Complete Solutions to Supplementary Problems 5

1. (i) First, we find the prime decomposition of 100:

$$100 = 2^2 \times 5^2 .$$

Using formula (5.9):

$$\boxed{\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)}$$

Evaluating the Euler Totient function we have

$$\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40 .$$

(ii) To find the last two digits of 2013^{2013} we apply Euler's Theorem:

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ provided } \gcd(a,\ n) = 1 .$$

First note that $2013 \equiv 13 \pmod{100}$. By Euler's Theorem and the result of part (i) we have

$$13^{40} \equiv 1 \pmod{100} \qquad \left[\text{Because } \phi(100) = 40\right]$$

So far

$$2013^{40} \equiv 13^{40} \equiv 1 \pmod{100} \qquad (*)$$

Applying the division algorithm to write the index 2013 in terms of 40:

$$2013 = (40 \times 50) + 13 .$$

Therefore using (*) we have

$$2013^{2013} \equiv \left(13^{40}\right)^{50} \times 13^{13} \underbrace{\equiv}_{\text{By } (*)} 1^{50} \times 13^{13} \equiv 13^{13} \pmod{100} .$$

Finding powers of 13 gives

$$13^3 \equiv 2197 \equiv -3 \pmod{100} .$$

Using this result we have

$$\begin{aligned} 2013^{2013} &\equiv 13^{13} \equiv \left(13^3\right)^4 \times 13 \qquad \left[\text{Writing index } 13 = (3\times 4)+1\right] \\ &\equiv (-3)^4 \times 13 \equiv 81 \times 13 \equiv 1053 \equiv 53 \pmod{100} \end{aligned}$$

The last two digits of 2013^{2013} are 53.

(iii) We need to find the last two digits of $2013^{2013^{2013}}$. We use the result of (*) given in part (ii).

First, we need to find $2013^{2013} \equiv x \pmod{40}$ where x is the least non – negative residue modulo 40. Note that $2013 \equiv 13 \pmod{40}$ so

$$2013^{2013} \equiv 13^{2013} \equiv x \pmod{40} \qquad (**)$$

Since 13 and 40 are relatively prime so we can use Euler's Theorem with $\phi(40)$ which is given by

$$\phi(40) = 40\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 16.$$

By Euler's Theorem we have

$$13^{16} \equiv 1 \pmod{40} \qquad (\dagger)$$

Writing the index 2013 in (**) as a multiple of 16 and any remainder we have

$$2013 = (125 \times 16) + 13.$$

Using the rules of indices in (**) and the result of (†) we have

$$2013^{2013} \equiv 13^{2013} \equiv 13^{(125\times16)+13} \equiv \left(13^{16}\right)^{125} \times 13^{13} \equiv 13^{13} \pmod{40}.$$

Evaluating simpler powers of 13 we have

$$13^2 \equiv 169 \equiv 9 \pmod{40} \quad \text{and} \quad 9^2 \equiv 81 \equiv 1 \pmod{40}.$$

Combining these gives $13^4 \equiv 1 \pmod{40}$. Hence

$$2013^{2013} \equiv 13^{13} \equiv \left(13^4\right)^3 \times 13 \equiv 1 \times 13 \equiv 13 \pmod{40}.$$

Therefore $2013^{2013} = 40k + 13$.

To find the last two digits of $2013^{2013^{2013}}$, we apply Euler's Theorem;

$$2013^{2013^{2013}} \equiv y \pmod{100}.$$

Substituting the index $2013^{2013} = 40k + 1$ and now using (*) yields

$$2013^{2013^{2013}} \equiv 2013^{40k+13} \equiv \left(2013^{40}\right)^k \times 2013^{13} \equiv 1 \times 13^{13} \equiv 53 \pmod{100}.$$

The last two digits of $2013^{2013^{2013}}$ is 53.

(iv) Because the $\gcd(100,\ 2014) = 2$.

