Mathematical Reasoning

Chapter 6. Number Theory

6.6. The Inclusion-Exclusion Principle and Euler's Function—Proofs of Theorems

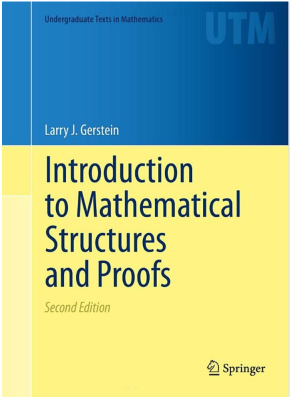

Table of contents

Corollary 6.57. Inclusion-Exclusion Principle

Corollary 6.57. Inclusion-Exclusion Principle.
Let S be a finite set and suppose $A_1, A_2, \ldots, A_n$ are subsets of S. Define $S_0 = |S|$ and, for $1 \leq k \leq n$, define

$$S_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|.$$

Then $|A_1' \cap A_2' \cap \cdots \cap A_n'| = \sum_{k=0}^{n} (-1)^k S_k$.

Proof. DeMorgan's Law (Theorem 2.16(g) and induction) states that $(\cup_{i=1}^n A_i)' = \cap_{i=1}^n A_i'$. That is (with S as the universal set), $A_1' \cap A_2' \cap \cdots \cap A_n' = S - (\cup_{i=1}^n A_i)$. So $A_1' \cap A_2' \cap \cdots \cap A_n'$ and $(\cup_{i=1}^n A_i)$ are disjoint. Hence, by the Addition Rule (Theorem 4.14) we have

$$|A_1' \cap A_2' \cap \cdots \cap A_n'| + |\cup_{i=1}^n A_i| = |S|$$

or

$$|\cup_{i=1}^n A_i| = |S| - |A_1' \cap A_2' \cap \cdots \cap A_n'|.$$

Corollary 6.57. Inclusion-Exclusion Principle

Corollary 6.57. Inclusion-Exclusion Principle.
Let S be a finite set and suppose $A_1, A_2, \ldots, A_n$ are subsets of S. Define $S_0 = |S|$ and, for $1 \leq k \leq n$, define

$$S_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|.$$

Then $|A_1' \cap A_2' \cap \cdots \cap A_n'| = \sum_{k=0}^{n} (-1)^k S_k$.

Proof. DeMorgan's Law (Theorem 2.16(g) and induction) states that $(\cup_{i=1}^n A_i)' = \cap_{i=1}^n A_i'$. That is (with S as the universal set), $A_1' \cap A_2' \cap \cdots \cap A_n' = S - (\cup_{i=1}^n A_i)$. So $A_1' \cap A_2' \cap \cdots \cap A_n'$ and $(\cup_{i=1}^n A_i)$ are disjoint. Hence, by the Addition Rule (Theorem 4.14) we have

$$|A_1' \cap A_2' \cap \cdots \cap A_n'| + |\cup_{i=1}^n A_i| = |S|$$

or

$$|\cup_{i=1}^n A_i| = |S| - |A_1' \cap A_2' \cap \cdots \cap A_n'|.$$

Corollary 6.57 (continued 1)

Proof (continued). ...

$$
\begin{aligned}
|\cup_{i=1}^{n} A_i| &= |S| - |A_1' \cap A_2' \cap \cdots \cap A_n'| \\
&= \sum_{i=1}^{n} |A_i| - \left(\sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| \right) \\
&\quad + \left(\sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \right) \\
&\quad - \left(\sum_{1 \le i_1 < i_2 < i_3 < i_4 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| \right) + \cdots \\
&\quad + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots A_n| \text{ by Theorem 6.56} \\
&= \sum_{k=1}^{n} (-1)^{k+1} S_k = -\sum_{k=1}^{n} (-1)^k S_k.
\end{aligned}
$$

Corollary 6.57 (continued 2)

Corollary 6.57. Inclusion-Exclusion Principle.
Let S be a finite set and suppose $A_1, A_2, \ldots, A_n$ are subsets of S. Define $S_0 = |S|$ and, for $1 \leq k \leq n$, define

$$S_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|.$$

Then $|A_1' \cap A_2' \cap \cdots \cap A_n'| = \sum_{k=0}^{n} (-1)^k S_k$.
Proof (continued). ...

$$|\cup_{i=1}^{n} A_i| = |S| - |A_1' \cap A_2' \cap \cdots \cap A_n'| = -\sum_{k=1}^{n} (-1)^k S_k.$$

