Complete Solutions to Exercise 4.1

1. In each case we use Fermat's Little Theorem – *FlT*.

   (a) We are required to find $7^{101} \equiv x \pmod{11}$. Since 11 is prime so we can apply *FlT*. Using

   $$a^{p-1} \equiv 1 \pmod{p}$$

   With $a = 7$ and $p = 11$ gives

   $$7^{10} \equiv 1 \pmod{11} \qquad (\dagger)$$

   Writing $101 = (10 \times 10) + 1$ we have

   $$\begin{aligned} 7^{101} &\equiv 7^{(10\times 10)+1} \\ &\equiv \left(7^{10}\right)^{10} \times 7 \qquad \left[\text{Using the rules of indices}\right] \\ &\equiv (1)^{10} \times 7 \qquad \left[\text{Because by } (\dagger) \text{ we have } 7^{10} \equiv 1 \pmod{11}\right] \\ &\equiv 7 \pmod{11} \end{aligned}$$

   Hence $7^{101} \equiv 7 \pmod{11}$ or 11 divides $7^{101} - 7$.

   (b) We need to find x which is the least non-negative residue modulo 13 in

   $$2^{1976} \equiv x \pmod{13}$$

   As 13 is prime and $13 \not| 2$ so we can use *FlT*:

   $$a^{p-1} \equiv 1 \pmod{p}$$

   Applying this with $a = 2$, $p = 13$ gives

   $$2^{12} \equiv 1 \pmod{13} \qquad (\dagger)$$

   Writing the given index 1976 in terms of a multiple of 12 plus any remainder:

   $$1976 = (164 \times 12) + 8$$

   Therefore

   $$\begin{aligned} 2^{1976} &\equiv 2^{(12\times 164)+8} \\ &\equiv \left(2^{12}\right)^{164} 2^8 \qquad \left[\text{Using the rules of indices}\right] \\ &\equiv (1)^{164} 2^8 \qquad \left[\text{By } (\dagger)\right] \\ &\equiv 2^8 \pmod{13} \end{aligned}$$

   Note that $2^4 \equiv 16 \equiv 3 \pmod{13}$. Using this in the last line of the above calculation:

$$\begin{aligned} 2^{1976} &\equiv 2^8 \\ &\equiv \left(2^4\right)^2 \equiv 3^2 \equiv 9 \left(\text{mod } 13\right) \end{aligned}$$

Hence $x \equiv 2^{1976} \equiv 9 \left(\text{mod } 13\right)$.

(c) We are given $5^{1961} \equiv x \left(\text{mod } 7\right)$. By applying *FlT* with $a = 5, \ p = 7$ gives

$$5^6 \equiv 1 \left(\text{mod } 7\right) \qquad (*)$$

We want to use this result (*) to simplify our given congruence. First we write 1961 as a multiple of 6 plus any remainder:

$$1961 = \left(326 \times 6\right) + 5$$

Using this on our given index

$$\begin{aligned} 5^{1961} &\equiv 5^{\left(326\times 6\right)+5} \\ &\equiv \left(5^6\right)^{326} \times 5^5 \\ &\equiv 1^{326} \times 5^5 \quad \left[\text{Because } 5^6 \equiv 1 \left(\text{mod } 7\right) \quad (*)\right] \\ &\equiv 5^5 \left(\text{mod } 7\right) \qquad (\dagger) \end{aligned}$$

Note that $5 \equiv -2 \left(\text{mod } 7\right)$. Replacing this in the last line gives

$$5^5 \equiv \left(-2\right)^5 \equiv -32 \equiv -4 \equiv 3 \left(\text{mod } 7\right)$$

Putting this into $(\dagger)$ yields

$$x \equiv 5^{1961} \equiv 5^5 \equiv 3 \left(\text{mod } 7\right)$$

(d) We need to find the least non-negative residue x in $3^{2013} \equiv x \left(\text{mod } 23\right)$.

Since 23 is prime and $23 \not| \ 3$ so we use *FlT*:

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

Applying this with $a = 3, \ p = 23$ we have

$$3^{22} \equiv 1 \left(\text{mod } 23\right) \qquad (*)$$

Writing 2013 in terms of a multiple of 22 plus any remainder:

$$2013 = \left(22 \times 91\right) + 11$$

Using this and (*) to simplify 3^{2013} gives

$$\begin{aligned} 3^{2013} &\equiv 3^{\left(22\times 91\right)+11} \\ &\equiv \left(3^{22}\right)^{91} \times 3^{11} \quad \left[\text{By rules of indices}\right] \\ &\equiv \underbrace{\left(1\right)^{91}}_{\text{By } (*)} \times 3^{11} \equiv 3^{11} \left(\text{mod } 23\right) \end{aligned}$$

We still need to evaluate 3^{11}. We write the index 11 in terms of a multiple of 3 and any remainder because $3^3 \equiv 27 \equiv 4 \pmod{23}$:

$$11 = (3 \times 3) + 2$$

Using this we have

$$\begin{aligned} 3^{11} &\equiv 3^{(3\times 3)+2} \\ &\equiv \left(3^3\right)^3 \times 3^2 \\ &\equiv 4^3 \times 9 \\ &\equiv 64 \times 9 \equiv -5 \times 9 \equiv -45 \equiv -22 \equiv 1 \pmod{23} \end{aligned}$$

Therefore $3^{2013} \equiv 1 \pmod{23}$. {Note that 2013 is *not* a multiple of 22 but we still get $1 \pmod{23}$, this is because $3^{11} \equiv 1 \pmod{23}$ and 2013 is a multiple of 11.

