Complete Solutions to Supplementary Problems 3

1. (a) Since the reminder after dividing 2015 by 10 is 5 so $2015 \equiv 5 \pmod{10}$ is true.

   (b) 266 divided by 7 gives 0 reminder so $266 \equiv 1 \pmod{7}$ is false.

   (c) 17 divided by 12 gives reminder 5 *not* -5 so $17 \equiv -5 \pmod{12}$ is false.

   (d) $-11 \equiv -57 \pmod{34}$ implies that

   $$-11 - 57 = -68 = -2 \times 34$$

   Hence $-11 \equiv -57 \pmod{34}$ is true.

   (e) Since every integer a divided by 1 gives reminder zero so $a \equiv 0 \pmod{1}$ is true.

2. We can use the following formula in each of the cases:

   (3.17) $$x \equiv x_0,\ x_0 + \left(\frac{n}{g}\right),\ x_0 + 2\left(\frac{n}{g}\right),\ x_0 + 3\left(\frac{n}{g}\right), \cdots,\ x_0 + (g-1)\left(\frac{n}{g}\right) \pmod{n}$$

   (a) We are given the equation $7x \equiv 21 \pmod{15}$. The $\gcd(7,\ 15) = 1$ and clearly $1 \mid 21$ so we have a unique solution.

   By inspection we have $x \equiv 3 \pmod{5}$ because

   $$7 \times 3 \equiv 21 \pmod{15}$$

   This is the only solution to the given congruence.

   (b) This time we need to solve $12x \equiv 24 \pmod{27}$. The $\gcd(12,\ 27) = 3$ and $3 \mid 24$ so we have 3 incongruent solutions to the given linear congruence.

   By inspection one of the solutions is $x_0 \equiv 2 \pmod{27}$. Using the (3.17) formula with $n = 27$, $g = 3$ we have

   $$x \equiv 2,\ 2 + \frac{27}{3}(1) \text{ and } 2 + \frac{27}{3}(2) \equiv 2,\ 11,\ 20 \pmod{27}$$

   Our three incongruent solutions are $x \equiv 2,\ 11,\ 20 \pmod{27}$.

(c) We are asked to solve the equation, $10x \equiv 20 \pmod{30}$. The $\gcd(10,\ 30) = 10$ and as $10 \mid 20$ we have 10 incongruent solutions. Clearly $x_0 \equiv 2 \pmod{30}$ is a solution. The others are found by substituting $\frac{n}{g} = \frac{30}{10} = 3$ and $x_0 = 2$ into the formula (3.17):

$$\begin{aligned} x &\equiv 2,\ 2+3,\ 2+(2\times 3),\ 2+(3\times 3),\ \cdots,\ 2+(9\times 3) \pmod{30} \\ &\equiv 2,\ 5,\ 8,\ 11,\ \cdots,\ 29 \pmod{30} \end{aligned}$$

(d) Solving the given equation $3x \equiv 2 \pmod{6}$ we have the $\gcd(3,\ 6) = 3$ but $3 \nmid 2$ so there are *no* solutions to this equation.

3. (a) Let x be the multiplicative inverse of $5 \pmod{12}$. Then x satisfies

$$5x \equiv 1 \pmod{12}$$

By trialling some x values we have $x = 5$ because

$$5 \times 5 = 25 \equiv 1 \pmod{12}$$

Hence the multiplicative inverse of $5 \pmod{12}$ is $5 \pmod{12}$.

(b) Similarly we have to find x such that

$$7x \equiv 1 \pmod{15}$$

Trialling $x = 2$ gives $7 \times 2 \equiv 14 \equiv -1 \pmod{15}$. Multiplying this by -1 gives

$$7 \times (-2) \equiv 1 \quad \Rightarrow \quad 7 \times 13 \equiv 1 \pmod{15}$$

Hence the multiplicative inverse of $7 \pmod{15}$ is $13 \pmod{15}$.

