數論中的組合對應

許博翔

March 12, 2021

定理 1. $\binom{2p}{p} \equiv 2(\pmod{p})^2$。

Proof. $\binom{2p}{p}$ 爲 $2p$ 顆石頭排成一列然後將 p 顆塗色的方法數。定義前變換，就是將第 i 顆石頭移到第 $i+1$ 顆石頭的位置 $\forall 1 \leq i \leq p-1$，然後將第 p 顆石頭移到第 1 顆石頭的位置；定義後變換，就是將第 i 顆石頭移到第 $i+1$ 顆石頭的位置 $\forall p+1 \leq i \leq 2p-1$，然後將第 $2p$ 顆石頭移到第 $p+1$ 顆石頭的位置。易知前或後變換之後仍然是 $\binom{2p}{p}$ 種塗色方法之一。將所有塗色方法扣掉全部塗前 p 個和全部塗後 p 個這兩個，剩下的每進行 p 次前變換會變回原本的塗色方法，且因爲 p 是質數，前變換次數又大於 1 次，所以無法透過少於 p 次的前變換變回來。於是剩下的塗色方法 p 個一循環，稱爲前 p 環，而且每個塗色方法只會恰出現在一個前 p 環中。另外，也可將這前 p 環中的每個塗色方法進行後變換，同理也是進行 p 次後變換之後會變回來，因爲每個前 p 環中的後 p 顆石頭都相同，所以要進行 p 次後變換才會回到原先的前 p 環中，因此可將所有前 p 環 p 個分成一組，也就是塗色方法 p^2 個一組。再加上原先扣掉的全部塗前 p 個和全部塗後 p 個這兩個，可知 $\binom{2p}{p} \equiv 2(\pmod{p})^2$。(以下分別爲 010110(1 表示有塗色的石頭，0 表示沒有塗色的石頭) 進行 3 次前變換變回自己與進行 3 次後變換變回自己)

$010110 \longrightarrow 001110 \longrightarrow 100110 \longrightarrow 010110$

$010110 \longrightarrow 010011 \longrightarrow 010101 \longrightarrow 010110$ ■

定理 2 (費馬小定理). $a^{p-1} \equiv 1(\pmod{p})$。

Proof. 此題等價於證明 $a^p \equiv a(\pmod{p})$，而 a^p 爲 p 顆石頭排成一列然後每顆都塗成 a 種顏色中的一種。定義一次變換，就是將第 i 顆石頭移到第 $i+1$ 顆石頭的位置 $\forall 1 \leq i \leq p-1$，然後將第 p 顆石頭移到第 1 顆石頭的位置，易知變換之

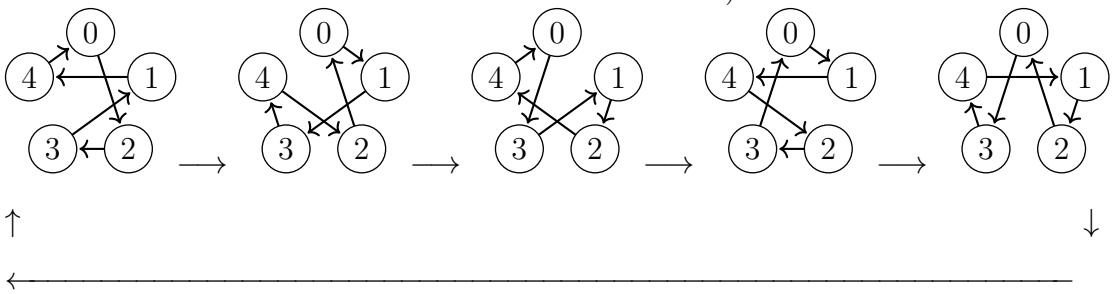
後仍然是 a^p 種塗色方法之一。將所有塗色方法扣掉全部塗同一種顏色的方法 (共 a 種)，剩下的每進行 p 次變換會變回原本的塗色方法，且因爲 p 是質數，變換次數又大於 1 次，所以無法透過少於 p 次的變換變回來。於是剩下的塗色方法 p 個一循環，而且每個塗色方法只會恰出現在一個循環中。再加上原先扣掉的 a 種塗色方法，可知 $a^p \equiv a(\pmod p)$。

$\therefore a^{p-1} \equiv 1(\pmod p)$。(以下即爲 12314 進行 5 次變換後回到自己)

$12314 \longrightarrow 41231 \longrightarrow 14123 \longrightarrow 31412 \longrightarrow 23141 \longrightarrow 12314$ ■

定理 3 (Wilson Theorem). $(p-1)! \equiv -1(\pmod p)$。

Proof. 畫一正 p 邊形，將頂點依順時針標上 $0, 1, \ldots, p-1$，$(p-1)!$ 爲從頂點 0 出發不重複地經過所有剩下的頂點再回到頂點 0 的方法數，將每一種方法的有向路徑畫出來。定義一次旋轉爲將路徑以正 p 邊形的中心順時針旋轉 $\frac{360^o}{p}$，可知一條路徑經過 p 次旋轉可轉回來，因此一條路徑可轉回來的最少次數就是 1 次或 p 次。若某條路徑一次可轉回來，則其必須滿足對於每個點都對稱，也就是每個點 i 在路徑中的下一個點 j 都必須滿足 $j-i$ 模 p 下相等，所以這種路徑數量一共 $p-1$ 個，分別爲 $j-i = 1, 2, \ldots, p-1$。剩下的路徑都是旋轉 p 次才能回來，於是剩下的路徑 p 個一循環，而且每條路徑只會恰出現在一個循環中。再加上那 $p-1$ 個一循環的路徑，可知 $(p-1)! \equiv p-1 \equiv -1(\pmod p)$。(以下即爲 $2314 \longrightarrow 1342 \longrightarrow 3124 \longrightarrow 1423 \longrightarrow 3412 \longrightarrow 2314$)



↑ ↓

←——————————————————————————————————————— ■