2. In each case we write the given integer into its prime factors and then use the formula (5.9):

$$\boxed{\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)}$$

(a) The prime decomposition of 1000 is evaluated by:

$$\frac{1000}{8} = 125 \quad \text{and} \quad 125 = 5^3.$$

Therefore $1000 = 8 \times 5^3 = 2^3 \times 5^3$. Using the above formula, we have

$$\phi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400.$$

(b) Using that $10\ 000 = 10 \times 1000$ we have

$$10\ 000 = 10 \times 1000 = 10 \times 2^3 \times 5^3 = 2 \times 5 \times 2^3 \times 5^3 = 2^4 \times 5^4.$$

Again using the above formula

$$\phi(10\ 000) = 10\ 000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4000.$$

(c) The prime factors of 100 000 are 2 and 5 so

$$\phi(100\ 000) = 100\ 000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40\ 000.$$

(d) Similarly we have

$$\phi(1\,000\,000) = 1\,000\,000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400\,000.$$

Since each of these numbers has the same prime factors, 2 and 5, so

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = \frac{4}{10} = \frac{2}{5}.$$

The given integer n is 10 times larger than the previous integer so each time we have $\phi(n)$ is 10 times larger as well.

3. (a) We need to evaluate $\phi(2014)$. The prime factorization of 2014 can be evaluated by:

$$\frac{2014}{2} = 1007 \qquad (*)$$

We don't know whether 1007 is prime or composite so we need to test it.

Let p be a prime factor of 1007 then it must satisfy:

$$p \le \left\lfloor \sqrt{1007} \right\rfloor = 31.$$

Clearly 2, 3 and 5 are not factors of 1001. Nor is 7, 11, 13 and 17 but 19 is a factor of 1007 because

$$\frac{1007}{19} = 53 \text{ and 53 is prime.}$$

Therefore $1007 = 19 \times 53$ which implies from (*) we have

$$2014 = 2 \times 19 \times 53.$$

Using the formula $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$ with the above primes:

$$\phi(2014) = 2014\left(1-\frac{1}{2}\right)\left(1-\frac{1}{19}\right)\left(1-\frac{1}{53}\right) = 936.$$

(b) Similarly, factorizing 2015 gives

$$\frac{2015}{5} = 403 \qquad (\ddagger)$$

We need to test whether 403 is a prime or composite integer. Let p be a prime factor of 403 then $p \le \left\lfloor \sqrt{403} \right\rfloor = 20$.

The prime numbers 2, 3, 5 and 11 are not factors of 403. Nor is 7 a factor. However, 13 is a factor of 403 because

$$\frac{403}{13} = 31 \quad \Rightarrow \quad 403 = 13 \times 31 \text{ and 31 is prime.}$$

Using ($\ddagger$) we have $2015 = 5 \times 403 = 5 \times 13 \times 31$.

Applying the Euler totient formula gives

$$\phi(2015) = 2015\left(1-\frac{1}{5}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{31}\right) = 1440.$$

(c) Factorizing 2016 we have

$$\frac{2016}{32} = 63.$$

And $63 = 9 \times 7 = 3^2 \times 7$. Remember $32 = 2^5$ so we have

$$2016 = 32 \times 63 = 2^5 \times 3^2 \times 7.$$

The only prime factors of 2016 are 2, 3 and 7, therefore

$$\phi(2016) = 2016\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) = 576.$$

(d) We are given that 2017 is prime so we use Proposition (5.2):

If p is prime, then $\phi(p) = p-1$.

$$\phi(2017) = 2017 - 1 = 2016.$$

4. We need to find natural numbers such that $\phi(n) = \frac{4n}{5}$. Using the formula for $\phi(n)$ we have

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) = \frac{4}{5}n.$$

The prime 5 must be a factor of n because on the right-hand side we have a denominator of 5. Also $1-\frac{1}{5}=\frac{4}{5}$ therefore there is only one prime factor of n which is 5. Hence $n=5^m$ where m is a natural number.

5. We need to find the last three digits of 2011^{2011}. This means we need to work with modulo 1000. From solution to question 2(a) we have

$$\phi(1000)=400.$$

We use Euler's Theorem (5.14):

$$\boxed{a^{\phi(n)}\equiv 1 \pmod{n} \text{ provided } \gcd(a,\ n)=1}$$

In order to apply this we first need to evaluate $\gcd(1000,\ 2011)$. By the Euclidean algorithm we have

$$\begin{aligned}2011&=(2\times 1000)+11\\ 1000&=(90\times 11)+10\\ 11&=(1\times 10)+1\end{aligned}$$

The $\gcd(1000,\ 2011)=1$ so we can apply Euler's Theorem:

$$2011^{\phi(1000)}\equiv 2011^{400}\equiv 1 \pmod{1000} \qquad (*)$$

We need to find $2011^{2011}\equiv ? \pmod{1000}$.

