Applications of the Binomial Theorem

Discrete Mathematics 27100 Winter 2022

Recall the Binomial Theorem:

Theorem 0.1 (Binomial Theorem)**.** *For all* $n \in \mathbb{N} \cup \{0\}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

1 Proof of Fermat's Little Theorem via the Binomial Theorem

Theorem 1.1 (Restatement of Fermat's Little Theorem)**.** *For all primes* $p \in \mathbb{P}$ *and all integers* $x \in \mathbb{Z}$, $x^p \equiv x \mod p$

Proof. The key idea for proving Fermat's Little Theorem via the Binomial Theorem is the following lemma:

Lemma 1.2. *For all primes* $p \in \mathbb{P}$ *and all integers* $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p \mod p$

Proof. Observe that

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j \equiv a^p + b^p \mod p$$

because for all $j \in [p-1]$, $p \mid \binom{p}{j} = \frac{p!}{j!(n-j)!}$ as $p \mid p!$, $p \nmid j!$ and $p \nmid (n-j)!$. □

Corollary 1.3. *For all primes* $p \in \mathbb{P}$ *and all integers* $x \in \mathbb{Z}$, $(x+1)^p \equiv x^p + 1 \mod p$ *and* $(x-1)^p \equiv x^p - 1 \mod p$

Proof. By Lemma 1.2, $(x+1)^p \equiv x^p + 1^p \equiv x^p + 1 \mod p$ and $(x-1)^p \equiv x^p + (-1)^p \mod p$. If p is odd then $(-1)^p = -1$ so $(x-1)^p \equiv x^p - 1 \mod p$. If $p = 2$ then $(-1)^2 = 1$ but $1 \equiv -1 \mod 2$ so we still have that $(x-1)^p \equiv x^p - 1 \mod p$. Thus, in either case, $(x-1)^p \equiv x^p - 1 \mod p$. □

With this corollary in hand, we can now prove Fermat's Little Theorem by induction. For the base case, if $x = 0$ then $x^p \equiv x \equiv 0 \mod p$. For the inductive step, assume $x^p \equiv x \mod p$ for all integers x such that $|x| \leq k-1$ and consider $x = k$ and $x = -k$. For $x = k$, by Corollary 1.3 and the inductive hypothesis,

$$k^p = ((k-1)+1)^p \equiv (k-1)^p + 1 \equiv (k-1) + 1 \equiv k \mod p$$

Similarly, for $x = -k$,

$$(-k)^p = (-(k-1)-1)^p \equiv (-(k-1))^p - 1 \equiv -(k-1) - 1 \equiv -k \mod p$$

□

2 Unlabeled Balls into Labeled Bins

Consider the following question:
Q: How many ways are there to put 5 unlabeled balls into 3 labeled bins A, B, and C?

Answer: One way to solve this problem is to split it into cases:

1. If there are 5 balls in bin A then there are no balls left for bin C. This gives 1 possibility.
2. If there are 4 balls in bin A then we can either put the remaining ball in bin B or bin C. This gives 2 possibilities.
3. If there are 3 balls in bin A then we can put 0, 1, or 2 balls in bin B and put the remaining balls in bin C. This gives 3 possibilities.
4. If there are 2 balls in bin A then we can put 0, 1, 2, or 3 balls in bin B and put the remaining balls in bin C. This gives 4 possibilities.
5. If there is 1 ball in bin A then we can put 0, 1, 2, 3 or 4 balls in bin B and put the remaining balls in bin C. This gives 5 possibilities.
6. If there are 0 balls in bin A then we can put 0, 1, 2, 3, 4, or 5 balls in bin B and put the remaining balls in bin C. This gives 6 possibilities.

Thus, the total number of possibilities is $1 + 2 + 3 + 4 + 5 + 6 = 21 = \binom{7}{2}$. In fact, this is not a coincidence and can be shown using the following trick:

Instead of trying to place the balls into the labeled bins, imagine placing two dividing lines among the balls. The balls to the left of the first dividing line will be in bin A, the balls between the two dividing lines will be in bin B, and the balls to the right of the second dividing line will be in bin C. For example, $BB|B|BB$ would place two balls in bin A, one ball in bin B, and two balls in bin C. Viewed in this way, choosing how to split up the 5 balls into 3 labeled bins is equivalent to choosing where to put the 2 dividing lines among the 7 objects (5 balls and 2 dividing lines) and there are $\binom{7}{2} = 21$ ways to do this.

This idea generalizes to putting any number of unlabeled balls into labeled bins.