(e) We are asked to find x in the following: $26^{2013} \equiv x \pmod{23}$. This is straightforward, why?

Because $26 \equiv 3 \pmod{23}$ and using

$$a \equiv b \pmod{n} \quad \Rightarrow \quad a^k \equiv b^k \pmod{n}$$

This gives $26^{2013} \equiv 3^{2016} \underbrace{\equiv}_{\text{by part (d)}} 1 \pmod{23}$.

2. In each case we use Fermat's Little Theorem to find the inverse of the given numbers. (We could also use the result of Example 4.)

(a) We need to find the inverse of $5 \pmod{11}$. By *FlT* with $a = 5,\ p = 11$ we have

$$5^{10} \equiv 1 \pmod{11}$$

Writing $5^{10} = 5\left(5^9\right)$ in the above

$$5^{10} = 5\left(5^9\right) \equiv 1 \pmod{11}$$

Therefore the inverse of $5 \pmod{11}$ is $5^9 \pmod{11}$. We need to evaluate this.

Note that $5^2 \equiv 25 \equiv 3 \pmod{11}$ and so

$$5^4 \equiv \left(5^2\right)^2 \equiv 3^2 \equiv 9 \equiv -2 \pmod{11}$$

Writing the index 9 as a multiple of 4 plus a remainder:

$$5^9 \equiv 5^{(2\times 4)+1} \equiv \left(5^4\right)^2 5 \equiv \left(-2\right)^2 5 \equiv 20 \equiv 9 \pmod{11}$$

Hence $9\left(\text{mod } 11\right)$ is the inverse of $5\left(\text{mod } 11\right)$ or $5^{-1} \equiv 9\left(\text{mod } 11\right)$

(b) We need to find the multiplicative inverse of $9\left(\text{mod } 23\right)$. Using *FlT*:

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

With $a = 9,\ \ p = 23$ gives

$$9^{22} \equiv 1\left(\text{mod } 23\right)$$

Rewriting the index 22 as

$$9^{22} \equiv 9\left(9^{21}\right) \equiv 1\left(\text{mod } 23\right)$$

Therefore $9^{21}\left(\text{mod } 23\right)$ is the inverse of $9\left(\text{mod } 23\right)$. We need to evaluate this $9^{21}\left(\text{mod } 23\right)$ by rewriting the power 21 into smaller indices. Firstly we try to find smaller residues than 9:

$$9^3 \equiv 729 \equiv 16 \equiv -7\left(\text{mod } 23\right) \qquad (*)$$

Squaring this gives

$$\left(9^3\right)^2 \equiv \left(-7\right)^2 \equiv 49 \equiv 3\left(\text{mod } 23\right)$$

We have

$$9^6 \equiv 3\left(\text{mod } 23\right) \qquad (**)$$

Writing the above index 21 as a multiple of 6 and remainder; $21 = \left(3 \times 6\right) + 3$:

$$\begin{aligned} 9^{21} \equiv 9^{3\times 6} \times 9^3 &\equiv \left(9^6\right)^3 \times \left(-7\right) \qquad \left[\text{By } (*)\right] \\ &\equiv 3^3 \times \left(-7\right) \qquad \left[\text{By } (**)\right] \\ &\equiv 27 \times \left(-7\right) \equiv 4 \times \left(-7\right) \equiv -28 \equiv -5 \equiv 18\left(\text{mod } 23\right) \end{aligned}$$

We have $9^{-1} \equiv 18\left(\text{mod } 23\right)$.

(c) We are required to find the inverse of $2\left(\text{mod } 37\right)$. Since 37 is prime we can use Fermat's Little Theorem:

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

Applying this with $a = 2,\ \ p = 37$ we have

$$2^{36} \equiv 1\left(\text{mod } 37\right)$$

Therefore, the inverse of $2\left(\text{mod } 37\right)$ is $2^{35}\left(\text{mod } 37\right)$. The index 35 is too large to evaluate so we break this down into smaller indices. Note that

$$2^5 \equiv 32 \equiv -5\left(\text{mod } 37\right)$$

Squaring this gives

$$\left(2^5\right)^2 \equiv \left(-5\right)^2 \equiv 25 \equiv -12 \left(\text{mod } 37\right)$$

We have

$$2^{10} \equiv -12 \left(\text{mod } 37\right) \qquad (\dagger)$$

Squaring this gives

$$\left(2^{10}\right)^2 \equiv \left(-12\right)^2 \equiv 144 \equiv -4 \left(\text{mod } 37\right)$$

