Complete Solutions to Exercises 5.1

1. Since we are given a prime in each case, so we use Proposition (5.2):

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

   (a) $\phi\left(13\right) = 13 - 1 = 12$.

   (b) $\phi\left(211\right) = 211 - 1 = 210$.

   (c) $\phi\left(311\right) = 311 - 1 = 310$.

   (d) $\phi\left(1973\right) = 1973 - 1 = 1972$.

   (e) $\phi\left(1999\right) = 1999 - 1 = 1998$.

   (f) $\phi\left(2017\right) = 2017 - 1 = 2016$.

2. In each case we use formula (5.9):

   $$\phi\left(n\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \quad \text{where } n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}$$

   This means we need to factorize each of the given numbers into its primes.

   (a) The prime decomposition of $15 = 5 \times 3$. Applying (5.9) gives

   $$\phi\left(15\right) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8.$$

   (There are 8 integers between 1 and 15 that are relatively prime to 15.)

   (b) We need to find the prime decomposition of 64;

   $$64 = 2^6.$$

   Applying (5.9) with $p = 2$ and $k = 6$ gives

   $$\phi\left(2^6\right) = 2^6\left(1 - \frac{1}{2}\right) = 2^6\left(\frac{1}{2}\right) = 2^5 = 32.$$

   Therefore $\phi\left(64\right) = 32$.

   (c) Evaluating the prime decomposition of 200 gives

   $$200 = 8 \times 25 = 2^3 \times 5^2$$

   Using formula (5.9) with $n = 200$, $p_1 = 2$ and $p_2 = 5$:

   $$\phi\left(200\right) = 200\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 200\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 80.$$

   (d) We can write 1000 in its prime decomposition as

   $$1000 = 10^3 = \left(2 \times 5\right)^3 = 2^3 \times 5^3.$$

   Using formula (5.9) gives

$$\phi\left(1000\right) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 1000\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 400\,.$$

(e) *Which prime numbers go into 1001?*

$$1001 = 7\times 11\times 13\,.$$

Using the above formula gives

$$\begin{aligned}\phi\left(1001\right) &= 1001\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)\\ &= 1001\left(\frac{6}{7}\right)\left(\frac{10}{11}\right)\left(\frac{12}{13}\right) = 720\end{aligned}$$

(f) The prime factorization of 666 is

$$666 = 6\times 111 = \left(2\times 3\right)\times\left(3\times 37\right) = 2\times 3^2\times 37\,.$$

So 666 is made up of the primes 2, 3 and 37 therefore

$$\begin{aligned}\phi\left(666\right) &= 666\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{37}\right)\\ &= 666\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{36}{37}\right) = 216\end{aligned}$$

There are 216 integers between 1 and 666 that only have a common factor of 1 with 666.

3. In each case we only have one prime factor. We can still use formula (5.9):

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

(a) We are given 2^{1000}. Applying this formula with $n = 2^{1000}$ and $p_1 = 2$ we obtain

$$\phi\left(2^{1000}\right) = 2^{1000}\left(1-\frac{1}{2}\right) = 2^{1000}\left(\frac{1}{2}\right) = 2^{999}\,.$$

Since the only factor is 2 so $\phi\left(2^{1000}\right) = 2^{999}$ is the number of odd numbers up to 2^{1000} which is ½ of 2^{1000}, hence 2^{999}.

(b) Similarly for 3^{1000} we have

$$\phi\left(3^{1000}\right) = 3^{1000}\left(1-\frac{1}{3}\right) = 3^{1000}\left(\frac{2}{3}\right) = 2\times 3^{999}\,.$$

$\phi\left(3^{1000}\right)$ means the number of natural numbers up to 3^{1000} which are *not* multiples of 3 is 2×3^{999}.

(c) For 5^{1000} we have

$$\phi\left(5^{1000}\right) = 5^{1000}\left(1-\frac{1}{5}\right) = 5^{1000}\left(\frac{4}{5}\right) = 4\times 5^{999}\,.$$

Similarly, $\phi\left(5^{1000}\right) = 4 \times 5^{999}$ is the number of integers between 1 and 5^{1000} which are *not* multiples of 5.

(d) Also for 7^{1000} we have

$$\phi\left(7^{1000}\right) = 7^{1000}\left(1 - \frac{1}{7}\right) = 7^{1000}\left(\frac{6}{7}\right) = 6 \times 7^{999}.$$

Hence there are 6×7^{999} natural numbers up to 7^{1000} which are *not* multiples of 7.

4. We need to prove $\phi\left(p^m\right) = \phi\left(p\right)p^{m-1} = \left(p-1\right)p^{m-1}$ where p is prime.

Proof.

Using formula (5.9) with one prime factor p gives

$$\begin{aligned}\phi\left(p^m\right) &= p^m\left(1 - \frac{1}{p}\right)\\ &= p^m\left(\frac{p-1}{p}\right) = p^{m-1}\left(p-1\right) = p^{m-1}\phi\left(p\right) \quad \left[\text{By (5.2)} \quad \phi\left(p\right) = p-1\right]\end{aligned}$$

This completes our proof.

■

5. *How do we show* $\phi\left(2^n\right) = \frac{1}{2}\left(2^n\right)$ *?*

Use the result of question 4.

Proof.

Using $\phi\left(p^m\right) = \left(p-1\right)p^{m-1}$ with $p = 2$ and $m = n$ gives

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

■

$\phi\left(2^n\right) = 2^{n-1} = \frac{1}{2}\left(2^n\right)$ means that half the natural numbers from 1 to 2^n are relatively prime to 2^n. Of course, these are all the odd numbers from 1 to 2^n.

6. We need to show that $\phi\left(10^m\right) = 4\left(10^{m-1}\right)$.

Proof.