Theorem 2.1. *The number of ways to put n unlabeled balls into k labeled bins is $\binom{n+k-1}{k-1}$.*

Proof. Again, instead of trying to place the balls into the labeled bins, imagine placing $k - 1$ dividing lines among the balls. Viewed in this way, choosing how to split up the n balls into k labeled bins is equivalent to choosing where to put the $k - 1$ dividing lines among the $n + k - 1$ objects (n balls and $k - 1$ dividing lines) and there are $\binom{n+k-1}{k-1}$ ways to do this. □

3 Proof of the Principle of Inclusion/Exclusion

Recall the principle of inclusion/exclusion

Theorem 3.1 (Principle of Inclusion/Exclusion)**.** *For all $k \in \mathbb{N}$ and all finite sets $S_1, S_2, \ldots, S_k$,*

$$\left|\cup_{i=1}^{k} S_k\right| = \sum_{I \subseteq [k]: I \neq \emptyset} (-1)^{|I|+1} |\cap_{i \in I} S_i|$$

Proof. We partition $\cup_{i=1}^{k} S_k$ into pieces as follows:

Definition 3.2. *Given a non-empty subset $J \subseteq [k]$, we define $P_J = (\cap_{j \in J} S_j) \setminus (\cup_{i: i \notin J} S_i)$*

Definition 3.3. *Given a point $x \in \cup_{i=1}^{k} S_k$, define $J_x = \{j : x \in S_j\}$*

Lemma 3.4. *For all $x \in \cup_{i=1}^{k} S_k$, $x \in P_{J_x}$ and for any other non-empty subset J' of $[k]$, $x \notin P_{J'}$*

Proof. By definition, $\forall j \in J_x, x \in S_j$, so $x \in \cap_{j \in J_x} S_j$. Also, $\forall j \notin J_x, x \notin S_j$ so $x \in P_{J_x} = (\cap_{j \in J_x} S_j) \setminus (\cup_{i: i \notin J_x} S_i)$.

If J' is a non-empty subset of $[k]$ such that $J' \neq J_x$ then either $J' \setminus J_x$ or $J_x \setminus J'$ is non-empty. If $J' \setminus J_x$ is non-empty then let j' be an element of $J' \setminus J_x$. $x \notin S_{j'}$ so $x \notin \cap_{j \in J'} S_j$ and thus $x \notin P_{J'}$. Similarly, if $J_x \setminus J'$ is non-empty then let j' be an element of $J_x \setminus J'$. $x \in S_{j'}$ so $x \in \cup_{i: i \notin J'} S_{J'}$ and thus $x \notin P_{J'}$ □

Corollary 3.5. *$\cup_{i=1}^{k} S_k = \cup_{J \subseteq [k]: J \neq \emptyset} P_J$ and for any two distinct non-empty subsets J, J' of $[k]$, $P_J \cap P_{J'} = \emptyset$*

Proposition 3.6. *If I and J are non-empty subsets of $[k]$ then*

1. *If $I \subseteq J$ then $P_J \subseteq \cap_{i \in I} S_i$.*
2. *If I is not a subset of J then $P_J \cap (\cap_{i \in I} S_i) = \emptyset$.*

Proof. For the first statement, by definition, $P_J \subseteq \cap_{j \in J} S_j$. Also, since $I \subseteq J$, $\cap_{j \in J} S_j \subseteq \cap_{i \in I} S_i$ (as fewer sets are being intersected in $\cap_{i \in I} S_i$). Thus, $P_J \subseteq \cap_{j \in J} S_j \subseteq \cap_{i \in I} S_i$.

For the second statement, if I is not a subset of J then $\exists i \in I : i \notin J$. Now by definition $P_J \cap S_i = \emptyset$ so $P_J \cap (\cap_{i \in I} S_i) = \emptyset$ □

Using this, we have that

$$\sum_{I \subseteq [k]: I \neq \emptyset} (-1)^{|I|+1} |\cap_{i \in I} S_i| = \sum_{J \subseteq [k]: J \neq \emptyset} \left(\sum_{I \subseteq J: I \neq \emptyset} (-1)^{|I|+1} \right) |P_J|$$

Now observe that for all non-empty subsets J of $[k]$,

$$\sum_{I \subseteq J} (-1)^{|I|+1} = -\sum_{t=0}^{|J|} \binom{|J|}{t} (1)^{|J|-t} (-1)^t = (1 + (-1))^{|J|} = 0$$

Thus, for all non-empty subsets J of $[k]$, $\sum_{I \subseteq J: I \neq \emptyset} (-1)^{|I|+1} = \sum_{I \subseteq J} (-1)^{|I|+1} + 1 = 1$ which implies that

$$\sum_{I \subseteq [k]: I \neq \emptyset} (-1)^{|I|+1} |\cap_{i \in I} S_i| = \sum_{J \subseteq [k]: J \neq \emptyset} \left(\sum_{I \subseteq J: I \neq \emptyset} (-1)^{|I|+1} \right) |P_J| = \sum_{J \subseteq [k]: J \neq \emptyset} |P_J| = \left|\cup_{i=1}^{k} S_k\right|$$

□