Math 222 Fall 2022, Lecture 20: Binomial coefficients

website: `https://www.cip.ifi.lmu.de/~grinberg/t/22fco`

2. Binomial coefficients (cont'd)

2.7. The principle of inclusion and exclusion (aka Sylvester's sieve formula) (cont'd)

2.7.1. Applications

Last time, we proved the Principle of Inclusion and Exclusion, which (in one of its forms) says the following:

Theorem 2.7.8 (Theorem, repeated for convenience)**.** Let $n \in \mathbb{N}$. Let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Then,

$$\begin{aligned}&(\#\text{ of all } s \in U \text{ such that } s \notin A_i \text{ for all } i \in [n])\\ &= \sum_{I \subseteq [n]} (-1)^{|I|} \left(\#\text{ of all } s \in U \text{ such that } s \in A_i \text{ for all } i \in I\right).\end{aligned}$$

Here is yet another way to restate this theorem, which I find easier to memorize (and thus also more convenient to apply):

"Rule-breaking interpretation" of the Principle of Inclusion and Exclusion.

Assume that we are given a finite set U, and we are given n rules (numbered $1, 2, \ldots, n$) that each element of U may or may not satisfy. (For instance, a rule can say "thou shalt be even" (if U is a set of numbers) or "thou shalt be nonempty" (if U is a set of sets).)

Assume that, for each $I \subseteq [n]$, we know how many elements $s \in U$ satisfy all rules in I (but may or may not satisfy the remaining rules). For example, this means that we know how many elements $s \in U$ satisfy rules 2, 3 and 5 simultaneously.

Then, we can compute the # of elements $s \in U$ that violate all n rules $1, 2, \ldots, n$ by the following formula:

$$\begin{aligned}&(\#\text{ of all } s \in U \text{ that violate all } n \text{ rules } 1, 2, \ldots, n)\\ &= \sum_{I \subseteq [n]} (-1)^{|I|} \left(\#\text{ of all } s \in U \text{ that satisfy all rules in } I\right).\end{aligned}$$

(Indeed, this is just Theorem 2.7.8, applied to $A_i = \{s \in U \mid s \text{ satisfies rule } i\}$.)

Now, let us use the Principle of Inclusion and Exclusion (in its "rule-breaking interpretation") to count several things that would otherwise be hard to count.

Example 1: Counting surjections. (See §2.9.4 in the 2019 notes for details.)

Let $m, n \in \mathbb{N}$. Let us compute $\operatorname{sur}(m,n)$. As we recall, this is the # of surjective maps (= surjections) from $[m]$ to $[n]$.

We set $U = [n]^{[m]} = \{\text{all maps from } [m] \text{ to } [n]\}$. We want to impose n rules $1, 2, \ldots, n$ on a map $s \in U$ in such a way that the surjective maps will be precisely those maps that violate all n rules $1, 2, \ldots, n$.

We set rule i to be "thou shalt not take i as a value". Then, a map $s : [m] \to [n]$ violates all rules $1, 2, \ldots, n$ if and only if it takes each of $1, 2, \ldots, n$ as a value, i.e., if it is surjective. Hence,

$$\begin{aligned}
&\operatorname{sur}(m,n) \\
&= (\#\text{ of surjective maps } [m] \to [n]) \\
&= (\#\text{ of all } s \in U \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (\#\text{ of all } s \in U \text{ that satisfy all rules in } I) \qquad (1)
\end{aligned}$$

(by the "rule-breaking interpretation" of the Principle of Inclusion and Exclusion).

Let us now compute the addends on the RHS of (1).

We fix a subset I of $[n]$. What is the # of all $s \in U$ that satisfy all rules in I ? This is just the # of all maps $s : [m] \to [n]$ that take none of the $i \in I$ as a value. These maps are essentially just the maps from $[m]$ to $[n] \setminus I$. Thus, their # is $|[n] \setminus I|^{[m]} = (n - |I|)^m$. So we obtain

$$(\#\text{ of all } s \in U \text{ that satisfy all rules in } I) = (n - |I|)^m . \qquad (2)$$

Forget that we fixed I. We thus have proved the equality (2) for every $I \subseteq [n]$.

