通信情報保護學會誌
第2卷 第4號, 1992. 12

암호학에서의 분할 함수에 관한 고찰

김경희* · 김영희** · 류송분*** · 오정환***

요 약

이 논문에서 우리는 여러 가지 분할 항등식을 유도했고 제한된 분할에 관한 새로운 항등식을 증명하고, 분할의 기본적인 이론과 분할함수(Partition Number Function)가 다항식 함수가 아니라는 것을 보이며, n의 분할의 수 $p(n)$에 대한 하계(Lower Bound)를 얻기 위해 Stirling의 $n!$에 대한 근사값을 소개한다. 그리고 Hardy-Ramanujan 공식, Euler 항등식과 $p(n)$의 순환식을 유도하며, 그리고 $d_m(n)$이 n을 m개의 부분으로 분할하는 분할의 수를 나타낼 때 우리는 $d_m(n)$에 관한 일반적인 공식을 $p(n)$과 함께 행렬식의 형태로 표현한다.

1. 서 론

분할(Partition)이란 단어는 수학에서 많은 뜻을 가진다. n의 분할은 합이 n이 되는 양의 정수들의 비증가 유한 수열이다.

분할론의 중요한 첫 발전은 18세기에 L. Euler에 의하여 이루어졌으며 그 후 많은 수학자들에 의해 발전되어 오고 있다. 본 논고에서는 유효한 암호 알고리듬을 개발하기 위해서는 Knapsack 암호계에 근간을 둔 분할함수의 이론을 세우는 것이다. 분할론은 수학의 한 분야로서, 응용은 암호이론, 조합론, 대수등 어디에서도 나타난다. 비모수 통계학에서는 제한된 분할(Restricted Partition)을 요구하며 확률론과 통계학에서의 여러 순열 문제들은 Simon Newcomb 문제와 관련된다. 또한, 분자물리학은 Partition Asymptotics와 분할항등식등을 이용하고 특히, 군론은 이와 밀접한 관계가 있음이 잘 알려져 있다. 분할에 많은 여러 가지 제한들이 주어질 수 있는데, 예를 들면

(a) 분할에서 부분(Part)의 수에 대한 제한

(b) 분할에서 부분의 크기에 대한 제한

(c) 분할에서 반복되는 부분의 수에 대한 제한

(d) 분할에서 일어나는 수의 유형에 대한 제한

등이 있다. (a) 부류의 제한은 분할의 부분의 수가 m 혹은 많아야 m일 수 있다. 또한, (b) 부류의 제한은 분할의 부분들의 크기가 m 이하 혹은 m 이상으로 주어질 수 있다. 우리는 제한이 주어지는 데에 따라 분할 수의 다른 수열을 얻는다. 동시에 여러가지

* 연세대학교 문리대학 수학과
** 충북대학교 자연과학대학 수학과
*** 연세대학교 이과대학 수학과

제한을 가하는 것도 가능하다.

2. 분할과 Stirling의 근사값

이 장에서는 분할에 대한 기초적 지식들과 비제한된 분할 수의 함수 $p(n)$이 다항식 함수가 아님을 알아보자.

2.1. 분 할

이 절에서 우리는 분할이 무엇인지를 설명한다. m개 부분 이하로 n을 분할하는 분할 수를 $p_m(n)$으로 표시하고 $p(0)=1$, $p_m(0)=1$이라 하자.

정의 : 분할

$$k_1+k_2+\cdots+k_s,\quad k_1\geq k_2\geq\cdots k_s,$$

의 dual은 분할

$$l_1+l_2+\cdots+l_t,\quad 1\leq i\leq t,\quad l_i=\#\{j|1\leq j\leq s,\ k_j\geq i\}$$

이다.

m이하의 크기의 부분들로 분할하는 n의 분할 수를 $q_m(n)$으로 표시하면 duality에 의하여 모든 자연수 m, n에 대해 $p_m(n)=q_m(n)$이다.