We use formula (5.9):

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

With $n = 10^m$. The prime factors of 10 are 2 and 5, so

$$10^m = 2^m \times 5^m.$$

Substituting $n = 10^m$, $p_1 = 2$ and $p_2 = 5$ into formula (5.9) yields

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

This completes our proof.

■

7. We need to prove that $\phi\left(n^m\right) = n^{m-1}\phi\left(n\right)$.

Proof.

Let the prime decomposition of n be

$$n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3} \times \cdots \times p_r^{k_r} \text{ where } p_j\text{'s are distinct primes.}$$

Expanding the right-hand-side of the given statement:

$$\begin{aligned}n^{m-1}\phi\left(n\right) &= \left(p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}\right)^{m-1} \phi\left(p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}\right) \qquad \begin{bmatrix}\text{Substituting}\\ n = p_1^{k_1} \times \cdots \times p_r^{k_r}\end{bmatrix}\\ &\underbrace{=}_{\text{Using the rules of indices}} p_1^{k_1 m-k_1} \times p_2^{k_2 m-k_2} \times \cdots \times p_r^{k_r m-k_r}\left[\phi\left(p_1^{k_1}\right) \times \phi\left(p_2^{k_2}\right) \times \cdots \times \phi\left(p_r^{k_r}\right)\right]\\ &= p_1^{k_1 m-k_1}\phi\left(p_1^{k_1}\right) \times p_2^{k_2 m-k_2}\phi\left(p_2^{k_2}\right) \times \cdots \times p_r^{k_r m-k_r}\phi\left(p_r^{k_r}\right)\\ &\underbrace{=}_{\text{Using } \phi\left(p^k\right)=p^k-p^{k-1}} p_1^{k_1 m-k_1}\left[p_1^{k_1} - p_1^{k_1-1}\right] \times p_2^{k_2 m-k_2}\left[p_2^{k_2} - p_2^{k_2-1}\right] \times \cdots \times p_r^{k_r m-k_r}\left[p_r^{k_r} - p_r^{k_r-1}\right]\\ &\underbrace{=}_{\text{Using the rules of indices}} \underbrace{\left[p_1^{k_1 m} - p_1^{k_1 m-1}\right]}_{=\phi\left(p_1^{k_1 m}\right)} \times \underbrace{\left[p_2^{k_2 m} - p_2^{k_2 m-1}\right]}_{=\phi\left(p_2^{k_2 m}\right)} \times \cdots \times \underbrace{\left[p_r^{k_r m} - p_r^{k_r m-1}\right]}_{=\phi\left(p_r^{k_r m}\right)}\\ &= \phi\left(p_1^{k_1 m}\right) \times \phi\left(p_2^{k_2 m}\right) \times \cdots \times \phi\left(p_r^{k_r m}\right)\\ &= \phi\left(p_1^{k_1 m} \times p_2^{k_2 m} \times \cdots \times p_r^{k_r m}\right) = \phi\left[\left(p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}\right)^m\right] = \phi\left(n^m\right)\end{aligned}$$

This completes our proof because we have $n^{m-1}\phi\left(n\right) = \phi\left(n^m\right)$.

■

8. There is only one example of $\phi\left(n\right) = n$ which is $n = 1$.

9. In the main text we have $\dfrac{\phi\left(n\right)}{n}$ gives the probability that a number we choose between 1 and n is relatively prime to n. Let $n = 164$ then

$$\phi\left(164\right) = \phi\left(2 \times 82\right) = \phi\left(4 \times 41\right) = \phi\left(4\right) \times \phi\left(41\right) = 2 \times 40 = 80.$$

Therefore, the probability that $m \in \{1, 2, 3, \cdots, 164\}$ is relatively prime to 164 is

$$\frac{\phi(164)}{164} = \frac{80}{164} = \frac{20}{41}.$$

10. (a) Recall $\phi(310)$ gives the number of incongruent residues which have an inverse modulo 310. Converting 310 into its prime factorization $310 = 31 \times 10 = 2 \times 5 \times 31$ and applying (5.9) yields

$$\phi(310) = 310\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{31}\right) = 120.$$

(b) *Proof.* We have $\phi(p^n) = p^n - p^{n-1}$. By part (a) this number $\phi(p^k) = p^k - p^{k-1}$ tells us how many integers have an inverse modulo p^n. Therefore the probability of a given residue $a \pmod{p^n}$ having an inverse is

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

This completes our proof.

■

11. (a) We need to find n such that $\phi(n) = \frac{n}{2}$.

Recall that $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$ where the p's are the primes in the prime decomposition of n. This implies we need to find n such that

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

So n can only have one prime $p = 2$ so $n = 2^a$ where a is a natural number and

$$n\left(1 - \frac{1}{2}\right) = \frac{n}{2}.$$

(b) We need to find n such that $\phi(n) = \frac{n}{3}$. Similarly to part (a) we have

$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) = \frac{n}{3}.$$

The only prime *cannot* be 3 because

$$n\left(1 - \frac{1}{3}\right) = \frac{2n}{3}.$$

Since we want to cancel the 2 on the numerator so the prime 2 must be present:

$$n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=n\left(\frac{1}{\cancel{2}}\right)\left(\frac{\cancel{2}}{3}\right)=\frac{n}{3}$$

Hence $n=2^a3^b$ where a and b are natural numbers.

12. We need to find a natural number n such that $\phi(n)<\frac{n}{3}$. This means we are looking for a number where less than a third of the natural numbers up to n have *no* factor in common with n apart from 1. This implies that we need a number which has lots of factors because 2/3 of the natural numbers up to n must have a common factor greater than 1.

By the solution to question 11(b) we can say that if n has the prime factors 2 and 3 present then $\phi(n)=\frac{n}{3}$. If we add another prime factor, 5 say, then we have the integer 30 because $2\times3\times5=30$ then

$$\phi(30)=\phi(2)\times\phi(3)\times\phi(5)=1\times2\times4=8<\frac{30}{3}=10.$$

Therefore, one example of $\phi(n)<\frac{n}{3}$ is $n=30$.