(c) We need to find the multiplicative inverse of $10 \pmod{27}$. This implies that we need to find x such that

$$10x \equiv 1 \pmod{27}$$

Trialling $x = 11$ we get

$$10 \times 11 \equiv 110 \equiv 2 \pmod{27} \qquad (\ddagger)$$

Easier to deal with 2 rather than 10. We know $2 \times 14 = 28$ and $28 \equiv 1 \pmod{27}$. Multiplying the congruence in (‡) by 14 gives

$$10\times 11\times 14 \equiv 2\times 14 \equiv 1 \pmod{27}$$

Now $11\times 14 = 154 \equiv 19 \pmod{27}$. Putting this into the above calculation yields

$$10\times 11\times 14 \equiv 10\times 19 \equiv 1 \pmod{27}$$

Hence the multiplicative inverse of $10 \pmod{27}$ is $19 \pmod{27}$.

(d) We need to find the inverse of $6 \pmod{15}$. Let x be the inverse then

$$6x \equiv 1 \pmod{15}$$

This linear congruence has *no* solution because $\gcd(6,\ 15) = 3$ and $3 \not| 1$.

This implies that $6 \pmod{15}$ has no inverse.

(e) We need to find x such that $7x \equiv 1 \pmod{12}$. Well we know that

$$7(5) \equiv 35 \equiv -1 \pmod{12}$$

Multiplying this by -1 gives

$$7(-5) \equiv (-1)(-1) \equiv 1 \pmod{12}$$

Hence $x \equiv -5 \equiv 7 \pmod{12}$.

(f) This time we need to solve $11x \equiv 1 \pmod{12}$. Note that $11 \equiv -1 \pmod{12}$.

Using this on $11x \equiv 1 \pmod{12}$ we have

$$11x \equiv (-1)x \equiv 1 \pmod{12} \quad \Rightarrow \quad x \equiv -1 \equiv 11 \pmod{12}$$

The multiplicative inverse of $11 \pmod{12}$ is $11 \pmod{12}$.

(g) We are asked to find the multiplicative inverse of $9 \pmod{13}$. This means we need to find x such that $9x \equiv 1 \pmod{13}$. Since $9 \equiv -4 \pmod{13}$ we have

$$9x \equiv -4x \equiv 1 \pmod{13}$$

Multiplying this $-4x \equiv 1 \pmod{13}$ by -1 yields

$$4x \equiv -1 \equiv 12 \pmod{13} \text{ implies that } x \equiv 3 \pmod{13}$$

Hence the inverse of $9 \pmod{13}$ is $3 \pmod{13}$ or $9^{-1} \equiv 3 \pmod{13}$.

(h) We are asked to find the multiplicative inverse of $9 \pmod{15}$. Note that $\gcd(9, \ 15) = 3$ therefore $9 \pmod{15}$ has *no* inverse.

4. It is all the residues which have a gcd greater than 1 with 12:

$$\gcd(2, \ 12) = 2, \ \gcd(3, \ 12) = 3, \ \gcd(4, \ 12) = 4, \ \gcd(6, \ 12) = 6,$$
$$\gcd(8, \ 12) = 4, \ \gcd(9, \ 12) = 3 \ \text{ and } \ \gcd(10, \ 12) = 2$$

Therefore there are no multiplicative inverses for

$$2, 3, 4, 6, 8, 9 \ \text{ and } 10 \pmod{12}$$

5. We are asked to factorize 48351. The ceiling of $\sqrt{48351}$ is

$$\left\lceil \sqrt{48351} \right\rceil = 220$$

Finding the difference between 220 squared and 48351 gives

$$220^2 - 48351 = 49 = 7^2$$

Rearranging this as a difference of two squares we have

$$48351 = 220^2 - 7^2 = (220 + 7) \times (220 - 7) = 227 \times 213$$

Hence $48351 = 227 \times 213$. Clearly 213 is divisible by 3 so

$$\frac{213}{3} = 71 \ \text{ and 71 is prime.}$$

We also need to find the prime factors of 227. Let p be a prime factor of 227 then

$$p \le \left\lfloor \sqrt{227} \right\rfloor = 15$$

The only primes below 15 are 2, 3, 5, 7, 11 and 13. Clearly 2, 3 and 5 do not go into 227. Also 227 is not divisible by 7, 11 and 13 (check this for yourself), therefore 227 is prime.

The prime decomposition of 48 351 is $3 \times 71 \times 227$.