We have

$$2^{20} \equiv -4 \left(\text{mod } 37\right) \qquad (\dagger\dagger)$$

Writing the above index 35 as a multiple of 20 plus remainder yields

$$35 = \left(1 \times 20\right) + 15$$

Therefore

$$\begin{aligned} 2^{35} \equiv 2^{(1\times 20)+15} &\equiv 2^{20} \times 2^{15} \\ &\equiv \left(-4\right) \times 2^{15} \qquad \left[\text{By } (\dagger\dagger)\right] \\ &\equiv \left(-4\right) \times 2^{10+5} \\ &\equiv \left(-4\right) \times 2^{10} \times 2^5 \\ &\equiv \left(-4\right) \times \left(-12\right) \times \left(-5\right) \qquad \left[\text{By } (\dagger)\right] \\ &\equiv 48 \times \left(-5\right) \equiv 11 \times \left(-5\right) \equiv -55 \equiv -18 \equiv 19 \left(\text{mod } 37\right) \end{aligned}$$

The inverse of $2 \left(\text{mod } 37\right)$ is $19 \left(\text{mod } 37\right)$.

[Since $2 \times 19 \equiv 38 \equiv 1 \left(\text{mod } 37\right)$ so we could have evaluated the inverse of $2 \left(\text{mod } 37\right)$ more easily by carrying out this calculation. However the question said use *FlT*.]

(d) Since 41 is prime, we can use Fermat's Little Theorem to find the inverse of $5 \left(\text{mod } 41\right)$. We have

$$5^{40} \equiv 1 \left(\text{mod } 41\right)$$

Therefore $5^{39} \left(\text{mod } 41\right)$ is the inverse of $5 \left(\text{mod } 41\right)$. The index 39 is too large to evaluate directly. We break this down as follows:

$$5^3 \equiv 125 \equiv 2 \left(\text{mod } 41\right) \qquad (\dagger)$$

$$2^7 \equiv 128 \equiv 5 \left(\text{mod } 41\right)$$

So $\left(5^3\right)^7 \equiv 2^7 \equiv 5 \left(\text{mod } 41\right)$ or

$$5^{21} \equiv 5 \left(\text{mod } 41\right) \qquad (*)$$

We use these results to evaluate $5^{39} \left(\text{mod } 41\right)$:

$$\begin{aligned} 5^{39} \equiv 5^{21+18} &\equiv 5^{21} \times 5^{18} \\ &\equiv 5 \times 5^{18} \qquad \left[\text{By } (*)\right] \\ &\equiv 5 \times \left(5^3\right)^6 \\ &\equiv 5 \times \underbrace{\left(2\right)}_{\text{By } (\dagger)}^{6} \equiv 5 \times 2^3 \times 2^3 \equiv 40 \times 8 \equiv -1 \times 8 \equiv -8 \equiv 33 \left(\text{mod } 41\right) \end{aligned}$$

Therefore $33 \left(\text{mod } 41\right)$ is the inverse of $5 \left(\text{mod } 41\right)$ or $5^{-1} \equiv 33 \left(\text{mod } 41\right)$.

[Easier to note that $5 \times 8 \equiv 40 \equiv -1 \left(\text{mod } 41\right)$. Therefore

$$5 \times \left(-8\right) \equiv -40 \equiv 1 \left(\text{mod } 41\right) \Rightarrow 5^{-1} \equiv -8 \equiv 33 \left(\text{mod } 41\right)]$$

3. (i) *How can we find the remainder when* 6^{2014} *is divided by 11?*

Since 11 is prime and $11 \not| 6$ we can make use of *FlT*:

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

Substituting $a = 6$ and $p = 11$ into this gives

$$6^{10} \equiv 1 \left(\text{mod } 11\right)$$

We need to write the given index 2014 as a multiple of 10 plus any remainder:

$$2014 = \left(201 \times 10\right) + 4$$

Using this we have

$$\begin{aligned} 6^{2014} &\equiv 6^{\left(201 \times 10\right)+4} \\ &\equiv \left(6^{10}\right)^{201} 6^4 \equiv \left(1\right)^{210} 6^4 \equiv 6^4 \left(\text{mod } 11\right) \end{aligned}$$

We know $6^2 = 36$ which is 3 modulo 11. Therefore

$$6^{2014} \equiv 6^4 \equiv \left(6^2\right)^2 \equiv 3^2 \equiv 9 \left(\text{mod } 11\right)$$

The remainder is 9.

(ii) We can use the calculation of part (i) to find the remainder of 6^{2013} when divided by 11. We have

$$6^{2013} \equiv 6^{\left(201 \times 10\right)+3} \equiv 6^3 \left(\text{mod } 11\right)$$

Evaluating 6^3 modulo 11 we have

$$6^{2013} \equiv 6^3 \equiv 6^2 \times 6 \equiv 3 \times 6 \equiv 18 \equiv 7 \left(\text{mod } 11\right)$$

The remainder is 7.