Thus, (1) becomes

$$\begin{aligned}
\operatorname{sur}(m,n) &= \sum_{I\subseteq[n]} (-1)^{|I|} \underbrace{(\#\text{ of all } s\in U \text{ that satisfy all rules in } I)}_{\substack{=(n-|I|)^m \\ \text{(by (2))}}} \\
&= \sum_{I\subseteq[n]} (-1)^{|I|} (n-|I|)^m \\
&= \sum_{k=0}^{n} \underbrace{(\#\text{ of subsets } I\subseteq[n] \text{ satisfying } |I|=k)}_{=\binom{n}{k}} \cdot (-1)^k (n-k)^m \\
&\qquad \left(\begin{array}{c}\text{here, we have split the sum according to}\\ \text{the value of } |I|\text{, and observed that all}\\ \text{subsets } I \text{ of } [n] \text{ satisfying } |I|=k \text{ give identical}\\ \text{addends } (-1)^{|I|}(n-|I|)^m = (-1)^k(n-k)^m\end{array}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k (n-k)^m = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m \\
&= \sum_{j=0}^{n} (-1)^{n-j} \underbrace{\binom{n}{n-j}}_{=\binom{n}{j}} \left(\underbrace{n-(n-j)}_{=j}\right)^m \qquad \left(\begin{array}{c}\text{here, we substituted } n-j\\ \text{for } k \text{ in the sum}\end{array}\right) \\
&= \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} j^m.
\end{aligned}$$

Thus, we have proved the following:

Theorem 2.7.13. For any $m,n\in\mathbb{N}$, we have

$$\operatorname{sur}(m,n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} j^m.$$

This is the optimal answer to the question of computing $\operatorname{sur}(m,n)$; there is no simpler formula. Note that a few corollaries spring out:

Corollary 2.7.14. Let $n\in\mathbb{N}$. Then:

(a) We have $\sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m = 0$ for any $m\in\mathbb{N}$ such that $m<n$.

(b) We have $\sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^n = n!$.

(c) We have $\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m \geq 0$ for any $m \in \mathbb{N}$.

(d) The number $\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$ is divisible by $n!$ for any $m \in \mathbb{N}$.

Proof. Theorem 2.7.13 yields that $\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m = \operatorname{sur}(m,n)$. Hence,

- Corollary 2.7.14 **(a)** follows from Proposition 2.4.10 **(f)** in Lecture 16.
- Corollary 2.7.14 **(b)** follows from Corollary 2.4.13 **(a)** in Lecture 17.
- Corollary 2.7.14 **(c)** follows from $\operatorname{sur}(m,n) \geq 0$, which is obvious.
- Corollary 2.7.14 **(d)** follows from Corollary 2.4.13 **(b)** in Lecture 17.

(Note that none of the four parts of Corollary 2.7.14 is obvious algebraically!) □

Example 2. (See §2.9.5 in the 2019 notes for details.)

Recall that a **derangement** of a set X means a permutation of X that has no fixed points (i.e., a permutation s of X such that $s(x) \neq x$ for any $x \in X$).

We let D_n denote the # of derangements of $[n]$ for each $n \in \mathbb{N}$. Let's compute D_n. (We discussed these numbers D_n in §1.7.3 in Lecture 12; let us now see if we can derive some of the formulas for D_n.)

Fix $n \in \mathbb{N}$. Let U be the set of all permutations of $[n]$. We want to impose n rules $1, 2, \ldots, n$ on a permutation $s \in U$ in such a way that the derangements will be precisely the permutations s that violate all n rules $1, 2, \ldots, n$.