6. (a) The first statement $n \equiv 0 \pmod{p^a}$ then $n \equiv 0 \pmod{p^{a+1}}$ is false because

$$32 \equiv 0 \pmod{2^5} \ \text{ but } \ 32 \not\equiv 0 \pmod{2^6} \ \text{ as } \ 32 \equiv 32 \pmod{2^6}$$

(b) This statement is true; $p^a \equiv 0 \pmod{n}$ then $p^{a+1} \equiv 0 \pmod{n}$.

Proof.

We are given that $p^a \equiv 0 \pmod{n}$. Using Corollary (3.7):

$$x \equiv y \pmod{n} \text{ implies } xc \equiv yc \pmod{n}$$

On $p^a \equiv 0 \pmod{n}$ by multiplying this by p gives

$$pp^{a+1} \equiv p^{a+1} \equiv 0 \pmod{n}$$

We have our required result.

■

(c) This statement is also true; $p^a \equiv 0 \pmod{n}$ then $p^{a+m} \equiv 0 \pmod{n}$.

Proof.

We assume $p^a \equiv 0 \pmod{n}$. By the definition of congruence we have

$$p^a = kn \text{ for some integer } k.$$

Using the rules of indices we can write $p^{a+m} \equiv p^a p^m \pmod{n}$. Substituting the above $p^a = kn$ in this gives

$$p^{a+m} \equiv p^a p^m \equiv knp^m \equiv 0 \pmod{n} \quad \left[\text{Because } kn \text{ is a multiple of } n\right]$$

This completes our proof.

■

(d) The given statement $p^a \equiv 0 \pmod{n}$ and $p^b \equiv 0 \pmod{m}$ then $p^{\min(a,\ b)} \equiv 0 \pmod{m+n}$ is false because $2^5 \equiv 0 \pmod{32}$ and $2^7 \equiv 0 \pmod{128}$ but $2^{\min(5,\ 7)} \equiv 2^5 \equiv 32 \not\equiv 0 \pmod{128+32}$.

7. (a) We need to prove; if n is odd then $n^2 \equiv 1 \pmod{8}$.

Proof.

Let n be an odd integer. By the division algorithm with $b = 8$ we have

$$n = 8q + r \text{ where } 0 \le r < 8$$

Since n is odd so the reminder r can only be 1, 3, 5 or 7.

Squaring this $n = 8q + r$ yields

$$\begin{aligned} n^2 = \left(8q + r\right)^2 &= \left(8q\right)^2 + \left(2 \times 8q \times r\right) + r^2 \\ &= 8\left[8q^2 + 2qr\right] + r^2 = 8m + r^2 \quad \text{where } m = 8q^2 + 2qr \end{aligned}$$

We have $n^2 = 8m + r^2$ where $r = 1,\ 3,\ 5,\ 7$. Writing this as a congruence we have

$$n^2 = 8m + r^2 \equiv 0 + r^2 \equiv r^2 \pmod 8$$

Substituting the above values of r into this yields

$$n^2 \equiv r^2 \equiv 1^2,\ 3^2,\ 5^2,\ 7^2 \equiv 1, 1, 1, 1 \pmod 8$$

Hence if n is odd then $n^2 \equiv 1 \pmod 8$. This completes our proof.

■

(b) We need to prove for any n we have $n^3 \equiv 0,\ 1,\ 6 \pmod 7$.

Proof.

In question 10 of the Supplementary Problems 1 we showed that:

The cube of any integer is of the form $7k$ or $7k \pm 1$. Let n be any integer then from this statement we have $n^3 = 7k,\ 7k \pm 1$.

Representing this $n^3 = 7k,\ 7k \pm 1$ as a congruence with modulo 7 gives

$$n^3 = 7k,\ 7k \pm 1 \equiv 0,\ \pm 1 \equiv 0,\ 1,\ 6 \pmod 7$$

■

(c) We are asked to prove for any n we have $n^4 \equiv 0$ or $1 \pmod 5$.

Proof.

