6.6. The Inclusion-Exclusion Principle and Euler's Function

Note. In this section, we state (without a general proof) the Inclusion-Exclusion Principle (in Corollary 6.57) concerning the cardinality of the union of several (finite) sets. This is then used to derive a formula for $\varphi(n)$ in terms of the standard factorization of n (in Theorem 6.59). In this section, we denote the number of elements in set X as $|X|$ (as is more traditional), as opposed to $\#X$ as done previously.

Note 6.6.A. For finite sets A and B, we saw in Corollary 4.16 of Section 4.1. Cardinality; Fundamental Counting Principles that

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

We want to consider a finite collection of finite sets, $A_1, A_2, \ldots, A_n$ and express the cardinality of the union of these sets in terms of the cardinalities of the sets themselves (similar to Corollary 4.16). For three sets, we have:

$$\begin{aligned}
\left|\cup_{i=1}^{3} A_i\right| &= |(A_1 \cup A_2) \cup A_3| \\
&= |A \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \text{ by Corollary 4.16} \\
&= |A_1 \cup A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| \text{ by Theorem 2.16(c)} \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - (|A_1 \cap A_3| + |A_2 \cap A_3| \\
&\quad -|A_1 \cap A_2 \cap A_3|) \\
&\quad \text{applying Corollary 4.16 to} |A_1 \cup A_2| \text{ and to } |(A_1 \cap A_3) \cup (A_2 \cap A_3)|
\end{aligned}$$

$$\begin{aligned} &= |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) \\ &\quad + |A_1 \cap A_2 \cap A_3| \\ &= \sum_{i=1}^{3} |A_i| - \left(\sum_{1 \le i < j \le 3} |A_i \cap A_j| \right) + |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

Notice that the first terms adds up the cardinalities of the three sets, but this counts some elements twice (or three times). The second term subtracts the count of the elements that are contained in pairs of sets, but this if an element was in all three sets then it is removed twice here. In the third term, the count of those elements removed twice by the second term are added back. That is, the first term *includes* all elements (but includes some multiple times), the second term then *excludes* the elements that were counted more than once by the first term (but removes some terms too many times), then the third term *includes* the terms removed too many times by the second term. That's why this idea is called the Inclusion-Exclusion Principle. Similar to the argument above, we can inductively prove the following general result. A proof is omitted here, but can be found in my online notes for Intermediate Probability and Statistics (not an official ETSU class) on Section 1.10. The Probability of a Union of Events (notice Theorem 1.10.2).

Theorem 6.56. Let $A_1, A_2, \ldots, A_n$ be sets. Then

$$|\cup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \left(\sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| \right) + \left(\sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \right)$$

$$- \left(\sum_{1 \le i_1 < i_2 < i_3 < i_4 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| \right) + \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots A_n|.$$

Note. Gerstein does not take Theorem 6.56 as the Inclusion=Exclusion Principle (unlike what you are likely to see in a statistics class; for example, see my online notes for Mathematical Statistics 1 (STAT 4047/5047) on Section 1.3. The Probability Set Function (notice Theorems 1.3.A and 1.3.B). Instead he expresses it as follows and uses this new version to find a formula for $\varphi(n)$.

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 $|A_1' \cap A_2' \cap \cdots \cap A_n'| = \sum_{k=0}^{n} (-1)^k S_k$. (Recall that A_i' is the complement of A in S.)

Example 6.58. A sports club has 54 members. Of those, 34 play tennis, 22 play golf, and 10 play both. Eleven members play handball and, of those, 6 play tennis, 4 play golf, and 2 play all three sports. How many club members participate in none of the sports?

Solution. Let A_1 be the set of those who play tennis, A_2 be the set of those who play golf, A_3 be the set of those who play handball, and let S be the set of all sports club members. Then $|S| = 54$, $|A_1| = 34$, $|A_2| = 22$, $|A_3| = 11$, $|A_1 \cap A_2| = 10$, $|A_1 \cap A_3| = 6$, $|A_2 \cap A_3| = 4$, and $|A_1 \cap A_2 \cap A_3| = 2$. Notice that the set of those who participate in none of the sports is $A_1' \cap A_2' \cap A_3'$. With $n = 3$ in the

Inclusion-Exclusion Principle (Corollary 6.57), we have

$$|A_1' \cap A_2' \cap A_3'| = \sum_{k=0}^{3} (-1)^k S_k$$

$$= S_0 - S_1 + S_2 - S_3 = (54) - (31 + 22 + 11) + (10 + 6 + 4) - (2) = \boxed{5}. \square$$

Note 6.6.B. We next use the Inclusion-Exclusion Principle to derive a formula for $\varphi(n)$, given a standard factorization of n, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. First, define $A_i = \{m \in \mathbb{N}_n \mid p_i \,|\, m\}$, so that the elements of A_i are all multiples of p_i less than or equal to n. Since p_i is prime, then $A_i' = \mathbb{N}_n - A_i$ is the set of positive integers less than or equal to n that are relatively prime with p_i. Since $p_1, p_2, \ldots, p_r$ are the only prime divisors of n, then set of all numbers less than or equal to n that are relatively prime with n are in the set $A_1' \cap A_2' \cap \cdots \cap A_r'$. That is, $\varphi(n) = |A_1' \cap A_2' \cap \cdots \cap A_r'|$.