4. (i) Using *FlT* with $p = 23,\ a = 8$:

$$8^{22} \equiv 1 \pmod{23} \qquad (*)$$

The multiplicative inverse of $8 \pmod{23}$ is $8^{21} \pmod{23}$ because

$$8^{22} \equiv 8\left(8^{21}\right) \equiv 1 \pmod{23} \quad \text{[Using (*)]}$$

We need to find $8^{21} \pmod{23}$. Since $8 \times 3 \equiv 24 \equiv 1 \pmod{23}$ so $8^{-1} \equiv 3 \pmod{23}$ because

$$8\left(8^{21}\right) \equiv 8(3) \equiv 1 \pmod{23}$$

Therefore

$$8^{21} \equiv 3 \pmod{23}.$$

(ii) We need to solve $8x \equiv 7 \pmod{23}$. By part (i) we have the inverse of $8 \pmod{23}$ is $3 \pmod{23}$ so multiplying both sides of $8x \equiv 7 \pmod{23}$ by 3 gives

$$x \equiv 7 \times 3 \equiv 21 \pmod{23}.$$

Our solution is $x \equiv 21 \pmod{23}$.

5. (a) We need to show that $2^{8190} \equiv 1 \pmod{8191}$. Evaluating a power of 2 which is close to 8191 is $2^{13} = 8192 \equiv 1 \pmod{8191}$. We can write the given index 8190 as a multiple of 13 plus any remainder:

$$8190 = 630 \times 13$$

Therefore we have $2^{8190} \underset{\substack{\text{by rules} \\ \text{of indices}}}{\equiv} \left(2^{13}\right)^{630} \equiv 1 \pmod{8191}$. We cannot be certain but it is likely that 8191 is prime.

(b) We need to show that $2^{65\,536} \equiv 1 \pmod{65\,537}$. Evaluating powers of 2 modulo 65 537:

$$2^{16} \equiv 65\,536 \equiv -1 \pmod{65\,537}.$$

Writing the given index 65 536 as a multiple of 16 and any remainder:

$$65\,536 = 16 \times 4096$$

Hence $2^{65\,536} \equiv 2^{16\times 4096} \equiv \left(2^{16}\right)^{4096} \equiv \left(-1\right)^{4096} \equiv 1 \left(\text{mod } 65\,537\right)$. Therefore 65 537 is likely to be prime but we *cannot* be certain because 65 537 maybe a pseudoprime.

6. We are required to show that $2^{2046} \equiv 1 \left(\text{mod } 2047\right)$. Evaluating powers of 2:

$$2^{11} \equiv 2048 \equiv 1 \left(\text{mod } 2047\right).$$

Writing the given index 2046 as a multiple of 11 plus any remainder gives

$$2046 = 186 \times 11.$$

Therefore, we have

$$2^{2046} \equiv \left(2^{11}\right)^{186} \equiv \left(1\right)^{186} \equiv 1 \left(\text{mod } 2047\right).$$

We have shown our required result $2^{2046} \equiv 1 \left(\text{mod } 2047\right)$.

However, 2047 is not prime because $2047 = 23 \times 89$.

Remember

$$a^{n-1} \equiv 1 \left(\text{mod } n\right) \quad \not\Rightarrow \quad n \text{ is prime}$$

In our case 2047 is composite.

7. We need to show that $7^{40\,353\,606} \equiv 0 \left(\text{mod } 40\,353\,607\right)$. Finding an appropriate power of 7 by evaluating:

$$7^9 \equiv 40\,353\,607 \equiv 0 \left(\text{mod } 40\,353\,607\right)$$

We have

$$7^{40\,353\,607} \equiv 7^9 \times 7^{40\,353\,607-9} \equiv 0 \times 7^{40\,353\,598} \equiv 0 \left(\text{mod } 40\,353\,607\right).$$

Since 40 353 607 is a power of 7, so 7 is a factor of 40 353 607 so it *cannot* be a prime.

8. Since we are given $2^{1\,234\,566} \equiv 899\,557 \left(\text{mod } 1\,234\,567\right)$ so

$$2^{1\,234\,566} \equiv 899\,557 \not\equiv 1 \left(\text{mod } 1\,234\,567\right)$$

Therefore 1 234 567 is definitely composite.

9. We need to find x such that $x^{101} \equiv 5 \left(\text{mod } 13\right)$. Since 13 is prime so we have by *FlT*:

$$x^{12} \equiv 1 \pmod{13} \qquad (*)$$

We need to write the index 101 as a multiple of 12 plus any remainder:

$$101 = (8 \times 12) + 5$$

Therefore rewriting x^{101} as

$$x^{101} \equiv x^{(8\times 12)+5} \equiv \left(x^{12}\right)^8 x^5 \equiv (1)^8 x^5 \equiv x^5 \equiv 5 \pmod{13}$$

We need to solve the equation $x^5 \equiv 5 \pmod{13}$. Creating a table of values for $x^5 \pmod{13}$:

x	1	2	3	4	**5**	6	7	8	9	10	11	12
$x^5 \pmod{13}$	1	6	9	10	**5**	*	*	*	*	*	*	*

Since $x \equiv 5 \pmod{13}$ satisfies $x^5 \equiv 5 \pmod{13}$ so we don't need to evaluate the remaining entries in the table. That is why we have * in the remaining entries.