Simplifying this $2011\equiv 11 \pmod{1000}$ because it is easier to work with residue 11 rather than 2011. This implies that we have to evaluate

$$2011^{2011}\equiv 11^{2011}\equiv ? \pmod{1000} \qquad (**)$$

By (*) we have $2011^{400}\equiv 11^{400}\equiv 1 \pmod{1000}$. Writing the index 2011 in terms of 40 by using the division algorithm:

$$2011=(5\times 400)+11.$$

Using this in (**) yields

$$11^{2011}\equiv 11^{(5\times 400)+11}\equiv \left(11^{400}\right)^5\times 11^{11}\equiv 11^{11} \pmod{1000} \qquad (\dagger)$$

We need to find the least non-negative residue $11^{11} \pmod{1000}$. Evaluating powers of 11 gives

$$11^2\equiv 121,\ \ 11^3\equiv 1331,\ \ 11^4\equiv 641,\ \ 11^5\equiv 51 \pmod{1000}.$$

Writing the index 11 as a multiple of 5 plus any remainder and working out the least non-negative residue we have

$$11^{11} \equiv 11^{(5\times2)+1} \equiv \left(11^5\right)^2 \times 11 \equiv 51^2 \times 11 \equiv 611 \pmod{1000}.$$

Putting this into (†) gives $11^{2011} \equiv 611 \pmod{1000}$. The last three digits of 2011^{2011} is 611.

6. Since we are given that n is odd so $\gcd\left(2^m,\ n\right) = 1$. Applying the multiplicative property of the ϕ function to the given $\phi\left(2^m n\right)$ we have

$$\begin{aligned}\phi\left(2^m n\right) &= \phi\left(2^m\right)\phi(n)\\ &= 2^m\left(1-\frac{1}{2}\right)\phi(n) = 2^m\left(\frac{1}{2}\right)\phi(n) = 2^{m-1}\phi(n)\end{aligned}$$

7. We need to solve $23x \equiv 5 \pmod{100}$. If we try to solve the equivalent Diophantine equation, then we would need to solve

$$23x - 100y = 1 \ \Rightarrow\ x = \frac{1+100y}{23}.$$

This is difficult to solve because we need both x and y to be integers.
We use the result established in question 12(b) of Exercises 5.2:

If $\gcd\left(a,\ n\right) = 1$ and $ax \equiv b \pmod{n}$ then $x \equiv ba^{\phi(n)-1}$.

We use this $x \equiv a^{\phi(n)-1}b \pmod{n}$ to solve $23x \equiv 5 \pmod{100}$. First, we need to check that $\gcd\left(23,\ 100\right) = 1$ which it is.
We have evaluated $\phi(100) = 40$ in question 1(i). Using the given result with $a = 23$, $b = 5$ and $n = 100$ we have:

$$x \equiv a^{\phi(n)-1} \times b \equiv 23^{40-1} \times 5 \equiv 23^{39} \times 5 \pmod{100} \qquad (\ddagger)$$

Evaluating powers of 23:

$$23^2 \equiv 29,\ 23^3 \equiv 67,\ 23^4 \equiv 41,\ 23^5 \equiv 43,\ 23^6 \equiv 89 \equiv -11 \pmod{100}.$$

Working with -11 is much easier than working with 23. Writing the index 39 as a multiple of 6 and a remainder gives

$$39 = (6\times 6) + 3.$$

Therefore, we have

$$23^{39} \equiv 23^{(6\times6)+3} \equiv \left(23^6\right)^6 \times 23^3 \equiv (-11)^6 \times 23^3 \equiv 61 \times 67 \equiv 87 \pmod{100}.$$

Substituting this result $23^{39} \equiv 87 \pmod{100}$ into (‡) gives

$$x \equiv 23^{39} \times 5 \equiv 87 \times 5 \equiv 35 \pmod{100}.$$

The solution of $23x \equiv 5 \pmod{100}$ is $x \equiv 35 \pmod{100}$.

8. We are given that $n = 2^m 3^k$ and need to show that $\phi(n) = \dfrac{n}{3}$.

Proof.

Using the formula $\phi(n) = n\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\cdots\left(1-\dfrac{1}{p_r}\right)$ with $p_1 = 2$ and $p_2 = 3$:

$$\phi(n) = \phi\left(2^m 3^k\right) = n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = n\left(\frac{1}{\cancel{2}}\right)\left(\frac{\cancel{2}}{3}\right) = \frac{n}{3}.$$

This completes our proof.

■

This $\phi(n) = \dfrac{n}{3}$ means that one third of the integers between 1 and n have a common factor of only 1 with n. Only one third of residues modulo n have an inverse.