Note 6.6.C. Notice that if k is a positive integer and $K \,|\, n$, then there are precisely n/k positive multiples of k less than or equal to k; namely, $k, 2k, 3k, \ldots, (n/k - 1)k, (n/k)n = k$. Since the elements of A_i are the multiples of p_i less than or equal to n, the $|A_i| = n/p_i$. Now $A_{i_1} \cap A_{i_2}$ is the set of all multiples of both p_{i_1} and p_{i_2} less than or equal to n; that is, all multiples of $p_{i_1} p_{i_2}$ less than or equal to n so that $|A_{i_1} \cap A_{i_2}| = \dfrac{n}{p_{i_1} p_{i_2}}$. Similarly

$$|A_{i_1} \cap A_{i_2} \cap A_{i_3}| = \frac{n}{p_{i_1} p_{i_2} p_{i_3}}, |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| = \frac{n}{p_{i_1} p_{i_2} p_{i_3} p_{i_4}}, \ldots$$

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_r}}.$$

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 $\varphi(mn)=\varphi(m)\varphi(n)$.

Corollary 6.60. If p is prime and $k\ge 1$, then $\varphi(p^k) = p^{k-1}(p-1) = p^k - p^{k-1}$.

Example 6.61. Corollary 6.60, along with the fact that $\varphi(mn)=\varphi(m)\varphi(n)$ when $(m,n)=1$ of Theorem 6.59, gives an efficient way to compute $\varphi(n)$, provided we have a standard factorization of n. Consider $n = 280{,}500 = 2^2\cdot 3\cdot 5^3\cdot 11\cdot 17$. We have

$$\begin{aligned}
\varphi(280{,}500 &= \varphi(2^2\cdot 3\cdot 5^3\cdot 11\cdot 17)\\
&= \varphi(2^2)\varphi(3)\varphi(5^3)\varphi(11) = \varphi(17) \text{ by Theorem 6.59)}\\
&= (2^1\cdot 1)(3^0\cdot 2)(5^2\cdot 4)(11^0\cdot 10)(17^0\cdot 16) \text{ by Corollary 6.60}\\
&= (2)(2)(100)(10)(16) = \boxed{64{,}000}.\ \square
\end{aligned}$$

Note. A table of values of $\varphi(n)$ starts as follows:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12	10

A Javascript App is online at JavaScripter.net which will compute $\varphi(n)$ for n up to 20 digits. The table above suggests the next theorem.

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

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

Note. We might think that every positive even integer is the value of $\varphi(n)$ for some n. That is, we might think that φ maps $\mathbb{N}$ onto the positive even integers. The next theorem shows that this is not the case.

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

Note. Gerstein concludes the discussion of Euler's φ function with some open conjectures.

1. In 1907, Robert Carmichael published the paper "On Euler's φ-Function," *Bulletin of the American Mathematical Society*, **13**(5), 241–243 (1907). In this he claimed to have proved that if k is in the range of φ, then there are at least two distinct natural numbers n and n' such that $\varphi(n) = \varphi(n') = k$. An error was found in his proof and in 1922 he had to issue a retraction. This has become known as Carmichael's Conjecture. Kevin Ford proved that the conjecture holds for all $n < 10^{10^{10}}$ in "The Distribution of Totients," *The Ramanujan Journal*, **2**(1-2), 67-151 (1998). A copy of this paper is available on Kevin Ford's website (see Theorem 6; accessed 2/26/2022). However, the general conjecture remains unproved.

2. We know that $\varphi(p) = p - 1$ if and only if p is prime. For n composite, we cannot have $\varphi(n) = n - 1$, but it is possible that $\varphi(n) \,|\, (n - 1)$. Derrick

H. Lehmer conjectured that no such composite n exist in "On Euler's Totient Function," *Bulletin of the American Mathematical Society*, **38**, 745-751 (1932). Thsi paper is online on the AMS website (accessed 2/26/2022).

3. Gerstein mentions a conjecture that there are infinitely many n such that $\varphi(n) = \varphi(n+1)$, and claims that there are 391 such values of n less that 200,000,000. He doesn't give references and your humble instructor is unsuccessful in finding more details.

Revised: 2/27/2022