Namely, rule i says "thou shalt send i to i". Violating all these n rules (for a permutation of $[n]$) means sending no i to i, which means being a derangement. Thus,

$$\begin{aligned} D_n &= (\text{\# of all derangements of } [n]) \\ &= (\text{\# of all } s \in U \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of all } s \in U \text{ that satisfy all rules in } I) \end{aligned} \tag{3}$$

(by the "rule-breaking interpretation" of the Principle of Inclusion and Exclusion).

Again, we now need to compute the addends on the RHS.

So we fix a subset I of $[n]$, and we try to find the # of all permutations $s \in U$ that satisfy all rules in I. For instance, if $I = \{2, 5\}$, then this is the # of all permutations s of $[n]$ that satisfy $s(2) = 2$ and $s(5) = 5$. How many such permutations are there?

If a permutation s of $[n]$ satisfies $s(2) = 2$ and $s(5) = 5$, then it has to permute the remaining elements of $[n]$ (that is, the elements of $[n] \setminus \{2,5\}$) among each other; i.e., its restriction to $[n] \setminus \{2,5\}$ has to be a permutation of $[n] \setminus \{2,5\}$ (because the values 2 and 5 are already taken on the inputs 2 and 5, and a permutation cannot take the same value twice). Thus, the # of all permutations s of $[n]$ that satisfy $s(2) = 2$ and $s(5) = 5$ is the # of all permutations of $[n] \setminus \{2,5\}$. But the latter # is $(n-2)!$ (by Theorem 1.7.2 in Lecture 12, since $[n] \setminus \{2,5\}$ is an $(n-2)$-element set).

More generally, for any subset I of $[n]$, a permutation s of $[n]$ that satisfies all rules in I is essentially just a permutation of the set $[n] \setminus I$ (because it sends each element of I to itself, and thus must permute the elements of $[n] \setminus I$ among each other). Hence, the # of the former permutations equals the # of the latter permutations. In other words,

$$\begin{aligned} &(\#\text{ of all } s \in U \text{ that satisfy all rules in } I) \\ &= (\#\text{ of all permutations of } [n] \setminus I) \\ &= (n - |I|)! \end{aligned} \tag{4}$$

(by Theorem 1.7.2 in Lecture 12, since $[n] \setminus I$ is an $(n-|I|)$-element set).

Now, forget that we fixed I. We thus have proved (4) for every subset I of

$[n]$. Thus, (3) becomes

$$\begin{aligned}
D_n &= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{(\#\text{ of all } s \in U \text{ that satisfy all rules in } I)}_{\substack{=(n-|I|)! \\ \text{(by (4))}}} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (n - |I|)! \\
&= \sum_{k=0}^{n} \underbrace{(\#\text{ of subsets } I \subseteq [n] \text{ satisfying } |I| = k)}_{= \binom{n}{k}} \cdot (-1)^k (n-k)! \\
&\qquad \left(\begin{array}{c} \text{here, we have split the sum according to} \\ \text{the value of } |I| \text{, and observed that all} \\ \text{subsets } I \text{ of } [n] \text{ satisfying } |I| = k \text{ give identical} \\ \text{addends } (-1)^{|I|} (n - |I|)! = (-1)^k (n-k)! \end{array} \right) \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)! = \sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k} (n-k)!}_{= \frac{n!}{k!}} \\
&\qquad \left(\text{since } \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \right) \\
&= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.
\end{aligned}$$

So we have proved the following:

Theorem 2.7.15. Let $n \in \mathbb{N}$. Then, the # of derangements of $[n]$ is

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \tag{5}$$

We can transform this expression even further, if we recall a few facts from real analysis. Let $e \approx 2.718\ldots$ be Euler's number (well, one of the many numbers that bear Euler's name). It is well-known that

$$e^x = \exp x = \sum_{k=0}^{\infty} \frac{x^k}{k!} \qquad \text{for any } x \in \mathbb{R}.$$

Applying this to $x = -1$, we obtain

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}. \tag{6}$$

The infinite sum on the RHS here resembles the finite sum on the RHS of (5). And indeed, the two sums are very close to one another. To wit, for any $n \in \mathbb{N}$, we have

$$\sum_{k=0}^{\infty} \frac{(-1)^k}{k!} - \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}. \tag{7}$$