9. (i) The given result $\phi(n) = \dfrac{n}{2}$ means that half the integers between 1 and n have an inverse modulo n.

(ii) We are asked to prove that if $\phi(n) = \dfrac{n}{2}$ then $n = 2^m$. (See question 5 of Exercises 5.1).

Proof.

Let the prime decomposition of $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}$ where p's are distinct primes. By using the formula $\phi(n) = n\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\cdots\left(1-\dfrac{1}{p_r}\right)$ and equating to $n/2$ we have

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) = \frac{n}{2} = n\left(\frac{1}{2}\right).$$

Cancelling out the n's on both sides gives

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) = \frac{1}{2} \qquad (*)$$

Remember we are informed that p's are distinct primes so the only solution to this equation (*) is $p_1 = 2$ and there are *no* other primes. *Why?*

Suppose there were other primes apart from 2 then the product

$$\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)<\frac{1}{2}.$$

Hence, we have our required result because n can only have the prime 2 so $n = 2^m$.

■

10. (i) We need to evaluate $3^4 + 3^2 + 2(3) \equiv ?\pmod 4$:

$$3^4 + 3^2 + 2(3) \equiv 81 + 9 + 6 \equiv 96 \equiv 0 \pmod 4.$$

(ii) Now we need to show this is always the case $a^4 + a^2 + 2a \equiv 0 \pmod 4$.

Proof.

If a is an even number then substituting $a = 2m$ into the given congruence will be a multiple of 4 because $a^4 + a^2 + 2a \equiv 4k \equiv 0 \pmod 4$.

If a is odd then $\gcd(a,\ 4) = 1$ and so we can use Euler's Theorem (5.14):

$$a^{\phi(n)} \equiv 1 \pmod n \text{ provided } \gcd(a,\ n) = 1$$

The Euler totient function of $\phi(4) = 2$ so $a^2 \equiv 1 \pmod 4$. Squaring this gives

$$\left(a^2\right)^2 \equiv a^4 \equiv 1 \pmod 4.$$

As we are assuming a is odd which we can write as $a = 2m+1$. Therefore

$$2a \equiv 2(2m+1) \equiv 4m + 2 \equiv 2 \pmod 4.$$

Substituting $a^2 \equiv 1 \pmod 4$, $a^4 \equiv 1 \pmod 4$ and $2a \equiv 2 \pmod 4$ into the given congruence $a^4 + a^2 + 2a \pmod 4$ yields

$$a^4 + a^2 + 2a \equiv 1 + 1 + 2 \equiv 4 \equiv 0 \pmod 4.$$

This completes our proof.

■

11. (a) We are given $n = 1\,299\,709 \times 15\,485\,863$ and we need to find $\phi(n)$.

We are also told that both of these are prime numbers. Using Proposition (5.2):

If p is prime then $\phi(p) = p - 1$.

And the property that Euler's phi function is multiplicative we have

$$\begin{aligned}\phi(n) &= \phi(1\ 299\ 709 \times 15\ 485\ 863)\\ &= \phi(1\ 299\ 709) \times \phi(15\ 485\ 863)\\ &= 1\ 299\ 708 \times 15\ 485\ 862 = 20\ 127\ 098\ 728\ 296\end{aligned}$$

(b) Similarly we have

$$\begin{aligned}\phi(n) &= \phi(1726\ 943 \times 179\ 424\ 673)\\ &= \phi(1726\ 943) \times \phi(179\ 424\ 673)\\ &= 1726\ 942 \times 179\ 424\ 672 = 309\ 856\ 001\ 913\ 024\end{aligned}$$

12. (i) We need to evaluate $\phi(561)$. Since $561 = 3 \times 11 \times 17$ and each of these factors are prime we have

$$\begin{aligned}\phi(561) &= \phi(3 \times 11 \times 17)\\ &= \phi(3) \times \phi(11) \times \phi(17)\\ &= 2 \times 10 \times 16 = 320\end{aligned}$$

This $\phi(561) = 320$ means there are 320 positive integers between 1 and 561 which have *no* factor in common with 561 apart from the trivial factor of 1.

(ii) We need to show $2^{320} \equiv 1 \pmod{561}$. Evaluating powers of 2 by using the given hint we have:

$$2^{10} \equiv 463 \equiv -98 \pmod{561},\quad 2^{20} \equiv (-98)^2 \equiv 67,\quad 2^{40} \equiv 67^2 \equiv 1 \pmod{561}$$

Since $320 = 8 \times 40$ so $2^{320} \equiv (2^{40})^8 \equiv 1 \pmod{561}$.

