Notes

September 15, 2014

assignment

Section 1.4: # 17, 19, 20, 23, 24, 27.

1.4 17. Using the formula for $\varphi(n)$, compute $\varphi(27), \varphi(81)$, and $\varphi(p^\alpha)$, where p is a prime number. Give a proof that the formula for $\varphi(n)$ is valid when $n = p^\alpha$, where p is a prime number.

$$\begin{aligned}\varphi(27) &= 27(1-\frac{1}{3}) = 18\\ \varphi(81) &= 81(1-\frac{1}{3}) = 54\\ \varphi(p^\alpha) &= p^\alpha(1-\frac{1}{p}) = p^\alpha\frac{p-1}{p} = p^\alpha - p^{\alpha-1}\end{aligned}$$

The result can be obtained by observing that the integers less than p^α that are not relatively prime to p^α are

19. Find all integers $n > 1$ such that $\varphi(n) = 2$

$$\begin{aligned}\varphi(n) = n(1-\frac{1}{p1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_k})\\ p1p2p3...pk \leq n \therefore 2 = (p1-1)(p2-l)\dots(pk-1)\end{aligned}$$

20.

$$\begin{aligned}\varphi(1) &= 1\\ \varphi(p^n) &= p^n - p^{n-1} \text{ from 17}\\ \varphi(p^{n+1}) &= p^{n+1} - p^n\\ p^{n+1} &= \varphi(p^{n+1}) + p^n\end{aligned}$$

so by induction

23. Show that if $n > 1$ then the sum of all positive integers less than n and relatively prime to n is $n\varphi(n)/2$. that is $\sum\limits_{0<a<n,(a,n)=1} a = n\varphi(n)/2$

observation:$(a,n) = 1 \Leftrightarrow (n-a,n) = 1$
$\sum\limits_{0<a<n,(a,n)=1} a = \sum\limits_{0<a<n,(a,n)=1} n-a$ just summed in opposite oreder, because $0 < a < n$ $\sum\limits_{0<a<n,(a,n)=1} a = \frac{1}{2}\sum\limits_{0<a<n,(a,n)=1} a+n-a$. Now $\varphi(n)$ is defined as the number of a's such that $(a,n) = 1, 0 < a < n$.
So $\sum\limits_{0<a<n,(a,n)=1} a = \frac{1}{2}\varphi(n)n$

24.

27.

2.3 permutations

a function that maps a set S to S is a permutation if the function is one to one and onto (bijective)
$\mathrm{Sym}(S) = \{\sigma : S \to S | \sigma \text{ bijective}\}$.
special case: S is finite with n elements. $S = \{1, 2, \dots, n\}$ for simplified notation.
observations:

1.1 $\sigma, \gamma \in \mathrm{Sym}(S)$ then $\sigma \circ \gamma \in$ Sym(S).

1.2 $1_S : S \to S$, $1_S \in \mathrm{Sym}(S)$

1.3 $\sigma \in \mathrm{Sym}(S) \Rightarrow \sigma^{-1} \in \mathrm{Sym}(S)$ and $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1_S$

notation for the case $S = \{1, 2, \dots, n\}$

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Notation: $S_n = \mathrm{Sym}(S)$ while S has n elements
observe $|S_n| = n!$

$$\sigma = \begin{pmatrix} 1,2,3,4 \\ 3,4,2,1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1,2,3,4 \\ 2,1,3,1 \end{pmatrix} \sigma\tau \qquad = \begin{pmatrix} 1,2,3,4 \\ 4,3,2,1 \end{pmatrix} \sigma^{-1} = \begin{pmatrix} 1,2,3,4 \\ 4,3,1,2 \end{pmatrix}$$

cycles

let $\sigma \in S_n$. σ is called a cycle of length k if there exist $a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$ such that $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots \sigma(a_k) = a_1$ and $\sigma(x) = x$ for $x \neq \{a_1, a_2, \dots, a_k\}$

$$\sigma = \begin{pmatrix} 1,2,3,4 \\ 2,4,3,1 \end{pmatrix} = (1, 2, 4) \in S_4$$

this is a cycle of length 3
definition of disjoint cycles
observe that for $\sigma \in S_n$ be a cycle of length k then $\sigma^k = 1_S$ (identity). In fact k is the smallest positive integer that has this property.

proposition

take two disjoint cycles σ, τ. then $\sigma\tau = \tau\sigma$ (note that permutations are not in general commutative).

proof

take $x \in \{1, \dots, n\}$. if $x = a_i$ for some i. then $\sigma\tau(a_i) = a_{i+1}$ because

main theorem

every permutation m in S_n can be written as a product of disjoint cycles. moreover, the cycles of length at least two that appear are unique. note that cycles of length one are identity, multiply them all day, nothing changes.
$\sigma = (2143) = (12)(34)$