Let n be any integer. Then using the division algorithm with $b = 5$ we have

$$n = 5q + r \text{ where } 0 \le r < 5.$$

Expanding the fourth power of n by the binomial theorem we have:

$$n^4 = (5q + r)^4 = \underbrace{(5q)^4 + 4(5q)^3 r + 6(5q)^2 r^2 + 4(5q) r^3}_{=5m \text{ because this is a multiple of 5}} + r^4$$

$$= 5m + r^4$$

Writing this as a congruence with modulo 5 yields

$$n^4 = 5m + r^4 \equiv 0 + r^4 \equiv r^4 \pmod 5$$

From above we have $0 \le r < 5$ so r can only have the values 0, 1, 2, 3 or 4.

Putting these into the above yields

$$n^4 \equiv r^4 \equiv 0^4,\ 1^4,\ 2^4,\ 3^4,\ 4^4$$

$$\equiv 0,\ 1,\ 16,\ 81,\ 256 \equiv 0, 1, 1, 1, 1 \pmod 5$$

Hence $n^4 \equiv 0$ or $1 \pmod 5$. This completes our proof.

■

8. We apply the division algorithm with $a = n$ and $b = 4$.

Proof.

Let n be an integer. Then by the division algorithm we can write this as

$$n = 4q + r \qquad 0 \le r < 4$$

Squaring this number gives

$$\begin{aligned} n^2 = \left(4q + r\right)^2 &= 16q^2 + 8qr + r^2 \\ &= 4\left(4q^2 + 2qr\right) + r^2 = 4m + r^2 \quad \text{where} \quad 4q^2 + 2qr = m \end{aligned}$$

Note that r can only have values 0, 1, 2 or 3. Squaring each of these gives

$$0^2 = 0\,,\ 1^2 = 1\,,\ 2^2 = 4 \ \text{ and } \ 3^2 = 9$$

Substituting this into the above yields

$$n^2 = 4m + r^2 = 4m,\ \ 4m + 1,\ \ 4m + 4,\ \ 4m + 9$$

Writing each of these as congruence in modulo 4:

$$\begin{aligned} n^2 &= 4m,\ \ 4m + 1,\ \ 4m + 4,\ \ 4m + 9 \\ &\equiv 0,\ \ 1,\ \ 0,\ \ 1 \left(\text{mod } 4\right) \end{aligned}$$

Hence a square number is only congruent to 0 or 1 modulo 4.

■

9. We need to prove if $a \equiv b \left(\text{mod } n\right)$ and $c > 0$ then $ac \equiv bc \left(\text{mod } nc\right)$.

Proof.

From $a \equiv b \left(\text{mod } n\right)$ we have

$$a - b = kn \ \text{ for some integer } k.$$

Multiplying this by c gives

$$ac - bc = knc$$

As we have $c > 0$ therefore $ac \equiv bc \left(\text{mod } nc\right)$. This is our required result.

■

10. We are required to prove that if $a \equiv b \left(\text{mod } n\right)$ and $d \mid a,\ \ d \mid b$ and $d \mid n$ where d is a positive integer then $\dfrac{a}{d} \equiv \dfrac{b}{d} \left(\text{ mod } \dfrac{n}{d}\right)$.

Proof.

From $a \equiv b \left(\text{mod } n\right)$ we have $a - b = kn$ for some integer k. Dividing this $a - b = kn$ by d yields

$$\frac{a}{d}-\frac{b}{d}=k\frac{n}{d}$$

We are given that $d \mid a,\ d \mid b$ and $d \mid n$ so these $\frac{a}{d},\ \frac{b}{d}$ and $\frac{n}{d}$ are all integers which implies we have $\frac{a}{d} \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{n}{d}\right)$. This completes our proof.

■

11. We are asked to prove that $a^p \equiv a\left(\mathrm{mod}\ p\right)$ then $a^{p-1} \equiv 1\left(\mathrm{mod}\ p\right)$ provided $p \nmid a$.

Proof.

We can write the given congruence $a^p \equiv a\left(\mathrm{mod}\ p\right)$ as

$$a\left(a^{p-1}\right) \equiv a\left(1\right)\left(\mathrm{mod}\ p\right)$$

Applying Cancellation Law (3.12):

> If $cx \equiv cy\left(\mathrm{mod}\ p\right)$ and prime p does *not* divide into c then $x \equiv y\left(\mathrm{mod}\ p\right)$.

To $a\left(a^{p-1}\right) \equiv a\left(1\right)\left(\mathrm{mod}\ p\right)$ gives $a^{p-1} \equiv 1\left(\mathrm{mod}\ p\right)$.