In view of (6) and (5), we can rewrite this as

$$e^{-1} - \frac{D_n}{n!} = \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}. \tag{8}$$

The RHS of this equality looks like it is very small (after all, the factorials $k!$ grow very quickly, so their reciprocals $\dfrac{1}{k!}$ quickly get microscopic). How small exactly? There is a nice (and easily proved) theorem in analysis that if $a_0, a_1, a_2, \ldots$ are positive real numbers satisfying $a_0 > a_1 > a_2 > a_3 > \cdots$, then $\left| \sum\limits_{k=m}^{\infty} (-1)^k a_k \right| < a_m$ for any $m \in \mathbb{N}$. Applying this to $a_k = \dfrac{1}{k!}$ and $m = n+1$, we obtain

$$\left| \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \right| < \frac{1}{(n+1)!} = \frac{1}{n! \cdot (n+1)}.$$

If $n \geq 1$, then this becomes

$$\left| \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \right| < \frac{1}{n! \cdot (n+1)} \leq \frac{1}{n! \cdot 2} \tag{9}$$

(since $n \geq 1$ entails $n+1 \geq 2$). In view of (8), this can be rewritten as

$$\left| e^{-1} - \frac{D_n}{n!} \right| < \frac{1}{n! \cdot 2}.$$

Multiplying this equality by the positive real $n!$, we obtain

$$\left| n! \cdot e^{-1} - D_n \right| < \frac{1}{2}.$$

In other words, the integer D_n is less than $\dfrac{1}{2}$ away from the real number $n! \cdot e^{-1}$ (provided that $n \geq 1$). Hence, D_n is the nearest integer to the real number $n! \cdot e^{-1} = \dfrac{n!}{e}$. We can rewrite this as follows:

$$D_n = \operatorname{round} \frac{n!}{e},$$

where $\operatorname{round} x$ denotes the nearest integer to a given real number x. Thus, we have proved the following:

Theorem 2.7.16. For any integer $n \geq 1$, we have

$$D_n = \operatorname{round} \frac{n!}{e}.$$

This strange formula for the # of derangements is suddenly not mysterious any more!

Back in Lecture 12, we have also stated two recursive formulas for D_n:

$$D_n = nD_{n-1} + (-1)^n \qquad \text{for all } n \geq 1;$$
$$D_n = (n-1)\left(D_{n-1} + D_{n-2}\right) \qquad \text{for all } n \geq 2.$$

These formulas can be derived purely algebraically from Theorem 2.7.15. (This is a fun exercise; for the solution, see Exercise 2.9.4 in the 2019 notes.)

Remark 2.7.17. From Theorem 2.7.16, we can easily derive the famous result that the number e is irrational.

Indeed, assume the contrary. Thus, $e = n/q$ for some positive integers n and q. Consider these n and q. Then, $\dfrac{n!}{e} = \dfrac{n!}{n/q} = q \cdot \dfrac{n!}{n} = q \cdot (n-1)!$ is an integer. Hence, $\operatorname{round} \dfrac{n!}{e} = \dfrac{n!}{e}$, so that Theorem 2.7.16 yields $D_n = \operatorname{round} \dfrac{n!}{e} = \dfrac{n!}{e}$.

Also, from $(n+1)! = (n+1) \cdot n!$, we obtain $\dfrac{(n+1)!}{e} = (n+1) \cdot \underbrace{\dfrac{n!}{e}}_{=q\cdot(n-1)!} = (n+1) \cdot q \cdot (n-1)!$, which is an integer as well. Thus, $\operatorname{round} \dfrac{(n+1)!}{e} = \dfrac{(n+1)!}{e}$. Hence, Theorem 2.7.16 (applied to $n+1$ instead of n) yields