13. We need to prove that $\phi(n)=\frac{4}{15}n$ given $n=2^{k_1}\times3^{k_2}\times5^{k_3}$.

Proof.

Using formula (5.9):

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

With $n=2^{k_1}\times3^{k_2}\times5^{k_3}$ gives

$$\begin{aligned}\phi(n)&=n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\&=n\left(\frac{1}{\cancel{2}}\right)\left(\frac{\cancel{2}}{3}\right)\left(\frac{4}{5}\right)=\frac{4}{15}n\end{aligned}$$

Therefore $\phi(n)=\frac{4}{15}n$.

■

14. We are asked to prove that $\phi(n)<\frac{n(p-1)}{p}$ where $p\mid n$.

Proof.

We are given that the prime p satisfies $p \mid n$ therefore $\gcd\left(p, \quad n\right) = p > 1$. Let S be the set of *some* residues modulo n that are *not* relatively prime to n:

$$S = \left\{p,\ 2p, 3p, \cdots, \frac{n}{p}p\right\}.$$

Then $Card\left(S\right) = \frac{n}{p}$. These $\frac{n}{p}$ residues are *not* relatively prime to n. There may be others as n may have other prime factors present. By the definition of the Euler totient function $\phi\left(n\right)$ we have

$$\phi\left(n\right) \le \left(n-1\right) - \frac{n}{p} < n - \frac{n}{p} = \frac{np-n}{p} = \frac{n\left(p-1\right)}{p}$$

This completes our proof.

■

15. (i) The only instance where $\phi\left(n\right) = n$ is if $n = 1$ (see question 8). But for $n > 1$ we have $\phi\left(n\right) < n$.

This $\phi\left(n\right) \ge n$ is impossible because $\phi\left(n\right)$ counts the natural numbers up to n which are relatively prime to n. This number *cannot* exceed n.

(ii) *Proof.*

To show that $0 < \frac{\phi\left(n\right)}{n} < 1$ we use the result of part (i). By the definition of $\phi\left(n\right)$ and part (i) we have $1 \le \phi\left(n\right) < n$. Substituting this into $\frac{\phi\left(n\right)}{n}$ gives

$$0 < \frac{1}{n} \le \frac{\phi\left(n\right)}{n} < \frac{n}{n} = 1.$$

■

16. We need to produce a counter example. Well

$$\phi\left(3+7\right) = \phi\left(10\right) = 4 \text{ but } \phi\left(3\right) + \phi\left(7\right) = 2 + 6 = 8.$$

17. We are required to prove that $\phi\left(\phi\left(p^k\right)\right) = p^{k-2}\phi\left[p\left(p-1\right)\right]$.

Proof.

In question 4 we have already shown that $\phi\left(p^m\right) = \left(p-1\right)p^{m-1}$. Applying this to $\phi\left(p^k\right)$ gives

$$\phi\left(p^k\right) = p^{k-1}\left(p-1\right).$$

We want to use the multiplicative property of ϕ. However to use this we need our natural numbers to be relatively prime, that is

$$\gcd\left(p^{k-1},\quad p-1\right)=1.$$

Suppose $\gcd\left(p^{k-1},\quad p-1\right)=g>1$. Then $g\mid p^{k-1}$ and $g\mid\left(p-1\right)$.

Now one of the factors of p^{k-1} is p. Clearly $p\le g$ because the only divisors greater than 1 of p^{k-1} are p, p^2, p^3, $\cdots$, p^{k-1}. This implies that $p\mid g$ because $g\mid p^{k-1}$. Since $g\mid\left(p-1\right)$ so $p\mid\left(p-1\right)$ which is impossible. Therefore our supposition $\gcd\left(p^{k-1},\quad p-1\right)=g>1$ must be wrong, so $\gcd\left(p^{k-1},\quad p-1\right)=1$.

Hence using the multiplicative property of ϕ we have

$$\begin{aligned}\phi\left[\phi\left(p^k\right)\right]&=\phi\left[p^{k-1}\left(p-1\right)\right]\\&=\phi\left(p^{k-1}\right)\phi\left(p-1\right)\\&=p^{k-2}\left(p-1\right)\phi\left(p-1\right)&&\left[\text{By using the result of question 4}\right]\\&=p^{k-2}\phi\left(p\right)\phi\left(p-1\right)&&\left[\text{Because }\ \phi\left(p\right)=p-1\right]\\&=p^{k-2}\phi\left(p\left(p-1\right)\right)&&\left[\text{By the multiplicative property of }\ \phi\right]\end{aligned}$$

We have shown $\phi\left(\phi\left(p^k\right)\right)=p^{k-2}\phi\left[p\left(p-1\right)\right]$.

■

18. We need to prove that $\phi\left(d\right)\mid\phi\left(n\right)$ provided $d\mid n$.

Proof.