■

12. Let $x=5$ and the prime $p=2$ then

$$5^2 \equiv 1\left(\mathrm{mod}\ 2\right)$$

We have both $5-1 \equiv 0\left(\mathrm{mod}\ 2\right)$ and $5+1 \equiv 0\left(\mathrm{mod}\ 2\right)$.

13. (a) We apply the Chinese Remainder Theorem to solve

$$x \equiv 1\left(\mathrm{mod}\ 3\right),\ x \equiv 2\left(\mathrm{mod}\ 4\right),\ x \equiv 3\left(\mathrm{mod}\ 5\right)$$

The formula is:

> (3.23) $$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + \cdots + a_rN_rx_r$$

Since we are given three equations so we use this formula with $r=3$:

$$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$$

In our case $N_1 = 20,\ N_2 = 15,\ N_3 = 12$.

We need to find the x_k's which are given by $N_k x_k \equiv 1 \pmod{n_k}$ for $k = 1,\ 2$ and 3:

$$20x_1 \equiv 1 \pmod{3} \Rightarrow 2x_1 \equiv 1 \pmod{3} \Rightarrow x_1 = 2$$

$$15x_2 \equiv 1 \pmod{4} \Rightarrow -x_2 \equiv 1 \pmod{4} \Rightarrow x_2 = 3$$

$$12x_3 \equiv 1 \pmod{5} \Rightarrow 2x_3 \equiv 1 \pmod{5} \Rightarrow x_3 = 3$$

Substituting $N_1 = 20,\ N_2 = 15,\ N_3 = 12$, $x_1 = 2$, $x_2 = 3$, $x_3 = 3$, $a_1 = 1$ $a_2 = 2$ and $a_3 = 3$ into the above formula:

$$\begin{aligned} x &= a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \\ &= (1 \times 20 \times 2) + (2 \times 15 \times 3) + (3 \times 12 \times 3) \\ &= 238 \end{aligned}$$

We write this number in modulo the product of the given moduli:

$$n = 3 \times 4 \times 5 = 60$$

Hence our solution is

$$x \equiv 238 \equiv 58 \pmod{60}$$

(b) Let x be the number of students in the class. Then x satisfies the following:

$$x \equiv 1 \pmod{3},\ x \equiv 3 \pmod{5},\ x \equiv 5 \pmod{7}$$

Applying the Chinese Remainder Theorem with $r = 3$ gives

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \qquad (*)$$

We have $N_1 = 5 \times 7 = 35$, $N_2 = 3 \times 7 = 21$ and $N_3 = 3 \times 5 = 15$. We also need to find x_1, x_2 and x_3 which are the inverse of 35, 21 and 15 moduli 3, 5 and 7 respectively:

$$35x_1 \equiv 2x_1 \equiv 1 \pmod{3} \Rightarrow x_1 = 2$$

$$21x_2 \equiv x_2 \equiv 1 \pmod{5} \Rightarrow x_2 = 1$$

$$15x_3 \equiv x_3 \equiv 1 \pmod{7} \Rightarrow x_3 = 1$$

Substituting $N_1 = 35,\ N_2 = 21,\ N_3 = 15$, $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, $a_1 = 1$, $a_2 = 3$ and $a_3 = 5$ into (*) yields

$$\begin{aligned} x &= (a_1 \times N_1 \times x_1) + (a_2 \times N_2 \times x_2) + (a_3 \times N_3 \times x_3) \\ &= (1 \times 35 \times 2) + (3 \times 21 \times 1) + (5 \times 15 \times 1) \\ &= 208 \end{aligned}$$

The modulo $n = 3 \times 5 \times 7 = 105$. So our general solution is

$$208 \equiv 103 \left(\text{mod } 105\right)$$

Therefore the number of students in the class are 103.

14. We need to prove the following is false:

If $a^p \equiv a \left(\text{mod } p\right)$ and $a^q \equiv a \left(\text{mod } q\right)$ then $a^{pq} \equiv a \left(\text{mod } pq\right)$.

How?