$$D_{n+1} = \operatorname{round} \frac{(n+1)!}{e} = \frac{(n+1)!}{e} = (n+1) \cdot \underbrace{\frac{n!}{e}}_{=D_n} = (n+1) \cdot D_n$$

$$= \underbrace{(n+1) \cdot n!}_{=(n+1)!} \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!} \qquad \text{(by (5))}$$

$$= (n+1)! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Comparing this with

$$D_{n+1} = (n+1)! \cdot \sum_{k=0}^{n+1} \frac{(-1)^k}{k!} \qquad \text{(by (5), applied to } n+1 \text{ instead of } n),$$

we obtain $\sum\limits_{k=0}^{n+1} \dfrac{(-1)^k}{k!} = \sum\limits_{k=0}^{n} \dfrac{(-1)^k}{k!}$. This entails $\dfrac{(-1)^{n+1}}{(n+1)!} = 0$, which is absurd. This contradiction shows that our assumption was false, so that e is indeed irrational.

Example 3. (See §2.9.6 in the 2019 notes for details.)
The following number-theoretical result is also due to Euler:[1]

Theorem 2.7.18. Let c be a positive integer with prime factorization

$$c = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},$$

where $p_1, p_2, \ldots, p_n$ are distinct primes, and where $a_1, a_2, \ldots, a_n$ are positive integers. Then,

$$\begin{aligned}&(\#\text{ of all } s \in [c] \text{ that are coprime to } c)\\ &= c \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{n} \left(p_i^{a_i} - p_i^{a_i - 1}\right).\end{aligned}$$

Note that the # of all $s \in [c]$ that are coprime to c is usually denoted by $\phi(c)$, and the map $\phi : \{1, 2, 3, \ldots\} \to \mathbb{N}$ that sends each c to $\phi(c)$ is known as **Euler's totient function**.

Example 2.7.19. Let $c = 18$. Then, the prime factorization of c is $c = 2^1 \cdot 3^2$. Thus, Theorem 2.7.18 claims that

$$\begin{aligned}&(\#\text{ of all } s \in [18] \text{ that are coprime to } 18)\\ &= 18 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = \left(2^1 - 2^0\right) \cdot \left(3^2 - 3^1\right).\end{aligned}$$

And indeed, both sides of this equality are 6. The six numbers $s \in [18]$ that are coprime to 18 are $1, 5, 7, 11, 13, 17$.

Theorem 2.7.18 is proved in most textbooks on number theory. Let us, however, outline a proof using the PIE. This proof will heavily use **Euclid's lemma**, which (in one of its forms) says that if a prime p divides a product $b_1 b_2 \cdots b_k$ of some integers $b_1, b_2, \ldots, b_k$, then p must divide (at least) one of the factors $b_1, b_2, \ldots, b_k$. This yields, in particular, that if a prime p divides an integer c whose prime factorization is $c = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, then p must be one of $p_1, p_2, \ldots, p_n$. We will also use the **product divisibility lemma**, which says that if several **distinct prime** numbers $q_1, q_2, \ldots, q_k$ all divide a given integer s, then their product $q_1 q_2 \cdots q_k$ also divides s. (More generally, this still holds if we replace "distinct prime" by "pairwise coprime".)

Proof of Theorem 2.7.18 (sketched). Let $U = [c]$. A number $s \in U$ is coprime to c if and only if it is not divisible by any of the primes $p_1, p_2, \ldots, p_n$ (this follows from Euclid's lemma stated in the preceding paragraph). This means that s

[1] Recall that two integers a and b are said to be **coprime** (to one another) if $\gcd(a, b) = 1$.

violates all n rules $1, 2, \ldots, n$, where rule i says "thou shalt be divisible by p_i". Hence,

$$\begin{aligned}
&(\#\text{ of all } s \in [c] \text{ that are coprime to } c) \\
&= (\#\text{ of all } s \in [c] \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (\#\text{ of all } s \in [c] \text{ that satisfy all rules in } I) \qquad (10)
\end{aligned}$$

(by the "rule-breaking interpretation" of the Principle of Inclusion and Exclusion).