(iii) By part (ii) we have $\lambda = 40$.

(iv) In this case $\lambda \mid \phi(561)$.

13. (i) The integer 111 is composite because 3 is factor of 111 as the sum of the digits $1+1+1=3$ and $3 \mid 3$. The other factor can be found by dividing 111 by 3 which gives 37. Both these integers 3 and 37 are prime factors of 111.

Evaluating the Euler phi function of 111:

$$\begin{aligned}\phi(111) &= \phi(3 \times 37)\\ &= \phi(3) \times \phi(37)\\ &= 2 \times 36 = 72\end{aligned}$$

(ii) Let the set $S = \{0, 1, 2, 3, \cdots, 111\}$ be the set of least non-negative residues modulo 111. Let a be in this set. Then it has a multiplicative inverse if we have a solution for $ax \equiv 1 \pmod{111}$. This linear congruence

$$ax \equiv 1 \pmod{111}.$$

has a solution if and only if $\gcd(a, \ \ 111) = 1$. *How many residues in the set S are relatively prime to 111?*

Since $\phi(111) = 72$ so there are 72 residues which will have a multiplicative inverse and there are $111 - 72 = 39$ which will *not* have a multiplicative inverse modulo 111.

14. *How do we prove* $\phi\left(10^{n^2}\right) = 4 \times 10^{n^2-1}$ *?*

Evaluate $\phi\left(10^{n^2}\right)$ by using the formula $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$ and then derive this is actually equal to $4 \times 10^{n^2-1}$.

Proof.

The factors of 10 are 2 and 5 so we have

$$\begin{aligned} \phi\left(10^{n^2}\right) &= \phi\left(\left[2 \times 5\right]^{n^2}\right) \\ &= \phi\left(\left[2^{n^2} \times 5^{n^2}\right]\right) \\ &= \phi\left(2^{n^2}\right) \times \phi\left(5^{n^2}\right) && \left[\begin{array}{l}\text{By the multiplicative property} \\ \text{because the gcd of 2 and 5 is 1}\end{array}\right] \end{aligned}$$

Using the above formula to evaluate each of these terms on the right-hand side:

$$\begin{aligned} \phi\left(10^{n^2}\right) = \phi\left(2^{n^2}\right) \times \phi\left(5^{n^2}\right) &= 2^{n^2}\left(1 - \frac{1}{2}\right) \times 5^{n^2}\left(1 - \frac{1}{5}\right) \\ &= 2^{n^2}\left(\frac{1}{2}\right) \times 5^{n^2}\left(\frac{4}{5}\right) \\ &= 4\left(2^{n^2-1}5^{n^2-1}\right) \\ &= 4\left(10^{n^2-1}\right) = 4 \times 10^{n^2-1} \end{aligned}$$

This completes our proof.

■

15. (a) The given statement - if $a \equiv b \pmod{n}$ then $\phi(a) = \phi(b)$ is false because

$$100 \equiv 5 \pmod{95} \text{ but } \phi(100) = 40 \neq 4 = \phi(5).$$

(b) Statement (b) which claims 'if $a \equiv b \pmod{n}$ then $\phi(a) \equiv \phi(b) \pmod{n}$' is also false because

$$100 \equiv 5 \pmod{95} \text{ but } \phi(100) = 40 \not\equiv 4 = \phi(5) \pmod{95}.$$

(c) This statement 'If $a \equiv b \pmod{n}$ then $\phi(a) \equiv \phi(b) \pmod{\phi(n)}$ may be true.' Let us check with the above numbers:

$$100 \equiv 5 \pmod{95}.$$

We have $\phi(100) = 40, \phi(5) = 4$. We need to evaluate $\phi(95)$.

The prime factorization of 95 is $95 = 5 \times 19$ so

$$\phi(95) = \phi(5) \times \phi(19) = 4 \times 18 = 72.$$

Hence the given statement is false because

$$40 \not\equiv 4 \pmod{72}.$$

16. We need to prove $\phi(2^p - 1) = 2^{p-1} + 2^{p-2} + \cdots + 2^2 + 2$ where $2^p - 1$ is prime.

Proof.