Produce a counter example:

Let $a = 2,\ p = 5,\ q = 7$ then we have

$$2^5 \equiv 32 \equiv 2 \left(\text{mod } 5\right) \text{ and } 2^7 \equiv 128 \equiv 2 \left(\text{mod } 7\right)$$

However

$$\begin{aligned} 2^{5\times 7} \equiv 2^{35} &\equiv \left(2^5\right)^7 \\ &\equiv \left(-3\right)^7 \equiv -2187 \equiv -17 \equiv 18 \left(\text{mod } 35\right) \end{aligned}$$

Hence the given statement is false.

15. We need to prove $a^h \equiv 1 \left(\text{mod } n\right) \Leftrightarrow k \mid h$ given $a^k \equiv 1 \left(\text{mod } n\right)$.

Proof.

$\left(\Leftarrow\right)$. We assume $k \mid h$ which implies that $km = h$ for some positive integer m.

Therefore, we have

$$a^h \equiv a^{km} \equiv \left(a^k\right)^m \equiv 1^m \equiv 1 \left(\text{mod } n\right).$$

$\left(\Rightarrow\right)$. Suppose $k \nmid h$. By the division algorithm there are integers q and r such that

$$h = qk + r \qquad 0 < r < k.$$

We are given that $a^h \equiv 1 \left(\text{mod } n\right)$. Substituting $h = qk + r$ into this yields

$$a^h \equiv a^{qk+r} \equiv \left(a^k\right)^q a^r \underbrace{\equiv}_{\text{because } a^k \equiv 1 \left(\text{mod } n\right)} 1^q a^r \equiv a^r \equiv 1 \left(\text{mod } n\right)$$

We have $a^r \equiv 1 \left(\text{mod } n\right)$. Recall $0 < r < k$ but we are given that k is the smallest positive integer such that $a^k \equiv 1 \left(\text{mod } n\right)$. This is a contradiction

because we have found a smaller integer, r, than k such that $a^r \equiv 1 \pmod{n}$.

Therefore our supposition $k \nmid h$ must be wrong so $k \mid h$.

■

16. We are asked to prove that if a is even and p be prime such that

$\gcd(a, \quad p) = 1$ but $a^2 \equiv -1 \pmod{p}$ then $p \equiv 1 \pmod{4}$.

Proof.

We are given that a is even, so let $a = 2m$ where m is an integer. We are also given that a satisfies $a^2 \equiv -1 \pmod{p}$ so substituting $a = 2m$ into this gives

$$a^2 \equiv (2m)^2 \equiv 4m^2 \equiv -1 \pmod{p} \qquad (*)$$

Recall that $-1 \equiv p - 1 \pmod{p}$. Putting this into (*) gives

$$4m^2 \equiv p - 1 \pmod{p} \quad \Rightarrow \quad 4m^2 + 1 \equiv p \equiv 0 \pmod{p}$$

As p is of the form $4m^2 + 1$ therefore $p \equiv 1 \pmod{4}$. This is our required result.

We are given a is even and $\gcd(a, \quad p) = 1$ therefore p must be odd. This implies that $p \equiv 1 \pmod{4}$ or $p \equiv 1 \pmod{3}$.

Suppose $p \equiv 1 \pmod{3}$ then

■

17. We need to show that the last two digits of a square number must be one of the following; 00, e1, e4, 25, o6 and e9.

Proof.

Let n be an integer. By the division algorithm we can write n as

$$n = 10q + r \quad \text{where} \quad 0 \le r < 10$$

Evaluating the square working with modulo 100 (because we are interested in the last two digits):

$$n^2 = (10q + r)^2 = 100q^2 + 20qr + r^2 \equiv 20qr + r^2 \pmod{100}$$

We have $n^2 \equiv 20qr + r^2 \pmod{100}$. Note that the first digit which is an integer multiple of 20 is going to be even because we can only have

$$20,\ 40,\ 60,\ 80 \text{ and } 100 \equiv 00 \pmod{100}$$

Hence the last two digits of a square number are

$$e0 + r^2 \text{ where } 0 \le r < 10 \text{ and } e \text{ is even.}$$

Substituting the values of $r = 0,\ 1,\ 2,\ 3,\ \cdots,\ 9$ gives

$$e0 + 0^2 = e0$$
$$e0 + 1^2 = e1$$
$$e0 + 2^2 = e4$$
$$e0 + 3^2 = e9$$
$$e0 + 4^2 = e0 + 16 = o6 \quad \text{where } o \text{ is odd}$$
$$e0 + 5^2 = e0 + 25 = e5$$
$$e0 + 6^2 = e0 + 36 = o6$$
$$e0 + 7^2 = e0 + 49 = e9$$
$$e0 + 8^2 = e0 + 64 = e4$$
$$e0 + 9^2 = e0 + 81 = e1$$