Hence one solution of $x^{101} \equiv 5 \pmod{13}$ is $x \equiv 5 \pmod{13}$.

10. (a) *Proof.*

Since p is prime so by *FlT* we have

$$a^{p-1} \equiv 1 \pmod{p}$$

Applying this to each of the residues 1, 2, 3, 4, $\cdots$, $p-1$ gives

$$\begin{aligned} 1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} &\equiv \underbrace{1+1+1+\cdots+1}_{=p-1} \\ &\equiv p-1 \equiv -1 \pmod{p} \end{aligned}$$

This completes our proof. ∎

(b) *Proof.*

By Corollary (4.2):

$$a^p \equiv a \pmod{p}$$

Applying this to each of the least positive residues:

$$1^p \equiv 1\,,\ 2^p \equiv 2\,,\ 3^p \equiv 3\,,\ \cdots,\ (p-1)^p \equiv (p-1) \pmod{p}$$

Using these in the calculation below:

$$1^p + 2^p + 3^p + \cdots + \left(p-1\right)^p \equiv 1 + 2 + 3 + \cdots + \left(p-1\right)$$
$$\equiv \frac{p\left(p-1\right)}{2} \pmod{p} \qquad \left[\begin{array}{l}\text{Using the given hint:} \\ 1 + 2 + \cdots + m = \dfrac{m\left(m+1\right)}{2}\end{array}\right]$$

We are given that p is an odd prime so $\dfrac{p-1}{2}$ is an integer k say. This implies that

$$1^p + 2^p + 3^p + \cdots + \left(p-1\right)^p \equiv \frac{p\left(p-1\right)}{2} \equiv kp \equiv 0 \pmod{p}$$

This completes our proof.

■

11. (i) We need to prove that the solution of the equation $nx \equiv a \pmod{p}$ is given by

$$x \equiv n^{p-2}a \pmod{p}$$

Proof.

By Example 4 we have the multiplicative inverse of $n \pmod{p}$ is $n^{p-2} \pmod{p}$. Multiplying both sides of the given equation $nx \equiv a \pmod{p}$ by n^{p-2} gives

$$n^{p-2}\left(nx\right) \equiv \underbrace{n^{p-2}n}_{\substack{\equiv 1 \text{ because} \\ n^{p-2} \text{ is the inverse}}} \quad x \equiv \left(1\right)x \equiv x \equiv n^{p-2}a \pmod{p}$$

Hence we have $x \equiv n^{p-2}a \pmod{p}$ which is our required result.

■

(ii) We need to solve the equation $10x \equiv 11 \pmod{17}$. If we try to solve the equivalent Diophantine equation, we have

$$10x = 11 + 17y \;\Rightarrow\; x = \frac{11 + 17y}{10}$$

This is going to be pretty tedious, because after trialling various integers for y, I found the solution $x = -33, y = -55$. Easier to use modular arithmetic.

Now we need to substitute appropriate values for y so that x is an integer. Since 17 is prime so we can use the result of part (i):

$$x \equiv 10^{17-2} \times 11 \equiv 10^{15} \times 11 \pmod{17} \qquad (*)$$

We have to evaluate $10^{15} \pmod{17}$ in order to find x. Trying some simpler values of the index:

$$10^2 \equiv 100 \equiv -2 \pmod{17} \qquad (\dagger)$$

$$(-2)^4 \equiv 16 \equiv -1 \pmod{17}$$

Easier to work with residue -1 rather than 10. We have

$$(10^2)^4 \equiv (-2)^4 \equiv -1 \pmod{17} \text{ implies } 10^8 \equiv -1 \pmod{17}$$

Writing 15 as a multiple of 8 plus any remainder:

$$15 = (1 \times 8) + 7$$

Therefore

$$\begin{aligned} 10^{15} &\equiv 10^{(1\times 8)+7} \\ &\equiv (10^8) \times 10^7 \\ &\equiv (-1) \times 10^{(2\times 3)+1} \\ &\equiv (-1) \times \underbrace{(-2)^3}_{\text{by } (\dagger)} \times 10 \equiv 80 \equiv -5 \pmod{17} \end{aligned}$$

Putting this $10^{15} \equiv -5 \pmod{17}$ into (*) gives

$$x \equiv 10^{15} \times 11 \equiv -5 \times 11 \equiv -55 \equiv -4 \equiv 13 \pmod{17}$$

Hence solving $10x \equiv 11 \pmod{17}$ gives $x \equiv 13 \pmod{17}$.