Using the hint and writing d and n in its prime decomposition:

$d=p_1^{m_1}\times p_2^{m_2}\times\cdots\times p_r^{m_r}$ and $n=p_1^{m_1+k_1}\times p_2^{m_2+k_2}\times\cdots\times p_r^{m_r+k_r}\times p_{r+1}^{m_{r+1}}\times\cdots\times p_k^{m_k}$

where the p's are distinct primes. From $d=p_1^{m_1}\times p_2^{m_2}\times\cdots\times p_r^{m_r}$ we have $p_1^{m_1}\mid d$ where m_1 is the highest power of the prime p_1 which divides into d. However, there may be higher powers of p_1 which divide into n. We have written the highest power of p_1 which divides into n as m_1+k_1. Similarly, for p_2, p_3, …, p_r. That is why we have

$$n=p_1^{m_1+k_1}\times p_2^{m_2+k_2}\times\cdots\times p_r^{m_r+k_r}\times p_{r+1}^{m_{r+1}}\times\cdots\times p_k^{m_k}$$

Finding the Euler totient function for each of these numbers gives

$$\begin{aligned}\phi\left(d\right)&=\phi\left(p_1^{m_1}\times p_2^{m_2}\times\cdots\times p_r^{m_r}\right)\\&=\phi\left(p_1^{m_1}\right)\times\phi\left(p_2^{m_2}\right)\times\cdots\times\phi\left(p_r^{m_r}\right)&&\left[\text{By Lemma (5.7)}\right]\end{aligned}$$

Similarly we have

$$\phi\left(n\right)=\phi\left(p_1^{\,m_1+k_1}\right)\times\phi\left(p_2^{\,m_2+k_2}\right)\times\cdots\times\phi\left(p_r^{\,m_r+k_r}\right)\times\phi\left(p_{r+1}^{\,m_{r+1}}\right)\times\cdots\times\phi\left(p_k^{\,m_k}\right)\quad(*)$$

By result of question 4:

$$\phi\left(p^m\right)=\left(p-1\right)p^{m-1}$$

We have

$$\phi\left(p_1^{\,m_1}\right)=\left(p_1-1\right)p_1^{\,m_1-1}$$

$$\phi\left(p_1^{\,m_1+k_1}\right)=\left(p_1-1\right)p_1^{\,m_1+k_1-1}$$

Therefore $\phi\left(p_1^{\,m_1}\right)\Big|\,\phi\left(p_1^{\,m_1+k_1}\right)$. Similarly, $\phi\left(p_2^{\,m_2}\right)\Big|\,\phi\left(p_2^{\,m_2+k_2}\right),\ \cdots,\phi\left(p_r^{\,m_r}\right)\Big|\,\phi\left(p_r^{\,m_r+k_r}\right)$

.

From this last evaluation and using (*) we have

$$\underbrace{\phi\left(p_1^{\,m_1}\right)\phi\left(p_2^{\,m_2}\right)\cdots\phi\left(p_r^{\,m_r}\right)}_{=\phi(d)}\ \Big|\ \phi\left(n\right)$$

Therefore $\phi\left(d\right)\Big|\,\phi\left(n\right)$.

■

19. We need to show that $\phi\left(2^{2k+1}\right)=l^2$.

Proof.

Using the result of question 4:

$$\phi\left(p^m\right)=\left(p-1\right)p^{m-1},$$

with $p=2$ and $m=2k+1$ gives

$$\begin{aligned}\phi\left(2^{2k+1}\right)&=\left(2-1\right)2^{2k+1-1}\\&=2^{2k}=\left(2^k\right)^2=l^2\quad\text{where}\quad l=2^k.\end{aligned}$$

This is our required result.

■

20. *How do we prove* $\phi\left(p^kq^k\right)=p^{k-1}q^{k-1}\phi\left(q\right)\phi\left(p\right)$ *?*

By using the multiplicative property of the ϕ function and Proposition (5.4):

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

Proof.

Since we are given that p and q are distinct primes so by Lemma (5.7):

$$\phi\left(p_1^{\,k_1}\times p_2^{\,k_2}\times\cdots\times p_r^{\,k_r}\right)=\phi\left(p_1^{\,k_1}\right)\times\phi\left(p_2^{\,k_2}\right)\times\cdots\times\phi\left(p_r^{\,k_r}\right)$$

We can use this multiplicative property because p and q are distinct primes so $\gcd\left(p^k,\ \ q^k\right)=1$:

$$\phi\left(p^k \times q^k\right) = \phi\left(p^k\right) \times \phi\left(q^k\right)$$

Applying Proposition (5.4) to each of these gives:

$$\begin{aligned}
\phi\left(p^k q^k\right) &= \phi\left(p^k\right)\phi\left(q^k\right) \\
&= \left(p^k - p^{k-1}\right)\left(q^k - q^{k-1}\right) \\
&= p^k q^k - p^k q^{k-1} - p^{k-1} q^k + p^{k-1} q^{k-1} && \left[\text{Expanding brackets}\right] \\
&= p^{k-1} q^{k-1}\left[pq - p - q + 1\right] && \left[\text{Factorizing}\right] \\
&= p^{k-1} q^{k-1}\left[q\left(p-1\right) - \left(p-1\right)\right] \\
&= p^{k-1} q^{k-1}\left[q-1\right]\left(p-1\right) && \left[\text{Factorizing}\right] \\
&= p^{k-1} q^{k-1}\phi\left(q\right)\phi\left(p\right) && \left[\text{Because } \phi\left(p\right) = p-1\right]
\end{aligned}$$

Hence we have $\phi\left(p^k \times q^k\right) = p^{k-1} q^{k-1}\phi\left(p\right)\phi\left(q\right)$ which is our required result.

■

21. We need to prove Corollary (5.6) which claims:

> $\phi\left(m_1 \times m_2 \times \cdots \times m_k\right) = \phi\left(m_1\right) \times \phi\left(m_2\right) \times \cdots \times \phi\left(m_k\right)$ provided the integers m_j are pairwise prime. That is $\gcd\left(m_i,\ \ m_j\right) = 1$ for $i \neq j$ and $1 \leq i,\ \ j \leq k$.

How do we prove this result?

Use mathematical induction and the three steps of induction are:

Step 1: Check for some base case $m_1,\ \ m_2$.

Step 2: Assume the result is true for $m_1,\ \ m_2,\ \ m_3,\ \ \cdots,\ \ m_j$.

Step 3: Prove this for $m_1,\ \ m_2,\ \ m_3,\ \ \cdots,\ \ m_j,\ \ m_{j+1}$.

Proof.