Since $S_0 = |S|$, then

$$|A_1' \cap A_2' \cap \cdots \cap A_n'| = |S| + \sum_{k=1}^{n} (-1)^k S_k = \sum_{k=0}^{n} (-1)^k S_k,$$

as claimed. □

Theorem 6.59

Theorem 6.59. If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{1 \le i \le r} \left(1 - \frac{1}{p_i}\right) = n \prod_{1 \le i \le r} \left(\frac{p_i - 1}{p_i}\right) = \prod_{1 \le i \le r} p_i^{\alpha_i - 1} \prod_{1 \le i \le r} (p_i - 1).$$

Moreover, if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. By Note 6.6.B, $\varphi(n) = |A_1' \cap A_2' \cap \cdots \cap A_r'|$ and by Note 6.6.C, $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = \dfrac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}$ for all $1 \le k \le r$. So by the Inclusion-Exclusion Principle (Corollary 6.57) with $S = \mathbb{N}_n$, we have

$$\varphi(n) = |A_1' \cap A_2' \cap \cdots \cap A_r'| = \sum_{k=0}^{r} (-1)^k S_k$$

$$= \sum_{k=0}^{r} (-1)^k \left(\sum_{1 \le i_1 < i_2 < \cdots < i_k \le r} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \right) \ldots$$

Theorem 6.59

Theorem 6.59. If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{1 \le i \le r} \left(1 - \frac{1}{p_i}\right) = n \prod_{1 \le i \le r} \left(\frac{p_i - 1}{p_i}\right) = \prod_{1 \le i \le r} p_i^{\alpha_i - 1} \prod_{1 \le i \le r} (p_i - 1).$$

Moreover, if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. By Note 6.6.B, $\varphi(n) = |A_1' \cap A_2' \cap \cdots \cap A_r'|$ and by Note 6.6.C, $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = \dfrac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}$ for all $1 \le k \le r$. So by the Inclusion-Exclusion Principle (Corollary 6.57) with $S = \mathbb{N}_n$, we have

$$\varphi(n) = |A_1' \cap A_2' \cap \cdots \cap A_r'| = \sum_{k=0}^{r} (-1)^k S_k$$

$$= \sum_{k=0}^{r} (-1)^k \left(\sum_{1 \le i_1 < i_2 < \cdots < i_k \le r} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \right) \ldots$$

Theorem 6.59 (continued 1)

Proof (continued). ...

$$\varphi(n) = \sum_{k=0}^{r} (-1)^k \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}} \text{ by Note 6.6.C.}$$

It is shown in Exercise 6.6.A (by induction) that

$$\sum_{k=0}^{r} (-1)^k \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_k}} = 1 - \sum_{1 \le i_1 \le r} \frac{1}{p_{i_1}} + \sum_{1 \le i_1 < i_2 \le r} \frac{1}{p_{i_1} p_{i_2}}$$

$$- \sum_{1 \le i_1 < i_2 < i_3 \le r} \frac{1}{p_{i_1} p_{i_2} p_{i_3}} + \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}$$

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

Theorem 6.59 (continued 2)

Theorem 6.59. If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{1 \leq i \leq r} \left(1 - \frac{1}{p_i}\right) = n \prod_{1 \leq i \leq r} \left(\frac{p_i - 1}{p_i}\right) = \prod_{1 \leq i \leq r} p_i^{\alpha_i - 1} \prod_{1 \leq i \leq r} (p_i - 1).$$

Moreover, if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof (continued). ...

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

Since $1 - \dfrac{1}{p_i} = \dfrac{p_i - 1}{p_i}$ for each $1 \leq i \leq r$ then the second equality holds.
Since $\dfrac{p_i - 1}{p_i} = p_i^{-1}(p_i - 1)$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ then the third equality holds.

Theorem 6.59 (continued 3)

Theorem 6.59. If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{1 \leq i \leq r} \left(1 - \frac{1}{p_i}\right) = n \prod_{1 \leq i \leq r} \left(\frac{p_i - 1}{p_i}\right) = \prod_{1 \leq i \leq r} p_i^{\alpha_i - 1} \prod_{1 \leq i \leq r} (p_i - 1).$$

Moreover, if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof (continued). If $(m, n) = 1$ then the standard factorization of m is $q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ for primes q_i for $1 \leq i \leq s$, and $p_i \neq q_j$ for all $1 \leq i \leq r$ and $1 \leq j \leq s$. So by the third equality,

$$\varphi(mn) = \prod_{1 \leq i \leq r} p_i^{\alpha_i - 1} \prod_{1 \leq i \leq r} (p_i - 1) \prod_{1 \leq j \leq s} q_i^{\beta_j - 1} \prod_{1 \leq j \leq s} (q_j - 1) = \varphi(m)\varphi(n),$$

as claimed. $\square$

Theorem 6.62

Theorem 6.62. If $n > 2$ then $\varphi(n)$ is even.