보조 정리2.1. : 두 실수 a, b가 $b>0$, $a\geq 0$이고 $m\in N$, $s=[\frac{a}{b}]$이면

$$a^{m-1}+(a-b)^{m-1}+(a-2b)^{m-1}+\cdots+(a-sb)^{m-1}>\frac{a^m}{b^m}.$$

증명 : 구간 $[a-sb,\ a]$에서 함수 $f(x)=x^{m-1}$의 성질을 이용하면 증명할 수 있다.

정의 2.2. : 모든 자연수 m, n에 대하여

$$p_m(n)\geq\frac{n^{m-1}}{(m-1)!\,m!}.$$

증명 : 보조정리 2.1과 수학적 귀납법에 의하여 증명된다.

2.2. 생성함수들(Generating Functions)과 Stirling의 근사값

이절에서는 수열 $\{p(n)\}$의 생성함수가 위로 유계이고 함수 p는 다항식 함수와 점근적이지 않다는 것을 말한다. k는 어떤 일정한 양의 정수라 하자. $|x|<1$에 대하여 등비급수 $\sum_{n=0}^{\infty}(x^k)^n$은 수렴하고 합 $\frac{1}{1-x^k}$을 갖는다. 따라서 수열 $\{q_k(n)\}$에 대한 생성함수는

$$x\longmapsto\frac{1}{(1-x)(1-x^2)\cdots(1-x^k)}=\prod_{m=1}^{k}\frac{1}{(1-x^m)}$$

이다[1]. 따라서 수열 $\{p_k(n)\}$의 생성함수도 같다. 우리는 이 함수를 P_k라 표시하자. 이제 비제한 분할 수들의 수열 $\{p(n)\}$에 대한 생성함수에 주의를 돌리자. 수열 $\{p(n)\}$에 대한 생성함수는

$$x\longmapsto\prod_{t=1}^{\infty}(1+x^t+x^{2t}+\cdots)=\prod_{t=1}^{\infty}\frac{1}{1-x^t}\qquad(2.1)$$

이다[1]. 이 함수를 P로 나타낼 때 P와 P_k의 관계는 $|x|<1$에 대하여

$$P(x)=\lim_{k\to\infty}P_k(x)$$

이다. 여기서 극한이 실제로 존재하는지에 관한 의문이 일어난다. 극한이 있다는 것을 보이는 것은 $\{P_k(x)\}$가 증가수열이므로 위로 유계임을 보이는 것과 같다. $m\in N$이고 $0<x<1$이라 가정하면 $x^m<x$이므로

$$\begin{aligned}\frac{1}{1-x^m}&=1+\frac{x^m}{1-x^m}\\&<1+\frac{x^m}{1-x}\\&<e^{\frac{x^m}{1-x}}.\end{aligned}$$

따라서,

$$P_k(x)=\prod_{m=1}^{k}\frac{1}{(1-x^k)}<\prod_{m=1}^{k}e^{\frac{x^m}{1-x}}\qquad(2.2)$$

부등식 (2. 2)는 수열 $\{P_k(x)\}$에 대한 상계를 주므로 이수열은 극한을 가진다. 그러므로 급수 $\sum_{n=0}^{\infty}p(n)x^n$은 $0<x<1$에서 수렴한다. 멱급수의 수렴구간은 0에 중심을 두므로 이 급수는 $|x|<1$에서 수렴한다.

정리 2.3. : 함수 f가 k 차 다항식 함수와 점근적이라면 모든 자연수 n에 대하여

$|f(x)|<An^k$

를 만족하는 양의 상수 A가 존재한다.

정리 2.3은 $p(n)$이 다항식 함수와 점근적이라면 다항식 함수에 의하여 지배된다는 것을 의미한다.

$p(n)$이 다항식 함수와 점근적이라고 가정하자. 그러면 모든 자연수 n에 대하여

$p(n)\leq An^k$

를 만족하는 자연수 k와 양의 상수 A가 존재한다. 정리 2.2에서 m을 $k+2$로 바꾸면 모든 자연수 n에 대하여

$$\frac{n^{k+1}}{(k+1)!\,(k+2)!}\leq p_{k+2}(n)\leq p(n)\leq An^k$$

따라서 모든 자연수 n에 대하여

$n\leq A(k+1)!\,(k+2)!$

이므로 모순이다.