Step 1: Since we are given that $\gcd\left(m_i,\ \ m_j\right) = 1$ so $\gcd\left(m_1,\ \ m_2\right) = 1$.

By Proposition (5.5):

> $$\phi\left(m \times n\right) = \phi\left(m\right) \times \phi\left(n\right) \quad \text{provided } \gcd\left(m,\ \ n\right) = 1$$

We have

$$\phi\left(m_1 \times m_2\right) = \phi\left(m_1\right) \times \phi\left(m_2\right)$$

Step 2:

Assume that

$$\phi\left(m_1 \times m_2 \times \cdots \times m_j\right) = \phi\left(m_1\right) \times \phi\left(m_2\right) \times \cdots \times \phi\left(m_j\right) \qquad (*)$$

Provided $\gcd\left(m_i,\ \ m_j\right) = 1$ where $i \neq j$.

Step 3:

We are required to prove that

$$\phi\left(m_1 \times m_2 \times \cdots \times m_j \times m_{j+1}\right) = \phi\left(m_1\right) \times \phi\left(m_2\right) \times \cdots \times \phi\left(m_j\right) \times \phi\left(m_{j+1}\right)$$

Consider the left-hand-side of this:

$$\phi\left(m_1 \times m_2 \times \cdots \times m_j \times m_{j+1}\right) = \phi\left(\left[m_1 \times m_2 \times \cdots \times m_j\right] \times m_{j+1}\right) \qquad (\ddagger)$$

In order to split the right-hand-side we need to ensure that

$$\gcd\left(\left[m_1 \times m_2 \times \cdots \times m_j\right], \quad m_{j+1}\right) = 1$$

We are given that

$$\gcd\left(m_1, \quad m_{j+1}\right) = \gcd\left(m_2, \quad m_{j+1}\right) = \gcd\left(m_3, \quad m_{j+1}\right) = \cdots = \gcd\left(m_j, \quad m_{j+1}\right) = 1$$

By the result of question 15(ii) of Exercises 1.3:

$$\gcd\left(a, \quad n_1\right) = \gcd\left(a, \quad n_2\right) = \cdots = \gcd\left(a, \quad n_k\right) = 1 \;\Rightarrow\; \gcd\left(a, \quad n_1 \times n_2 \times \cdots \times n_k\right) = 1$$

We have $\gcd\left(\left[m_1 \times m_2 \times \cdots \times m_j\right], \quad m_{j+1}\right) = 1$.

Now we are in a position to apply Proposition (5.5) to (‡):

$$\begin{aligned}
\phi\left(m_1 \times m_2 \times \cdots \times m_j \times m_{j+1}\right) &= \phi\left(\left[m_1 \times m_2 \times \cdots \times m_j\right] \times m_{j+1}\right) \\
&= \phi\left(\left[m_1 \times m_2 \times \cdots \times m_j\right]\right) \times \phi\left(m_{j+1}\right) \\
&= \underbrace{\phi\left(m_1\right) \times \phi\left(m_2\right) \times \cdots \times \phi\left(m_j\right)}_{\text{By (*)}} \times \phi\left(m_{j+1}\right)
\end{aligned}$$

By mathematical induction we have our result;

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

■

22. We need to prove the following:

If $n = p_1^{k_1} \times p_2^{k_2} \times p_3^{k_3} \times \cdots \times p_r^{k_r}$ then

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

Proof.

By Proposition (5.8) we have

$$\phi\left(n\right) = \left(p_1^{k_1} - p_1^{k_1 - 1}\right)\left(p_2^{k_2} - p_2^{k_2 - 1}\right)\left(p_3^{k_3} - p_3^{k_3 - 1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r - 1}\right)$$

Taking out factors gives

$$\begin{aligned}\phi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\left(p_3^{k_3} - p_3^{k_3-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= p_1^{k_1}\left(1 - p_1^{-1}\right)p_2^{k_2}\left(1 - p_2^{-1}\right)p_3^{k_3}\left(1 - p_3^{-1}\right)\cdots p_r^{k_r}\left(1 - p_r^{-1}\right)\\ &= \underbrace{p_1^{k_1}p_2^{k_2}p_3^{k_3}\cdots p_r^{k_r}}_{=n}\left[\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right)\right] \qquad \left[\text{Because } p_m^{-1} = \frac{1}{p_m}\right]\\ &= n\left[\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right)\right]\end{aligned}$$

This completes our proof.

■

23. We are required to prove that if $\gcd(m,\ n) = 2$ then

$$\phi(m \times n) = 2 \times \phi(m) \times \phi(n).$$

Proof.

We are given that $\gcd(m,\ n) = 2$ so there are integers x and y such that

$$2x = m \text{ and } 2y = n.$$

Then $\gcd(x,\ y) = 1$. *Why?*

Because $x = \frac{m}{2}$ and $y = \frac{n}{2}$ so by Proposition (1.5) of chapter 1:

$$\gcd(a,\ b) = g \text{ implies } \gcd\left(\frac{a}{g},\ \frac{b}{g}\right) = 1$$

We have $\gcd(x,\ y) = \gcd\left(\frac{m}{2},\ \frac{n}{2}\right) = 1$.

Since $\gcd(x,\ y) = 1$ we can apply the multiplicative property of the Euler totient function ϕ. Therefore, we have

$$\phi(m \times n) = \phi(2x \times 2y) = \phi(2^2 xy).$$

Let the primes of x which are distinct from 2 be $p_1,\ p_2,\ \cdots,\ p_r$ and the primes of y distinct from 2 be $q_1,\ q_2,\ \cdots,\ q_t$.