12. We need to find x which is the least non-negative residue such that

$$3^{2013} \equiv x \pmod{43}$$

Recall that 43 is prime and 43 does *not* divide 3 so we can use *FlT*:

$$a^{p-1} \equiv 1 \pmod{p}$$

We have

$$3^{42} \equiv 1 \pmod{43}$$

By applying the Division Algorithm to 2013 with multiple of 43 and any remainder we have

$$2013 = (47 \times 42) + 39$$

Using the rules of indices gives

$$\begin{aligned} 3^{2013} \equiv 3^{(47\times 42)+39} &\equiv (3^{42})^{47}\, 3^{39} \\ &\equiv (1)^{47}\, 3^{39} \equiv 3^{39} \pmod{43} \qquad (\dagger) \end{aligned}$$

We need to evaluate 3^{39} modulo 43 in (†). Evaluating simple powers of 3:

$$3^3 \equiv 27,\ \ 3^4 \equiv 38,\ \ 3^5 \equiv 28,\ \ 3^6 \equiv 41 \equiv -2 \pmod{43}$$

So far the simplest power to use is $3^6 \equiv -2 \pmod{43}$. Using this index:

$$\begin{aligned} 3^{39} \equiv 3^{(6\times 6)+3} &\equiv \left(3^6\right)^6 \times 3^3 \\ &\equiv \left(-2\right)^6 \times 27 \equiv 64 \times 27 \equiv 21 \times 27 \equiv 567 \equiv 8 \pmod{43} \end{aligned}$$

By (†) we have $3^{2013} \equiv 3^{39} \equiv 8 \pmod{43}$.

Hence the remainder of 3^{2013} when divided by 43 is 8.

13. We are asked to evaluate the least positive residue x modulo 103 such that

$$3^{101} \equiv x \pmod{103}$$

We know 103 is prime so by *FlT* we have

$$3^{102} \equiv 1 \pmod{103} \qquad (*)$$

However we are interested in finding $3^{101} \equiv x \pmod{103}$. *How can we use (*) to determine this x?*

By rewriting the index 102 as $102 = 101 + 1$:

$$3^{102} \equiv 3^{1+101} \equiv 3 \times 3^{101} \equiv 1 \pmod{103}$$

This $3 \times 3^{101} \equiv 1 \pmod{103}$ implies that $3^{101} \pmod{103}$ is the inverse of $3 \pmod{103}$, so $3^{-1} \equiv 3^{101} \pmod{103}$. Let $x = 3^{101}$ then

$$3x \equiv 1 \pmod{103} \qquad (**)$$

From the test of divisibility of 3 we know that $3 \mid 102$, actually $3 \times 34 = 102$.

Using this yields

$$3 \times 34 \equiv 102 \equiv -1 \pmod{103}$$

Multiplying both sides of this $3 \times 34 \equiv -1 \pmod{103}$ by -1 gives

$$3 \times \left(-34\right) \equiv 1 \pmod{103} \text{ and so } x \equiv -34 \equiv 69 \pmod{103}$$

Hence $x \equiv 69 \pmod{103}$. Multiplying both sides of (**) by $69 \pmod{103}$ gives

$$\underbrace{69 \times 3}_{\equiv 1 \pmod{103}} \times x \equiv 1 \times 69 \equiv 69 \pmod{103}$$

We have $x \equiv 3^{101} \equiv 69 \pmod{103}$.

14. (i) We need to show product of any three consecutive integers is divisible by 3.

Proof.

Let $n-1, n, n+1$ be three consecutive integers. The product of these is given by

$$(n-1)\times n\times(n+1) = n(n^2-1) = n^3 - n \qquad (*)$$

Using the corollary to *FlT* (4.2):

$$n^p \equiv n \pmod{p}$$

with prime $p = 3$ gives

$$n^3 \equiv n \pmod{3} \quad \Leftrightarrow \quad n^3 - n \equiv 0 \pmod{3}$$

From this $n^3 - n \equiv 0 \pmod{3}$ we have $3 \mid (n^3 - n)$, Therefore by (*) we have

$$3 \mid (n-1)\times n\times(n+1)$$

Hence 3 divides the product of three consecutive integers. ■

(ii) We need to show product of any three consecutive integers is divisible by 6.

Proof.

Let $n-1, n, n+1$ be three consecutive integers. Then by Example 6 we have 2 divides any two consecutive integers so $2 \mid \big((n-1)\times n\times(n+1)\big)$. By part (i) we have $3 \mid \big((n-1)\times n\times(n+1)\big)$. The $\gcd(2, 3) = 1$ so by question 12 (i) of Exercises 1.3:

If $a \mid c$ and $b \mid c$, and $\gcd(a, b) = 1$ then $(a\times b) \mid c$.

We have

$$(2\times 3) \mid \big((n-1)\times n\times(n+1)\big) \Rightarrow 6 \mid \big((n-1)\times n\times(n+1)\big)$$

Hence 6 divides three consecutive integers. ■

15. The integer 211 is prime but $1055^{210} \not\equiv 1 \pmod{211}$ because $211 \mid 1055$.

Remember *FlT* only works when the prime p does *not* divide a where $a^{p-1} \equiv 1 \pmod{p}$.

16. This time we need to show that $\dfrac{25n^{61}+52n}{77}$ is an integer.

Proof.