Proof. First, suppose n is a power of 2, say $n = 2^k$ with $k \geq 2$. Then by Corollary 6.60, $\varphi(2^k) = 2^{k-1}(2-1) = 2^{k-1}$ where $k - 1 \geq 1$. That is, $\varphi(n)$ is even.

Theorem 6.62

Theorem 6.62. If $n > 2$ then $\varphi(n)$ is even.

Proof. First, suppose n is a power of 2, say $n = 2^k$ with $k \geq 2$. Then by Corollary 6.60, $\varphi(2^k) = 2^{k-1}(2-1) = 2^{k-1}$ where $k - 1 \geq 1$. That is, $\varphi(n)$ is even.

If n is not a power of 2, then $n = p^k m$ for some odd prime p, $k \geq 1$, and $(p, m) = 1$. Then

$$\begin{aligned} \varphi(n) &= \varphi(p^k m) = \varphi(p^k)\varphi(m) \text{ by Theorem 6.59} \\ &= p^{k-1}(p-1)\varphi(m) \text{ by Corollary 6.60.} \end{aligned}$$

Since $p - 1$ is even, then $\varphi(n)$ is even in this case also, as claimed. □

Theorem 6.62

Theorem 6.62. If $n > 2$ then $\varphi(n)$ is even.

Proof. First, suppose n is a power of 2, say $n = 2^k$ with $k \geq 2$. Then by Corollary 6.60, $\varphi(2^k) = 2^{k-1}(2-1) = 2^{k-1}$ where $k - 1 \geq 1$. That is, $\varphi(n)$ is even.

If n is not a power of 2, then $n = p^k m$ for some odd prime p, $k \geq 1$, and $(p, m) = 1$. Then

$$\begin{aligned} \varphi(n) &= \varphi(p^k m) = \varphi(p^k)\varphi(m) \text{ by Theorem 6.59} \\ &= p^{k-1}(p-1)\varphi(m) \text{ by Corollary 6.60.} \end{aligned}$$

Since $p - 1$ is even, then $\varphi(n)$ is even in this case also, as claimed. □

Theorem 6.63

Theorem 6.63. If n is a positive integer, then $\varphi(n) > \sqrt{n}/2$. Hence, $\lim_{n\to\infty} \varphi(n) = \infty$.

Proof. If $n = 1$, then $\varphi(1) = 1 > \sqrt{1}/2 = 1/2$. If $n = 2^k$ is a power of 2, then as shown in the proof of Theorem 6.62,
$\varphi(2^k) = 2^{k-1} > 2^{k/2-1} = \sqrt{2^k}/2$. If $n > 1$ is not a power of 2, the n has a standard factorization of the form $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $\alpha_0 \geq 0$ and $\alpha_i \geq 1$ for some $1 \leq i \leq r$.

Theorem 6.63

Theorem 6.63. If n is a positive integer, then $\varphi(n) > \sqrt{n}/2$. Hence, $\lim_{n\to\infty} \varphi(n) = \infty$.

Proof. If $n = 1$, then $\varphi(1) = 1 > \sqrt{1}/2 = 1/2$. If $n = 2^k$ is a power of 2, then as shown in the proof of Theorem 6.62, $\varphi(2^k) = 2^{k-1} > 2^{k/2-1} = \sqrt{2^k}/2$. If $n > 1$ is not a power of 2, the n has a standard factorization of the form $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $\alpha_0 \geq 0$ and $\alpha_i \geq 1$ for some $1 \leq i \leq r$. Then

$$\begin{aligned}
\varphi(n) &= \varphi(2^{\alpha_0})\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_r^{\alpha_r}) \text{ by Theorem 6.59} \\
&= 2^{\alpha_0-1} p_1^{\alpha_1-1}(p_1^{\alpha_1}-1) p_2^{\alpha_2-1}(p_2^{\alpha_2}-1)\cdots p_r^{\alpha_r-1}(p_1^{\alpha_1}-1) \\
&\quad \text{by Corollary 6.60} \\
&> 2^{\alpha_0-1} p_1^{\alpha_1-1/2} p_2^{\alpha_2-1/2} \cdots p_r^{\alpha_r-1/2} \text{ since } p_i - 1 \geq \sqrt{p_i} \\
&\quad \text{for all prime } p_i > 2
\end{aligned}$$

Theorem 6.63

Theorem 6.63. If n is a positive integer, then $\varphi(n) > \sqrt{n}/2$. Hence, $\lim_{n\to\infty} \varphi(n) = \infty$.