By formula (5.9):

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

Applying this formula to $\phi(mn) = \phi(2^2 xy)$ gives

$$\begin{aligned}\phi(2^2 xy) &= 2^2 xy\left(1-\frac{1}{2}\right)\times\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\times\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_t}\right)\\ &= 2xy\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\times\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_t}\right) \qquad (\dagger)\end{aligned}$$

Applying formula (5.9) to $2\phi(m)\phi(n)$ gives

$$\begin{aligned}
2\phi(m)\phi(n) &= 2\times\phi(2x)\times\phi(2y)\\
&= 2\times 2x\left(1-\frac{1}{2}\right)\times\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\times 2y\left(1-\frac{1}{2}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_t}\right)\\
&= 2\times x\times y\times\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\times\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_t}\right)\\
&= 2xy\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\times\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_t}\right)\\
&= \phi\left(2^2xy\right) \qquad \left[\text{By } (\dagger)\right]
\end{aligned}$$

Hence we have $\phi(mn)=\phi\left(2^2xy\right)=2\phi(m)\phi(n)$ which is our required result.

■

24. We need to prove $\phi(m)=2^{n-1}\left(2^{n-1}-1\right)$ given that $m=2^{n-1}\left(2^n-1\right)$ where 2^n-1 is prime (Mersenne prime).

Proof.

Since we are given that 2^n-1 is prime and as $n\geq 2$ so this number is an *odd* prime. The only prime factor of 2^{n-1} is 2. Therefore

$$\gcd\left(2^{n-1},\quad 2^n-1\right)=1\,.$$

We apply the multiplicative property of ϕ on m:

$$\begin{aligned}
\phi(m) &= \phi\left(2^{n-1}\left(2^n-1\right)\right)\\
&= \underbrace{\phi\left(2^{n-1}\right)}_{\substack{=(2-1)2^{n-2}\\ \text{by question 4}}}\times\underbrace{\phi\left(2^n-1\right)}_{\substack{=2^n-1-1\\ \text{because } 2^n-1 \text{ is prime}}}\\
&= 2^{n-2}\times\left(2^n-2\right)\\
&= 2^{n-1}2^{-1}\times\left(2^n-2\right)\\
&= 2^{n-1}\left(2^{n-1}-1\right)
\end{aligned}$$

We have our required result.

■

25. (i) We are asked to prove $\phi(m\times n)=\dfrac{\phi(m)\times\phi(n)\times g}{\phi(g)}$.

Proof.

Let $\gcd(m,\quad n)=g$.

<u>Case I</u> If $m=n$ then $m\times n=n^2$ then by the result of question 7:

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

We have $\phi\left(n^2\right) = n^{2-1}\phi\left(n\right) = n\phi\left(n\right)$. Also $g = \gcd\left(n, \quad n\right) = n$ so evaluating the right-hand-side of the given result:

$$\frac{\phi\left(m\right)\times\phi\left(n\right)\times g}{\phi\left(g\right)} = \frac{\phi\left(n\right)\times \cancel{\phi\left(n\right)}\times n}{\cancel{\phi\left(n\right)}} = n\phi\left(n\right)$$

Hence, we have our result if $m = n$.

Case II

If $m \neq n$ then m and n *will* have some *different* primes in their decomposition.

Let $m = \left(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\right)\times\left(q_1^{a_1}q_2^{a_2}\cdots q_l^{a_l}\right)$ and $n = \left(p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}\right)\times\left(s_1^{b_1}s_2^{b_2}\cdots s_j^{b_j}\right)$ be the prime decompositions of m and n and $e_j > 0$ and $f_j > 0$.

By Proposition (2.21) of Chapter 2 the gcd is given by:

$$\gcd\left(m, \quad n\right) = p_1^{\min\left(e_1,\, f_1\right)}\times p_2^{\min\left(e_2,\, f_2\right)}\times\cdots\times p_k^{\min\left(e_k,\, f_k\right)}$$

Therefore, we have

$$g = p_1^{\min\left(e_1,\, f_1\right)}\times p_2^{\min\left(e_2,\, f_2\right)}\times\cdots\times p_r^{\min\left(e_r,\, f_r\right)}.$$

By formula (5.9):

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

We have $\phi\left(g\right) = g\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$ which implies

$$\frac{\phi\left(g\right)}{g} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) \qquad (\dagger)$$

Similarly, by this formula (5.9):

$$\phi\left(m\right) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_l}\right)$$

$$\phi\left(n\right) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{s_1}\right)\left(1-\frac{1}{s_2}\right)\cdots\left(1-\frac{1}{s_j}\right)$$

$$\phi\left(mn\right) = mn\left[\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)\right]\times\left[\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_l}\right)\right]\times\left[\left(1-\frac{1}{s_1}\right)\cdots\left(1-\frac{1}{s_j}\right)\right] \quad (*)$$

Evaluating $\dfrac{\phi\left(m\right)\times\phi\left(n\right)}{\phi\left(g\right)/\,g}$ gives

$$\frac{\phi(m)\times\phi(n)}{\phi(g)/g} = \frac{m\cancel{\left(1-\frac{1}{p_1}\right)}\cdots\cancel{\left(1-\frac{1}{p_r}\right)}\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_l}\right)\times n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{s_1}\right)\cdots\left(1-\frac{1}{s_j}\right)}{\underbrace{\cancel{\left(1-\frac{1}{p_1}\right)}\cancel{\left(1-\frac{1}{p_2}\right)}\cdots\cancel{\left(1-\frac{1}{p_r}\right)}}_{\text{by }(\dagger)}}$$

$$= mn\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_l}\right)\left(1-\frac{1}{s_1}\right)\cdots\left(1-\frac{1}{s_j}\right)$$

The last line is identical to (*). Therefore, we have

$$\phi(mn) = \frac{\phi(m)\times\phi(n)}{\phi(g)/g} = \frac{\phi(m)\times\phi(n)\times g}{\phi(g)}.$$

This completes our proof,

■

(ii) We need to prove that Euler's totient function is multiplicative.

Proof.