We need to show that

$$25n^{61}+52n \equiv 0 \pmod{77} \qquad (\ddagger)$$

because by the definition of congruence this implies that $77 \mid \left(25n^{61}+52n\right)$ or $25n^{61}+52n$ is a multiple of 77.

The prime decomposition of 77 is 7×11.

Applying Fermat's Little Theorem (4.1):

$$n^{p-1} \equiv 1 \pmod{p} \text{ provided } p \nmid n$$

To the primes 7 and 11 gives

$$n^{6} \equiv 1 \pmod{7} \qquad (*)$$

$$n^{10} \equiv 1 \pmod{11} \qquad (**)$$

We use this to find n^{61}:

$$n^{61} \equiv \left(n^{6}\right)^{10} n \equiv n \pmod{7} \quad [\text{By } (*)]$$

This result is also true when $7 \mid n$ because then $n^{61} \equiv n \equiv 0 \pmod{7}$.

Similarly with modulo 11 we have

$$n^{61} \equiv \left(n^{10}\right)^{6} n \equiv n \pmod{11} \quad [\text{By } (**)]$$

We now use the hint:

$$a \equiv b \pmod{m_k} \Rightarrow a \equiv b \pmod{m_1 \times m_2 \times \cdots \times m_n} \text{ where } k = 1, 2, \cdots, n$$

Using this with

$$n^{61} \equiv n \pmod{7} \text{ and } n^{61} \equiv n \pmod{11}$$

Gives $n^{61} \equiv n \pmod{77}$. Putting this into the left hand side of $(\ddagger)$ yields

$$25n^{61}+52n \equiv 25n+52n \equiv 77n \equiv 0 \pmod{77}.$$

Hence $\dfrac{25n^{61}+52n}{77}$ is an integer. This completes our proof.

■

17. This time we need to show that $\dfrac{12n^{13}+23n}{35}$ is an integer.

Proof.

We show that

$$12n^{13} + 23n \equiv 0 \pmod{35} \qquad (\ddagger)$$

because by the definition of congruence this implies that $35 \mid \left(12n^{13} + 23n\right)$ or $12n^{13} + 23n$ is a multiple of 35.

The prime decomposition of 35 is 5×7.

Applying Fermat's Little Theorem (4.1):

$$n^{p-1} \equiv 1 \pmod{p} \text{ provided } p \nmid n$$

To the primes 5 and 7 gives

$$n^4 \equiv 1 \pmod{5} \qquad (*)$$

$$n^6 \equiv 1 \pmod{7} \qquad (**)$$

We use this to find n^{13}:

$$n^{13} \equiv \left(n^4\right)^3 n \equiv n \pmod{5} \quad [\text{By } (*)]$$

This result is also true when $5 \mid n$ because then $n^{13} \equiv n \equiv 0 \pmod{5}$.

Similarly with modulo 7 we have

$$n^{13} \equiv \left(n^6\right)^2 n \equiv n \pmod{7} \quad [\text{By } (**)]$$

We now use the following result:

$$a \equiv b \pmod{m_k} \Rightarrow a \equiv b \pmod{m_1 \times m_2 \times \cdots \times m_n} \text{ where } k = 1, 2, \cdots, n$$

Applying this to

$$n^{13} \equiv n \pmod{5} \text{ and } n^{13} \equiv n \pmod{7}$$

Gives $n^{13} \equiv n \pmod{35}$. Putting this into the left hand side of $(\ddagger)$ yields

$$12n^{13} + 23n \equiv 12n + 23n = 35n \equiv 0 \pmod{35}$$

Hence $\dfrac{12n^{13} + 23n}{35}$ is an integer. This completes our proof.

■

18. We need to prove that $n^{k(p-1)} \equiv 1 \pmod{p}$.

Proof.

Since p is prime and $p \nmid n$ so by *FlT* we have

$$n^{p-1} \equiv 1 \pmod{p}$$

Let k be a natural number then

$$n^{k(p-1)} \equiv \left[n^{(p-1)}\right]^k \equiv (1)^k \equiv 1 \pmod{p}$$

We have $n^{k(p-1)} \equiv 1 \pmod{p}$ which is our required result.

■

19. We need to show that $n^{\frac{p-1}{2}} \pmod{p}$ is its own inverse.

Proof.

Finding the product of $n^{\frac{p-1}{2}} \pmod{p}$ and $n^{\frac{p-1}{2}} \pmod{p}$ gives

$$n^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv n^{\frac{p-1}{2}+\frac{p-1}{2}} \equiv n^{2\left(\frac{p-1}{2}\right)} \equiv n^{p-1} \equiv 1 \pmod{p}$$

Hence $n^{\frac{p-1}{2}} \pmod{p}$ is the multiplicative inverse of $n^{\frac{p-1}{2}} \pmod{p}$.

This completes our proof.

■

20. We need to show that $x^{p+1} \equiv 4 \pmod{p} \quad \Rightarrow \quad x \equiv 2 \text{ or } x \equiv -2 \pmod{p}$.

Proof.