Proof. If $n = 1$, then $\varphi(1) = 1 > \sqrt{1}/2 = 1/2$. If $n = 2^k$ is a power of 2, then as shown in the proof of Theorem 6.62, $\varphi(2^k) = 2^{k-1} > 2^{k/2-1} = \sqrt{2^k}/2$. If $n > 1$ is not a power of 2, the n has a standard factorization of the form $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $\alpha_0 \geq 0$ and $\alpha_i \geq 1$ for some $1 \leq i \leq r$. Then

$$\begin{aligned}
\varphi(n) &= \varphi(2^{\alpha_0})\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_r^{\alpha_r}) \text{ by Theorem 6.59} \\
&= 2^{\alpha_0-1}p_1^{\alpha_1-1}(p_1^{\alpha_1}-1)p_2^{\alpha_2-1}(p_2^{\alpha_2}-1)\cdots p_r^{\alpha_r-1}(p_1^{\alpha_1}-1) \\
&\quad \text{ by Corollary 6.60} \\
&> 2^{\alpha_0-1}p_1^{\alpha_1-1/2}p_2^{\alpha_2-1/2}\cdots p_r^{\alpha_r-1/2} \text{ since } p_i - 1 \geq \sqrt{p_i} \\
&\quad \text{ for all prime } p_i > 2
\end{aligned}$$

Theorem 6.63 (continued)

Theorem 6.63. If n is a positive integer, then $\varphi(n) > \sqrt{n}/2$. Hence, $\lim_{n\to\infty} \varphi(n) = \infty$.

Proof (continued). ...

$$\begin{aligned} \varphi(n) &> 2^{\alpha_0-1} p_1^{\alpha_1-1/2} p_2^{\alpha_2-1/2} \cdots p_r^{\alpha_r-1/2} \\ &\geq 2^{\alpha_0-1} p_1^{\alpha_1/2} p_2^{\alpha_2/2} \cdots p_r^{\alpha_r/2} \text{ since } \alpha_i - 1/2 \geq \alpha_i/2 \\ &\quad \text{ because } \alpha_i \geq 1 \text{ for } 1 \leq i \leq r \\ &\geq 2^{\alpha_0/2-1} p_1^{\alpha_1/2} p_2^{\alpha_2/2} \cdots p_r^{\alpha_r/2} \text{ since } \alpha_0/2 - 1 \leq \alpha_0 - 1 \\ &= \sqrt{n}/2. \end{aligned}$$

So $\varphi(n) > \sqrt{n}/2$ in all cases, as claimed. □

Theorem 6.64

Theorem 6.64. If $m = 2 \cdot 5^{2k}$, with $k \in \mathbb{N}$, then there is no integer n such that $\varphi(n) = m$.

Proof. ASSUME that there is some n such that $\varphi(n) = 2 \cdot 5^{2k}$. Let the standard factorization of n be $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then by Theorem 6.59 and Corollary 6.60,

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1)(p_2 - 1) \cdots (p_r - 1). \ (*)$$

Theorem 6.64

Theorem 6.64. If $m = 2 \cdot 5^{2k}$, with $k \in \mathbb{N}$, then there is no integer n such that $\varphi(n) = m$.

Proof. ASSUME that there is some n such that $\varphi(n) = 2 \cdot 5^{2k}$. Let the standard factorization of n be $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then by Theorem 6.59 and Corollary 6.60,

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1)(p_2 - 1) \cdots (p_r - 1). \; (*)$$

Now for each odd prime p_i, $p_i - 1$ is even. But since $\varphi(n) = 2 \cdot 5^{2k}$, then only one p_i can be an odd prime. Moreover, if $n = 2^\ell$ then $\varphi(n) = 2^{\ell - 1}$ as seen in the proof of Theorem 6.62, but then $\varphi(n)$ lacks the power of 5 so this cannot be the case. That is, n must be of the form $n = 2^\alpha p^\beta$ where p is an odd prime, $\beta \geq 1$, and $\alpha \in \{0, 1\}$; for if $\alpha \geq 2$ then $\varphi(n)$ includes a factor of $2^{\alpha - 1}$ and another factor of 2 from $p - 1$, by $(*)$ in which case $\varphi(n)$ has a factor of 4.

Theorem 6.64

Theorem 6.64. If $m = 2 \cdot 5^{2k}$, with $k \in \mathbb{N}$, then there is no integer n such that $\varphi(n) = m$.