From this list we can only have $e0, e1, e4, e9, o6, e5$. Note that the ones with the last digit equal to 0 and 5 must have their squares ending in 00 and 25 (which is covered by e5) respectively. Hence the last two digits of a square number must be one of the form; 00, e1, e4, 25, o6 and e9.

■

18. (i) We need to solve $x^2 \equiv 1 \pmod{8}$. Creating a table of values gives

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1

From this table our solutions are

$$x \equiv 1,\ 3,\ 5 \text{ and } 7 \pmod{8}$$

(ii) This time we create a table for modulo 7:

$x \pmod 7$	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1

The only solutions of $x^2 \equiv 1 \pmod 7$ are

$$x \equiv 1,\ 6 \equiv \pm 1 \pmod 7$$

19. We are asked to factorize 2 027 651 281.

Let $a_1 = \left\lceil \sqrt{2\ 027\ 651\ 281} \right\rceil = 45030$ then

$b_1 = 45030^2 - 2\ 027\ 651\ 281 = 49619$ which is not a square number.

Repeating this we have

$b_2 = 45031^2 - 2\ 027\ 651\ 281 = 139\ 680$ which is not a square number.

Continuing in this manner we find that

$$b_{12} = 45041^2 - 2\ 027\ 651\ 281 = 1\ 040\ 400 = 1020^2$$

Rearranging this last result gives

$$\begin{aligned} 2\ 027\ 651\ 281 &= 45041^2 - 1020^2 \\ &= (45\ 041 - 1020) \times (45\ 041 + 1020) \\ &= 44\ 021 \times 46\ 061 \end{aligned}$$

20. We are required to prove

> Let a and b be integers which satisfy the congruence
>
> $$a^2 \equiv b^2 \pmod n \text{ and } a \not\equiv \pm b \pmod n.$$
>
> Then $\gcd(a-b,\ n)$ is a *non-trivial* factor of n.

Proof.

Let $g = \gcd(a-b,\ n)$. Therefore, we must show that $g \neq n$ and $g \neq 1$.

Case I: First we prove $g \neq n$.

Suppose $g = \gcd(a-b,\ n) = n$ then $n \mid (a-b)$ and by the definition of congruence we have $a \equiv b \pmod n$. This is a contradiction because we are given $a \not\equiv \pm b \pmod n$ therefore $g \neq n$.

Case II: Now we prove $g \neq 1$.

Suppose $g = \gcd(a-b,\ n) = 1$.

We are given that $a^2 \equiv b^2 \pmod{n}$. Rewriting this

$$a^2 - b^2 \equiv (a-b)(a+b) \equiv 0 \pmod{n} \qquad (\ddagger)$$

Which we can also express as

$$(a-b)(a+b) \equiv (a-b)0 \pmod{n}$$

By Cancellation Law (3.11):

If $cx \equiv cy \pmod{n}$ and $\gcd(c, \ n) = 1$ then $x \equiv y \pmod{n}$.

Applying this corollary to the above line $(a-b)(a+b) \equiv (a-b)0 \pmod{n}$ gives

$$(a+b) \equiv 0 \pmod{n} \text{ which implies } a \equiv -b \pmod{n}$$

This last congruence $a \equiv -b \pmod{n}$ contradicts our given result

$a \not\equiv \pm b \pmod{n}$. Hence $g \neq 1$.

By combining both these cases, $g \neq 1$ and $g \neq n$, we have g is a *non-trivial* factor of n.

■

21. Creating a table of $x^5 \pmod{7}$ we have

$x \pmod{7}$	0	1	2	3	4	5	6
$x^5 \pmod{7}$	0	1	4	5	2	3	6

Since $x^5 \pmod{7}$ produces the residues 0, 1, 2, 3, 4, 5 and 6 so we have a complete residue system modulo 7.