Substituting $g=1$ into part (i) gives us our required result:

$$\phi(m\times n) = \phi(m)\times\phi(n) \text{ provided } \gcd(m,\ n) = 1.$$

■

[Here is another proof of this result:

Consider the array of positive integers:

$$\underbrace{\left.\begin{array}{cccc} 1 & 2 & \cdots & n \\ n+1 & n+2 & n+\cdots & n+n \\ \vdots & \vdots & \vdots & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+\cdots & mn \end{array}\right\}}_{n \text{ columns}} m \text{ rows}$$

There are $\phi(n)$ columns which are relatively prime to n. In each of these columns there are only $\phi(m)$ elements which are relatively prime to m. The number of elements in the array which are relatively prime to $m\times n$ is $\phi(m\times n)$. Each of these numbers are relatively prime to m or n. From above we have there are $\phi(m)\times\phi(n)$ of these numbers. Therefore $\phi(m\times n) = \phi(m)\times\phi(n)$.]

■

26. We need to prove $\phi(lcm(a,\ b))\times\phi(\gcd(a,\ b)) = \phi(a)\times\phi(b)$ because we are given that $[a,\ b] = lcm(a,\ b)$.

Proof.

Let $g' = \gcd(lcm(a,\ b),\ \gcd(a,\ b))$. Then by the definition of gcd we have

$$g' = \gcd\Big(lcm\big(a,\quad b\big),\quad \gcd\big(a,\quad b\big)\Big) = \gcd\big(a,\quad b\big) = g \text{ say.}$$

By Proposition (2.22):

$$\gcd\big(a,\quad b\big)\times\big[a,\quad b\big] = a\times b$$

We have $lcm\big(a,\quad b\big)\times\gcd\big(a,\quad b\big) = a\times b$. Therefore

$$\phi\Big(lcm\big(a,\quad b\big)\times\gcd\big(a,\quad b\big)\Big) = \phi\big(a\times b\big) \qquad (*)$$

Re-arranging the result of the last question part (i):

$$\phi\big(m\times n\big) = \frac{\phi\big(m\big)\times\phi\big(n\big)\times g}{\phi\big(g\big)}$$

We have

$$\phi\big(m\big)\times\phi\big(n\big) = \frac{\phi\big(m\times n\big)\phi\big(g\big)}{g}$$

Applying this with $m = lcm\big(a,\quad b\big)$ and $n = \gcd\big(a,\quad b\big)$ gives

$$\begin{aligned}\phi\Big(lcm\big(a,\quad b\big)\Big)\times\phi\Big(\gcd\big(a,\quad b\big)\Big) &= \frac{\phi\Big(lcm\big(a,\quad b\big)\times\gcd\big(a,\quad b\big)\Big)\phi\big(g\big)}{g}\\ &= \frac{\phi\big(a\times b\big)\phi\big(g\big)}{g} \qquad \big[\text{By } (*)\big]\\ &= \phi\big(a\big)\times\phi\big(b\big)\end{aligned}$$

This completes our proof.

■

27. (i) We are asked to prove $\displaystyle\sum_{d\,\big|\,p^k}\phi\big(d\big) = p^k$.

Proof.

The divisors of p^k are $1, p, p^2, \cdots, p^{k-1}, p^k$. We have

$$\begin{aligned}\sum_{d\,\big|\,p^k}\phi\big(d\big) &= \phi\big(1\big)+\phi\big(p\big)+\phi\big(p^2\big)+\cdots+\phi\big(p^{k-1}\big)+\phi\big(p^k\big)\\ &= 1+\big(p-1\big)+\big(p^2-p\big)+\cdots+\big(p^{k-1}-p^{k-2}\big)+\big(p^k-p^{k-1}\big)\\ &= 1+\big(p-1\big)+p\big(p-1\big)+\cdots+p^{k-2}\big(p-1\big)+p^{k-1}\big(p-1\big) \qquad \big[\text{Factorizing}\big]\\ &= 1+\big(p-1\big)\underbrace{\big[1+p+\cdots+p^{k-2}+p^{k-1}\big]}_{=\frac{1-p^k}{1-p}\text{ by sum of geometric series}}\\ &= 1+\big(p-1\big)\frac{1-p^k}{1-p} = 1+\cancel{\big(p-1\big)}\left[\frac{p^k-1}{\cancel{p-1}}\right] \qquad \left[\begin{array}{l}\text{Multiplying numerator and}\\ \text{denominator by } -1\end{array}\right]\\ &= 1+p^k-1 = p^k\end{aligned}$$

This completes our proof.

■

(ii) Similarly, we prove $\sum_{d \mid p^k q^m} \phi(d) = \sum_{d \mid p^k} \phi(d) \sum_{d' \mid q^m} \phi(d') = p^k q^m$.

Proof.

It is longer proof than part (i) but the procedure is very similar. Since the given primes p and q are distinct so $\gcd(p, \quad q) = 1$. We have