Since we are given that $2^p - 1$ is prime so we use (5.2):

$$\boxed{\phi(q) = q - 1 \text{ where } q \text{ is prime.}}$$

Applying this with $q = 2^p - 1$ we have

$$\begin{aligned}
\phi(2^p - 1) &= 2^p - 1 - 1 \\
&= 2^p - 2 \\
&= 2(2^{p-1} - 1) \\
&= 2(2-1)(2^{p-2} + 2^{p-3} + \cdots + 2 + 1) \qquad \left[\text{By } (x^n - 1) = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)\right] \\
&= 2(2^{p-2} + 2^{p-3} + \cdots + 2 + 1) \\
&= 2^{p-1} + 2^{p-2} + \cdots + 2^2 + 2
\end{aligned}$$

We have proved the required result.

■

17. (a) We need to evaluate $\dfrac{\phi(500)}{500}$. The prime factorization of 500 is

$$500 = 4 \times 125 = 2^2 \times 5^3.$$

By applying the formula $\phi(n) = n\left(1 - \dfrac{1}{p_1}\right)\left(1 - \dfrac{1}{p_2}\right)\cdots\left(1 - \dfrac{1}{p_r}\right)$:

$$\phi(500) = 500\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 200.$$

The probability that a number is relatively prime to 500 is

$$\frac{\phi(500)}{500} = \frac{200}{500} = \frac{2}{5} = 0.4.$$

(b) We are given that $n = 929$ is prime so by (5.2):

$$\boxed{\phi(q) = q - 1 \text{ where } q \text{ is prime}}$$

We have $\phi(929) = 929 - 1 = 928$.

The probability that a number is relatively prime to 929 is

$$\frac{\phi(929)}{929} = \frac{928}{929}.$$

(c) This time $n = 111 \times 929$. The integer 929 is prime but 111 is composite. Clearly 3 is a factor of 111 because the sum of the digits $1+1+1=3$ and $3 \mid 3$. Therefore

$$\frac{111}{3} = 37 \text{ implies that } 111 = 3 \times 37.$$

This implies that $\gcd(111, \quad 929) = 1$. This means that we can use the multiplicative property of the Euler totient function:

$$\begin{aligned}\phi(111 \times 929) &= \phi(111)\phi(929)\\ &= \phi(3 \times 37)\phi(929)\\ &= \phi(3)\phi(37)\phi(929)\\ &= 2 \times 36 \times 928 \qquad \left[\text{Because 3, 37 and 929 are prime}\right]\\ &= 66\ 816\end{aligned}$$

The probability that a chosen number is relatively prime to $111 \times 929 = 103119$ is

$$\frac{\phi(111 \times 929)}{111 \times 929} = \frac{\phi(103\ 119)}{103\ 119} = \frac{66\ 816}{103\ 119} = 0.65 \text{ (2dp)}.$$

65% of the numbers below 103 119 are relatively prime to it.

We need to prove $\dfrac{\phi(p)}{p} = 1 - \dfrac{1}{p}$.

Proof.

Given that p is prime we have $\phi(p) = p - 1$ so

$$\frac{\phi(p)}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}.$$

■

This result signifies that the probability that a chosen number is relatively prime to a prime number is close to 1 for large prime p.

18. We need to find all the residues that are relatively prime to 30 and these are

$\{1, 7, 11, 13, 17, 19, 23, 29\}$. Note that these are all the prime numbers below 30 apart from 2, 3 and 5, only 1 is not a prime.

19. (i) We are asked to prove that $\phi(\phi(p^m)) = [p^{m-1} - p^{m-2}]\phi(p-1)$.

Proof.

By Proposition (5.4):

$$\boxed{\phi(p^k) = p^k - p^{k-1}}$$

Using this we have

$$\begin{aligned}\phi(\phi(p^m)) &= \phi[p^m - p^{m-1}] \\ &= \phi[p^{m-1}(p-1)]\end{aligned}$$

The gcd of p^{m-1} and $p-1$ is 1 because the prime p cannot be a factor of $p-1$. Using the multiplicative property of the ϕ function:

$$\boxed{\phi(mn) = \phi(m)\phi(n) \text{ provided } \gcd(m, \quad n) = 1}$$

in the above derivation gives

$$\begin{aligned}\phi(\phi(p^m)) &= \phi[p^{m-1}(p-1)] \\ &= \phi(p^{m-1})\phi(p-1) \\ &= [p^{m-1} - p^{m-2}]\phi(p-1) \qquad \left[\text{By } \phi(p^k) = p^k - p^{k-1}\right]\end{aligned}$$

■

(ii) Now we need to prove $\phi(\phi(p^m)) = p^{m-2}\phi\left[(p-1)^2\right]$.