22. (a) We need to show that $2^p \not\equiv 2 \pmod{p^2}$. Let $p = 3$ then

$$2^3 \equiv 8 \not\equiv 2 \pmod{9}$$

(b) We are asked to show $2^{1093} \equiv 2 \pmod{1093^2}$.

By using the hint $2^{364} \equiv 1 \pmod{1093^2}$ we need to write the index 1093 as a multiple of 364 and any remainder:

$$1093 = (3 \times 364) + 1$$

Applying the rules of indices, we have

$$2^{1093} \equiv 2^{(3\times 364)+1} \equiv \left(2^{364}\right)^3 \times 2^1 \equiv 1^3 \times 2 \equiv 2 \left(\text{mod } 1093^2\right)$$

We have our result.

23. We are asked to prove

$P\left(x\right) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0 \equiv 0 \left(\text{mod } p\right)$ has at most m solutions.

How do we prove this result?

By induction on the degree m.

Proof.

If $m = 1$ then we have the polynomial

$$P\left(x\right) = c_1 x + c_0 \equiv 0 \;\Rightarrow\; c_1 x \equiv -c_0 \left(\text{mod } p\right)$$

The theorem also stipulates $c_m \not\equiv 0 \left(\text{mod } p\right)$ so in our case $c_1 \not\equiv 0 \left(\text{mod } p\right)$ which implies that $p \nmid c_1$. By question 3(a) of Exercises 2.1:

> If $p \nmid a$ then $\gcd\left(p, \;\; a\right) = 1$.

Applying this result to $p \nmid c_1$ gives $\gcd\left(p, \;\; c_1\right) = 1$. Hence $c_1 x \equiv -c_0 \left(\text{mod } p\right)$ has a unique solution.

Assume the result is true for degree $m = k$:

$$P\left(x\right) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0 \equiv 0 \left(\text{mod } p\right)$$

has at most k incongruent solutions. Required to prove the case $m = k+1$:

$$P\left(x\right) = c_{k+1} x^{k+1} + c_k x^k + \cdots + c_1 x + c_0 \equiv 0 \left(\text{mod } p\right)$$

has at most $k+1$ incongruent solutions

If $P\left(x\right) \equiv 0 \left(\text{mod } p\right)$ has *no* solutions then we are finished.

Now assume $P\left(x\right) \equiv 0 \left(\text{mod } p\right)$ has at least one solution $x = a$. Therefore $P\left(x\right)$ can be divided by $x - a$ and by the Division Algorithm we have

$$P\left(x\right) = \left(x - a\right) Q\left(x\right) + R \qquad (*)$$

where $Q\left(x\right)$ is an integral coefficient polynomial of degree k and R is the remainder which in this case is an integer. Substituting $x = a$ into (*) gives

$$P\left(a\right) = \left(a - a\right) Q\left(a\right) + R \equiv R \equiv 0 \left(\text{mod } p\right)$$

Therefore the integer R satisfies $R \equiv 0 \left(\text{mod } p\right)$. Substituting this into (*) yields

$$P(x) \equiv (x-a)Q(x) + R \equiv (x-a)Q(x) \pmod{p}$$

If $x = b$ is another incongruent solution then substituting this gives

$$P(b) \equiv (b-a)Q(b) \pmod{p}$$

Since the integers a and b are incongruent which implies

$$a \not\equiv b \pmod{p} \;\Rightarrow\; a - b \not\equiv 0 \pmod{p}.$$

By Proposition (3.14) (a):

If $xy \equiv 0 \pmod{p}$ then $x \equiv 0 \pmod{p}$ or $y \equiv 0 \pmod{p}$.

Applying this to $P(b) \equiv (b-a)Q(b) \equiv 0 \pmod{p}$ gives $Q(b) \equiv 0 \pmod{p}$. This implies that any solution of $P(x) \equiv 0 \pmod{p}$ which is distinct from $x = a$ must satisfy $Q(x) \equiv 0 \pmod{p}$. By the above induction hypothesis this polynomial $Q(x) \equiv 0 \pmod{p}$ has at most k incongruent solutions. Hence the given polynomial $P(x) \equiv 0 \pmod{p}$ has at most $k+1$ incongruent solutions. By mathematical induction we have our result.

■