Since p is prime and x is a positive residue modulo p so p does *not* divide into x. By *FlT* we have

$$x^{p-1} \equiv 1 \pmod{p} \qquad (*)$$

Rewriting the index in the given congruence $x^{p+1} \equiv 4 \pmod{p}$:

$$x^{p+1} \equiv x^{p-1+2} \equiv \underbrace{x^{p-1}}_{\equiv 1 \text{ by } (*)} x^2 \equiv x^2 \equiv 4 \pmod{p}.$$

We need to solve $x^2 \equiv 4 \pmod{p}$ which we can write as $x^2 \equiv 2^2 \pmod{p}$.

Applying (3.14)(b):

$$a^2 \equiv b^2 \pmod{p} \Leftrightarrow a \equiv \pm b \pmod{p}$$

We have

$$x^2 \equiv 2^2 \pmod{p} \quad \Rightarrow \quad x \equiv \pm 2$$

Hence we have our solution $x \equiv 2$ or $x \equiv -2 \pmod{p}$.

■

21. We need to show $n^{2^p} \equiv n^2 \pmod{2^p - 1}$.

Proof.

Since we are given that 2^p-1 is prime and 2^p-1 does *not* divide n so we can use *FlT*:

$$n^{2^p-2} \equiv 1 \left(\text{mod } 2^p-1\right) \qquad (*)$$

We can write the index 2^p as $2^p = 2^p-2+2$:

$$n^{2^p} \equiv n^{2^p-2+2} \equiv n^2 \times n^{2^p-2} \equiv n^2 \times \underbrace{1}_{\text{by (*)}} \equiv n^2 \left(\text{mod } 2^p-1\right)$$

We have shown that $n^{2^p} \equiv n^2 \left(\text{mod } 2^p-1\right)$.

■

22. We are required to prove $a^p \equiv b^p \left(\text{mod } p\right) \Rightarrow a \equiv b \left(\text{mod } p\right)$.

Proof.

We consider two cases:

Case I): $p \mid a$ or $p \mid b$ Case II) $p \nmid a$ and $p \nmid b$

If $p \mid a$ then $a \equiv 0 \left(\text{mod } p\right) \Rightarrow a^p \equiv 0^p \equiv 0 \left(\text{mod } p\right)$. We are given $a^p \equiv b^p \left(\text{mod } p\right)$ so

$$a^p \equiv b^p \equiv 0 \left(\text{mod } p\right)$$

From $b^p \equiv 0 \left(\text{mod } p\right)$ we need to show that $b \equiv 0 \left(\text{mod } p\right)$.

Since p is prime so we can apply the result of question 10 of Exercises 3.2:

> If $c^n \equiv 0 \left(\text{mod } p\right)$ where p is prime then $c \equiv 0 \left(\text{mod } p\right)$.

Applying this to $b^p \equiv 0 \left(\text{mod } p\right)$ gives $b \equiv 0 \left(\text{mod } p\right)$. Therefore if $p \mid a$ we have $a \equiv b \equiv 0 \left(\text{mod } p\right)$. Similar if $p \mid b$.

If $p \nmid a$ and $p \nmid b$ then by *FlT* we have

$$a^{p-1} \equiv b^{p-1} \equiv 1 \left(\text{mod } p\right) \qquad (\dagger)$$

Using this on the given congruence $a^p \equiv b^p \left(\text{mod } p\right)$ yields

$$a^p \equiv a\underbrace{\left(a^{p-1}\right)}_{\equiv 1} \equiv a \equiv b^p \equiv b\underbrace{\left(b^{p-1}\right)}_{\equiv 1} \equiv b \left(\text{mod } p\right) \qquad [\text{By } (\dagger)]$$

Hence we have $a \equiv b \left(\text{mod } p\right)$.

■

23. *How do we show p divides $\big(1-n\big)\big(1+n+n^2+n^3+\cdots+n^{p-2}\big)$?*

We prove

$$\big(1-n\big)\big(1+n+n^2+n^3+\cdots+n^{p-2}\big)\equiv 0\ \big(\mathrm{mod}\ p\big)$$

We use the identity

$$\big(1-x\big)\big(1+x+x^2+x^3+\cdots+x^{m-1}\big)=1-x^m \qquad (\dagger)$$

Proof.

Substituting $x=n$ and $m=p-1$ into $(\dagger)$ gives

$$\big(1-n\big)\big(1+n+n^2+n^3+\cdots+n^{p-2}\big)=1-n^{p-1}$$

Since p is prime and $p \not| n$ so by *FlT* we have

$$n^{p-1}\equiv 1\ \big(\mathrm{mod}\ p\big) \quad\Leftrightarrow\quad n^{p-1}-1\equiv 1-n^{p-1}\equiv 0\ \big(\mathrm{mod}\ p\big)$$

Combining these two results we have

$$\big(1-n\big)\big(1+n+n^2+n^3+\cdots+n^{p-2}\big)\equiv 1-n^{p-1}\equiv 0\ \big(\mathrm{mod}\ p\big)$$

This is our required result; $p \mid \Big[\big(1-n\big)\big(1+n+n^2+\cdots+n^{p-2}\big)\Big]$.

■