$$\begin{aligned}
\sum_{d \mid p^k q^m} \phi(d) &\underset{\substack{\text{Divisor 1 is included in the first term on the right hand side.}}}{=} \phi(1) + \underbrace{\left[\sum_{d \mid p^k} \phi(d) - 1\right]}_{\text{by part (i)}} + \underbrace{\left[\sum_{d \mid q^m} \phi(d) - 1\right]}_{\text{by part (i)}} + \\
&\quad + \phi(pq) + \phi(p^2 q) + \cdots + \phi(p^k q) \\
&\quad + \phi(pq^2) + \phi(p^2 q^2) + \cdots + \phi(p^k q^2) \\
&\quad \vdots \qquad \vdots \qquad \vdots \\
&\quad + \phi(pq^m) + \phi(p^2 q^m) + \cdots + \phi(p^k q^m) \\
&\underset{\substack{\text{By multiplicative property of } \phi}}{=} \phi(1) + \left[p^k - 1\right] + \left[q^m - 1\right] + \phi(p)\phi(q) + \phi(p^2)\phi(q) + \cdots + \phi(p^k)\phi(q) \\
&\quad + \phi(p)\phi(q^2) + \phi(p^2)\phi(q^2) + \cdots + \phi(p^k)\phi(q^2) \\
&\quad \vdots \qquad \vdots \qquad \vdots \\
&\quad + \phi(p)\phi(q^m) + \phi(p^2)\phi(q^m) + \cdots + \phi(p^k)\phi(q^m) \\
&\underset{\substack{\text{By } \phi(q^\ell) = q^\ell - q^{\ell-1}}}{=} \phi(1) + \left[p^k - 1\right] + \left[q^m - 1\right] + \phi(p)(q-1) + \phi(p^2)(q-1) + \cdots + \phi(p^k)(q-1) \\
&\quad + \phi(p)(q^2 - q) + \phi(p^2)(q^2 - q) + \cdots + \phi(p^k)(q^2 - q) \\
&\quad \vdots \qquad \vdots \qquad \vdots \\
&\quad + \phi(p)(q^m - q^{m-1}) + \phi(p^2)(q^m - q^{m-1}) + \cdots + \phi(p^k)(q^m - q^{m-1}) \\
&\underset{\substack{\text{Factorizing}}}{=} \phi(1) + \left[p^k - 1\right] + \left[q^m - 1\right] + (q-1)\left[\phi(p) + \phi(p^2) + \cdots + \phi(p^k)\right] \\
&\quad + (q^2 - q)\left[\phi(p) + \phi(p^2) + \cdots + \phi(p^k)\right] \\
&\quad \vdots \qquad \vdots \\
&\quad + (q^m - q^{m-1})\left[\phi(p) + \phi(p^2) + \cdots + \phi(p^k)\right] \qquad (*)
\end{aligned}$$

From part (i) we have

$$\phi(p) + \phi(p^2) + \cdots + \phi(p^k) = p^k - 1$$

Substituting this into (*) yields

$$\begin{aligned}
\sum_{d\,|\,p^k q^m}\phi(d) &= \phi(1)+\left[p^k-1\right]+\left[q^m-1\right]+(q-1)\left[p^k-1\right] \\
&\quad +\left(q^2-q\right)\left[p^k-1\right]+\cdots+\left(q^m-q^{m-1}\right)\left[p^k-1\right] \\
&= 1+\left[p^k-1\right]+\left[q^m-1\right]+\left[p^k-1\right]\left[(q-1)+\left(q^2-q\right)+\cdots+\left(q^m-q^{m-1}\right)\right] \\
&= 1+\left[p^k-1\right]+\left[q^m-1\right]+\left[p^k-1\right]\underbrace{(q-1)}_{\text{Factorizing out }(q-1)}\left[1+q+q^2+\cdots+q^{m-1}\right] \\
&= 1+\left[p^k-1\right]+\left[q^m-1\right]+\left[p^k-1\right](q-1)\left[\frac{1-q^m}{1-q}\right] \quad \left[\begin{array}{l}\text{Using the sum of}\\ \text{geometric series on the}\\ \text{last brackets.}\end{array}\right] \\
&= 1+\left[p^k-1\right]+\left[q^m-1\right]+\left[p^k-1\right]\left(q^m-1\right) \quad \left[\begin{array}{l}\text{Multiplying the numerator}\\ \text{and denominator by } -1.\end{array}\right] \\
&= 1+p^k-1+q^m-1+p^k q^m-p^k-q^m+1 \quad [\text{Expanding}] \\
&= p^k q^m
\end{aligned}$$

By Part (i) we have

$$\sum_{d\,|\,p^k q^m}\phi(d) = p^k q^m = \sum_{d\,|\,p^k}\phi(d)\sum_{d'\,|\,q^m}\phi(d')$$

Hence, we have our required result.

■

(iii) To prove $\sum_{d\,|\,n}\phi(d) = n$ we write n in prime decomposition form and then apply proof by induction.

Proof.

Let $n = p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_r^{k_r}$ where p are distinct primes. Then by part (i) we have

$$\sum_{d\,|\,p_1^{k_1}}\phi(d) = p_1^{k_1}$$

We assume the result is true for $r = m$:

$$\sum_{d\,|\,p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m}}\phi(d) = p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m} \qquad (*)$$

Required to prove the result for $r = m+1$:

$$\sum_{d\,|\,p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m}\times p_{m+1}^{k_{m+1}}}\phi(d) = p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m}\times p_{m+1}^{k_{m+1}}.$$

We can write

$$p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m}\times p_{m+1}^{k_{m+1}} = \left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m}\right)\times p_{m+1}^{k_{m+1}}.$$

Since the p's are distinct primes so $\gcd\left(p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_m^{k_m},\ \ p_{m+1}^{k_{m+1}}\right) = 1$. By part (ii) we have

$$\sum_{d \,\left|\, \left(p_1^{\,k_1} \times p_2^{\,k_2} \times \cdots \times p_m^{\,k_m}\right) \times p_{m+1}^{\,k_{m+1}}} \phi\left(d\right) = \sum_{d \,\left|\, \left(p_1^{\,k_1} \times p_2^{\,k_2} \times \cdots \times p_m^{\,k_m}\right)} \phi\left(d\right) \;\times \sum_{d \,\left|\, p_{m+1}^{\,k_{m+1}}\right.} \phi\left(d\right)$$

$$= \underbrace{\left(p_1^{\,k_1} \times p_2^{\,k_2} \times \cdots \times p_m^{\,k_m}\right)}_{\text{by (*)}} \times \underbrace{p_{m+1}^{\,k_{m+1}}}_{\text{by part (i)}} = n$$

This completes our proof.

■