Proof. ASSUME that there is some n such that $\varphi(n) = 2 \cdot 5^{2k}$. Let the standard factorization of n be $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then by Theorem 6.59 and Corollary 6.60,

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1)(p_2 - 1) \cdots (p_r - 1). \ (*)$$

Now for each odd prime p_i, $p_i - 1$ is even. But since $\varphi(n) = 2 \cdot 5^{2k}$, then only one p_i can be an odd prime. Moreover, if $n = 2^\ell$ then $\varphi(n) = 2^{\ell - 1}$ as seen in the proof of Theorem 6.62, but then $\varphi(n)$ lacks the power of 5 so this cannot be the case. That is, n must be of the form $n = 2^\alpha p^\beta$ where p is an odd prime, $\beta \geq 1$, and $\alpha \in \{0, 1\}$; for if $\alpha \geq 2$ then $\varphi(n)$ includes a factor of $2^{\alpha - 1}$ and another factor of 2 from $p - 1$, by $(*)$ in which case $\varphi(n)$ has a factor of 4.

Theorem 6.64 (continued)

Theorem 6.64. If $m = 2 \cdot 5^{2k}$, with $k \in \mathbb{N}$, then there is no integer n such that $\varphi(n) = m$.

Proof (continued). Hence

$$\varphi(n) = \varphi(2^\alpha p^\beta) = \varphi(2^\alpha)\varphi(p^\beta) = (1)p^{\beta-1}(p-1) = 2 \cdot 5^{2k}.$$

Now if $\beta > 1$ then $p = 5$ (since the only prime divisors of $2 \cdot 5^{2k}$ are 2 and 5, and we know p is an odd prime). This gives $p - 1 = 4$, but then we have too many factors of 2 in $\varphi(n)$. So we must have $\beta = 1$, and then $\varphi(n) = p^{\beta-1}(p-1) = p - 1 = 2 \cdot 5^{2k}$, or $p = 1 + 2 \cdot 5^{2k}$. But $5^{2k} = (25)^k \equiv 1 \pmod 3$ (since $25 \equiv 1 \pmod 3$ and by Corollary 6.43), so $2 \cdot 5^{2k} \equiv 2 \pmod 3$ (also by Corollary 6.43). Therefore, $p = 1 + 2 \cdot 5^{2k} \equiv 0 \pmod 3$. But the only prime which is divisible by 3 is 3 itself, so we must have $p = 3$. Since $n = 2^\alpha \cdot p^\beta$ and we have that $\alpha \in \{0, 1\}$, $\beta = 1$, and $p = 3$ then we conclude that $n = 3$ or $n = 4$. But $\varphi(3) = \varphi(4) = 2 \neq 2 \cdot 5^{2k}$ where $k \in \mathbb{N}$, a CONTRADICTION. So the assumption that $\varphi(n) = 2 \cdot 5^{2k}$ for some n is false, and the claim holds. □

Theorem 6.64 (continued)

Theorem 6.64. If $m = 2 \cdot 5^{2k}$, with $k \in \mathbb{N}$, then there is no integer n such that $\varphi(n) = m$.

Proof (continued). Hence

$$\varphi(n) = \varphi(2^\alpha p^\beta) = \varphi(2^\alpha)\varphi(p^\beta) = (1)p^{\beta-1}(p-1) = 2 \cdot 5^{2k}.$$

Now if $\beta > 1$ then $p = 5$ (since the only prime divisors of $2 \cdot 5^{2k}$ are 2 and 5, and we know p is an odd prime). This gives $p - 1 = 4$, but then we have too many factors of 2 in $\varphi(n)$. So we must have $\beta = 1$, and then $\varphi(n) = p^{\beta-1}(p-1) = p - 1 = 2 \cdot 5^{2k}$, or $p = 1 + 2 \cdot 5^{2k}$. But $5^{2k} = (25)^k \equiv 1 \pmod 3$ (since $25 \equiv 1 \pmod 3$ and by Corollary 6.43), so $2 \cdot 5^{2k} \equiv 2 \pmod 3$ (also by Corollary 6.43). Therefore, $p = 1 + 2 \cdot 5^{2k} \equiv 0 \pmod 3$. But the only prime which is divisible by 3 is 3 itself, so we must have $p = 3$. Since $n = 2^\alpha \cdot p^\beta$ and we have that $\alpha \in \{0, 1\}$, $\beta = 1$, and $p = 3$ then we conclude that $n = 3$ or $n = 4$. But $\varphi(3) = \varphi(4) = 2 \neq 2 \cdot 5^{2k}$ where $k \in \mathbb{N}$, a CONTRADICTION. So the assumption that $\varphi(n) = 2 \cdot 5^{2k}$ for some n is false, and the claim holds. $\square$