so we can cancel the 15 on both sides to get $x \equiv 5 \pmod 9$. Hence $x = 5$.

Alternatively, we can try to find an inverse for 15 modulo 49. Note that

$$\begin{aligned} 49 &= 3 \cdot 15 + 4 \\ 15 &= 3 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

$\gcd(49, 15) = \gcd(15, 4) = \gcd(4, 3) = \gcd(3, 1) = 1$. Using the table method, we have

		x	y
R_1	49	1	0
R_2	15	0	1
$R_3 = R_1 - 3R_2$	4	1	-3
$R_4 = R_2 - 3R_3$	3	-3	10
$R_5 = R_3 - R_4$	1	4	-13

and thus $49 \cdot 4 + 15 \cdot (-13) = 1$. Hence -13 is an inverse of 15 modulo 49. Multiplying both sides of $15x \equiv 26 \pmod{49}$ by (-13) gives us

$$x \equiv (-13) \cdot 26 \pmod{49}$$

and $(-13) \cdot 26 = -338$ and $-338 \equiv 5 \pmod{49}$, since $7 \cdot 49 = 343$ and $-338 = 5 - 343 = 5 + 49 \cdot (-7)$.

(g) $-15x + 22 \equiv -9 \pmod{28}$

Solution. .
Subtracting 22 from both sides, we have $-15x \equiv -31 \pmod{28}$ or $15x \equiv 31 \equiv 3 \pmod{28}$, by multiplying both sides by -1. We will now find an inverse for 15 modulo 28. Using the Euclidean algorithm,

$$\begin{aligned} 28 &= 1 \cdot 15 + 13 \\ 15 &= 1 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \end{aligned}$$

and thus $\gcd(28, 15) = \gcd(15, 13) = \gcd(13, 2) = \gcd(2, 1) = 1$. Using the table method, we have

		x	y
R_1	28	1	0
R_2	15	0	1
$R_3 = R_1 - R_2$	13	1	-1
$R_4 = R_2 - R_3$	2	-1	2
$R_5 = R_3 - 6R_4$	1	7	-13

and thus $28 \cdot 7 + 15(-13) = 1$. This means that -13 and $28 + (-13) = 15$ are inverses of 15 modulo 28. So we can multiply both sides by 15 to get

$$15 \cdot 15x \equiv 15 \cdot 3 \pmod{28}.$$

But $15 \cdot 3 = 45 = 28 + 17$, so $15 \cdot 3 \equiv 17 \pmod{28}$. Also $15 \cdot 15 \equiv 1 \pmod{28}$ hence $15 \cdot 15x \equiv 1 \cdot x \pmod{28}$. This gives us

$$1 \cdot x \equiv 17 \pmod{28}.$$

Thus $x = 17$.