Proof.

From the result of part (i) we have

$$\begin{aligned}\phi(\phi(p^m)) &= [p^{m-1} - p^{m-2}]\phi(p-1) \\ &= p^{m-2}(p-1)\phi(p-1) \qquad (\dagger)\end{aligned}$$

We use the result of question 7 of Exercise 5.1:

$$\boxed{n^{m-1}\phi(n) = \phi(n^m)}$$

Applying this result to $(p-1)\phi(p-1)$ with $n = p-1$ and $m = 2$ gives

$$(p-1)\phi(p-1) = \phi\left[(p-1)^2\right].$$

Substituting this into $(\dagger)$ gives

$$\phi(\phi(p^m)) = p^{m-2}(p-1)\phi(p-1) = p^{m-2}\phi\left[(p-1)^2\right].$$

This is our required result.

■

20. We are given that $n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3}$ and need to show

$$\phi(n) = \left[p_1^{k_1-1} \times p_2^{k_2-1} \times p_3^{k_3-1}\right]\phi(p_1)\phi(p_2)\phi(p_3).$$

Proof.

Since $n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3}$ so by using formula (5.9):

$$\boxed{\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)}$$

We have

$$\begin{aligned}\phi(n) &= \phi\left(p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3}\right)\\ &= \left[p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3}\right]\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\\ &= \left[p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3}\right]\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\left(\frac{p_3-1}{p_3}\right)\\ &= \left[p_1^{k_1-1} \times p_2^{k_2-1} \times p_3^{k_3-1}\right](p_1-1)(p_2-1)(p_3-1)\\ &= \left[p_1^{k_1-1} \times p_2^{k_2-1} \times p_3^{k_3-1}\right]\phi(p_1)\phi(p_2)\phi(p_3)\end{aligned}$$

This is our required result.

■

21. (a) We need to show that if n is odd then $\phi(2n) = \phi(n)$.

Proof.

We are given that n is odd therefore $\gcd(2,\ n) = 1$. Applying the multiplicative property of Euler's phi function gives

$$\begin{aligned}\phi(2 \times n) &= \phi(2) \times \phi(n)\\ &= 1 \times \phi(n) = \phi(n)\end{aligned}$$

We have our required result.

■

(b) This time we are asked to prove that if n is even then $\phi(2n) = 2\phi(n)$.

Proof.

Let $n = 2^k a$ where a is odd and k is a natural number. By using the multiplicative property of the Euler's phi function we have

$$\phi(2n) = \phi(2 \times 2^k a) = \phi(2^{k+1} a) = \phi(2^{k+1})\phi(a).$$

By the result of question 5 of Exercise 5.1:

$$\boxed{\phi\left(2^n\right) = \frac{1}{2}\left(2^n\right) = 2^{n-1}}$$

Using this in the above derivation gives

$$\phi\left(2n\right) = \phi\left(2^{k+1}\right)\phi\left(a\right) = 2^k\phi\left(a\right) = 2\left(2^{k-1}\phi\left(a\right)\right)$$

Applying the above boxed result to the last line gives

$$\phi\left(2n\right) = 2\left(2^{k-1}\phi\left(a\right)\right) = 2\left(\phi\left(2^k\right)\phi\left(a\right)\right)$$

Since a is odd so the $\gcd\left(2^k, \quad a\right) = 1$ and using the multiplicative property

$$\phi\left(2n\right) = 2\left(\phi\left(2^k\right)\phi\left(a\right)\right) = 2\phi\left(2^k \times a\right) = 2\phi\left(n\right) \qquad \left[\text{Because } \ 2^k \times a = n\right]$$

This completes our proof.

■

22. We need to show that the following is false:

If $\gcd\left(m_1, \quad m_2, \quad \cdots, \quad m_k\right) = 1$ then

$$\phi\left(m_1 \times m_2 \times \cdots \times m_k\right) = \phi\left(m_1\right) \times \phi\left(m_2\right) \times \cdots \times \phi\left(m_k\right).$$

Let $m_1 = 8, \ m_2 = 9$ and $m_3 = 10$ then using the given gcd of three integers we have

$$\gcd\left(8, \quad 9, \quad 10\right) = \gcd\left(8, \quad \gcd\left(9, \quad 10\right)\right) = \gcd\left(8, \quad 1\right) = 1.$$

Evaluating the Euler phi function of the product $8 \times 9 \times 10$ gives

$$\phi\left(8 \times 9 \times 10\right) = 192.$$

However

$$\begin{aligned}\phi\left(8 \times 9 \times 10\right) &= \phi\left(8\right) \times \phi\left(9\right) \times \phi\left(10\right)\\ &= 4 \times 6 \times 4 = 96\end{aligned}$$

Thus we have produced an example where

$$\phi\left(8 \times 9 \times 10\right) = 192 \neq 96 = \phi\left(8\right) \times \phi\left(9\right) \times \phi\left(10\right).$$

23. (i) We need to find a formula for $\dfrac{\phi\left(n\right)}{n}$.

Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime decomposition of n. By formula (5.9):

$$\boxed{\phi\left(n\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)}$$

Applying this gives

$$\frac{\phi(n)}{n}=\frac{\cancel{n}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)}{\cancel{n}}$$
$$=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$
$$=\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\cdots\left(\frac{p_r-1}{p_r}\right)=\frac{1}{p_1p_2\cdots p_r}(p_1-1)(p_2-1)\cdots(p_r-1)$$

(ii) We need to prove that if $\phi(n)\,\big|\,n$ then $\frac{n}{\phi(n)}=3$.

Proof.

Which integers satisfy $\phi(n)\,\big|\,n$ *?*

Using the result of part (i) with $\frac{n}{\phi(n)}=\alpha$ where α is an integer gives

$$\frac{n}{\phi(n)}=p_1p_2\cdots p_r\frac{1}{(p_1-1)(p_2-1)\cdots(p_r-1)}=\alpha$$
$$p_1p_2\cdots p_r=\alpha(p_1-1)(p_2-1)\cdots(p_r-1)$$

Note that for primes $p\geq 5$ the expression $p-1$ is *not* prime. *Why not?*

Because for $p\geq 5$ we have $p-1$ is even and the only even prime is 2.

This implies that $p_1p_2\cdots p_r\frac{1}{(p_1-1)(p_2-1)\cdots(p_r-1)}$ is an integer *only* if it contains the primes $p_1=2$ and $p_2=3$. Evaluating this integer

$$\frac{n}{\phi(n)}=2\times 3\frac{1}{(2-1)(3-1)}=3.$$

This is our required result.

■

24. We need to prove that $\phi(ma)\phi(mb)=[\phi(m)]^2\,\phi(a)\phi(b)$ where m, a and b are pairwise prime.

Proof.

We are given that m, a and b are pairwise prime. *What does this mean?*

$$\gcd(m,\ a)=\gcd(m,\ b)=\gcd(a,\ b)=1.$$

By the multiplicative property of the Euler phi function we have

$$\begin{aligned}\phi(ma)\phi(mb) &= \phi(m)\phi(a)\phi(m)\phi(b)\\ &= [\phi(m)]^2\,\phi(a)\phi(b)\end{aligned}$$

This completes our proof.

■

25. (a) The divisors of $n = 10$ are $d = 1, 2, 5$ and 10. Thus, the sum

$$\begin{aligned}\sum_{d\,|\,n}\phi(d) &= \phi(1)+\phi(2)+\phi(5)+\phi(10)\\ &= 1+1+4+4 = 10\end{aligned}$$

(b) The factors of 15 are $d = 1, 3, 5$ and 15. Finding the sum $\sum_{d\,|\,n}\phi(d)$ for $n = 15$ gives

$$\begin{aligned}\sum_{d\,|\,n}\phi(d) &= \phi(1)+\phi(3)+\phi(5)+\phi(15)\\ &= 1+2+4+8 = 15\end{aligned}$$

(c) In a similar manner we have the divisors of $n = 24$ are

$$d = 1, 2, 3, 4, 6, 8, 12 \text{ and } 24.$$

We need to find ϕ of each of these. The first three are simple enough and the remaining are given by

$$\phi(4)=2,\ \phi(6)=2,\ \phi(8)=\phi(2^3)=2^3-2^2=4,\ \phi(12)=12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=4.$$

The Euler totient function 24 is $\phi(24)=24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=8$.

Substituting each of these into the evaluation of $\sum_{d\,|\,n}\phi(d)$ gives

$$\begin{aligned}\sum_{d\,|\,n}\phi(d) &= \phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(8)+\phi(12)+\phi(24)\\ &= 1+1+2+2+2+4+4+8 = 24\end{aligned}$$

Note that in each case we have $\sum_{d\,|\,n}\phi(d) = n$.