Now, let I be a subset of $[n]$. Then, an integer $s \in [c]$ satisfies all rules in I if and only if it is divisible by all primes p_i with $i \in I$; but this is equivalent to s being divisible by $\prod_{i \in I} p_i$ (here we are using the product divisibility lemma). Therefore,

$$\begin{aligned}
&(\#\text{ of all } s \in [c] \text{ that satisfy all rules in } I) \\
&= \left(\#\text{ of all } s \in [c] \text{ that are divisible by } \prod_{i \in I} p_i\right). \qquad (11)
\end{aligned}$$

However, $\prod_{i \in I} p_i$ is a divisor of c. Therefore, the numbers $s \in [c]$ that are divisible by $\prod_{i \in I} p_i$ are the numbers

$$\prod_{i \in I} p_i, \quad 2\prod_{i \in I} p_i, \quad 3\prod_{i \in I} p_i, \quad \ldots, \quad c.$$

These are $\dfrac{c}{\prod_{i \in I} p_i}$ many numbers. Therefore,

$$\left(\#\text{ of all } s \in [c] \text{ that are divisible by } \prod_{i \in I} p_i\right) = \frac{c}{\prod_{i \in I} p_i}.$$

Hence, (11) can be rewritten as

$$\begin{aligned}
&(\#\text{ of all } s \in [c] \text{ that satisfy all rules in } I) \\
&= \frac{c}{\prod_{i \in I} p_i}. \qquad (12)
\end{aligned}$$

Forget that we have fixed I. We thus have proved (12) for each subset I of $[n]$.

Now, (10) becomes

$$\begin{aligned}
&(\#\text{ of all } s \in [c] \text{ that are coprime to } c) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{(\#\text{ of all } s \in [c] \text{ that satisfy all rules in } I)}_{\substack{= \dfrac{c}{\prod\limits_{i \in I} p_i} \\ \text{(by (12))}}} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \frac{c}{\prod\limits_{i \in I} p_i} = c \cdot \sum_{I \subseteq [n]} (-1)^{|I|} \frac{1}{\prod\limits_{i \in I} p_i} \\
&= c \cdot \sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i}. \qquad (13)
\end{aligned}$$

The RHS of this equality turns out to be simplifiable. Indeed, for any n numbers $a_1, a_2, \ldots, a_n$, we have

$$\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} a_i = (1 - a_1)(1 - a_2) \cdots (1 - a_n)$$

(this is not hard to see by expanding the product on the RHS[2]). Applying this to $a_i = \dfrac{1}{p_i}$, we obtain

$$\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right) = \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right).$$

Hence, we can rewrite (13) as

$$(\#\text{ of all } s \in [c] \text{ that are coprime to } c) = c \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right).$$

We can rewrite this further:

$$\begin{aligned}
&(\#\text{ of all } s \in [c] \text{ that are coprime to } c) \\
&= \underbrace{c}_{\substack{= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\ = \prod\limits_{i=1}^{n} p_i^{a_i}}} \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) = \left(\prod_{i=1}^{n} p_i^{a_i}\right) \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{n} \underbrace{\left(p_i^{a_i}\left(1 - \frac{1}{p_i}\right)\right)}_{= p_i^{a_i} - p_i^{a_i - 1}} \\
&= \prod_{i=1}^{n} \left(p_i^{a_i} - p_i^{a_i - 1}\right).
\end{aligned}$$

This completes the proof of Theorem 2.7.18. □

[2] For example, for $n = 3$, we have $(1 - a_1)(1 - a_2)(1 - a_3) = 1 - a_1 - a_2 - a_3 + a_1 a_2 + a_1 a_3 + a_2 a_3 - a_1 a_2 a_3$, which is precisely $\sum\limits_{I \subseteq [3]} (-1)^{|I|} \prod\limits_{i \in I} a_i$. For a formal proof, see Lemma 2.9.21 **(b)** in the 2019 notes.