정리 2.4. : 함수 p는 다항식 함수와 점근적이 아니다.

정리 2.5. : (Stirling의 $n!$에 대한 근사값)

$$n!\sim\left(\frac{n}{e}\right)^n\sqrt{2\pi n}\ .$$

증명 : 참고문헌 8. 참조.

정리 2.2와 정리 2.4에 의하여

$$p(n)\sim\frac{1}{4\sqrt{3}}\left(\frac{e^{\pi\sqrt{\frac{2}{3}}n}}{n}\right)$$

임이 증명된다. 이 공식은 G.H. Hardy와 S. Ramanujan에 의해 1918년에 출판된 논문에 있다[5].

3. 고전적 항등식과 분할함수의 공식들

여기서 우리는 분할의 몇몇 공식들과 항등식들을 기술한다. 정확히 m개 부분으로 n을 분할하는 n의 분할 수를 $d_m(n)$으로 나타내면 $d_m(n)$은 가장 큰 부분이 m인 부분들로 n을 분할하는 n의 분할 수와 같다. 한편, m개의 서로 다른 부분들로 이루어진 n의 분할 수를 $s_m(n)$으로 표시한다면

$$s_m\left(n+\frac{1}{2}m(m-1)\right)=d_m(n)$$

이다.

이 식은 다음의 대응에 의하여 보여진다 :

$(a_1+m-1,\ a_2+m-2,\ \cdots a_m)\vdash\!\!\rightarrow\ (a_1, a_2,\ \cdots, a_m)$,
$a_1\geq a_2\geq\cdots\geq a_m,\quad \Sigma a_i=n.$

정리 3.1. : $n=0, 1, 2, \cdots$에 대하여

(a) $\sum_{m=0}^{n} d_m(n)=p(n)$

(b) $p_m(n)-p_{m-1}(n)=d_m(n)$.

정리 3.2. : m이상의 수로 이루어진 부분들로 분할하는 n의 분할 수를 $r(n, m)$이라 하자.

(a) $r(n, m)=r(n, m+1)+r(n-m, m)$

(b) $r(n, m)=\sum_{i=0}^{s} p_i(n-im),\quad s=\left[\frac{n}{m}\right]$.

증명 : 참고문헌 3. 4. 참조.

정리 3.3. : 각 부분들이 N이하이고 기껏해야 M개의 부분들로 이루어진 n의 분할 수를 $p(N, M, n)$이라 하자. 그러면 모든 $N, M, n\geq 0$에 대하여

(a) $p(N, M, n)=p(M, N, n)$

(b) $p(N, M, n)=p(N, M, NM-n)$

(c) $0\leq n\leq\frac{NM}{2}$에 대하여

$p(N, M, n)-p(N, M, n-1)\geq 0.$

증명 : 참고문헌 7. 참조.

정리 3.4. : (Erdös-Lehner)

$n\to\infty$일 때 $m=o\left(n^{\frac{1}{3}}\right)$이라면

$$d_m(n)\sim\frac{1}{m!}\binom{m-1}{n-1}.$$

증명 : 참고문헌 2. 참조.

정리 3.5. : (The Pentagonal Number Theorem)

$$\prod_{m=1}^{\infty}(1-x^m)=\sum_{\lambda=-\infty}^{\infty}(-1)^{\lambda}x^{\lambda(3\lambda-1)/2}$$
$$=\sum_{\lambda=0}^{\infty}(-1)^{\lambda}x^{\lambda(3\lambda\pm 1)/2}$$

증명 : 참고문헌 6. 참조.

따름정리 3.6. : (Euler의 항등식)

n≥0이면

$$p(n)-p(n-1)-p(n-2)+p(n-5)+p(n-1)+\cdots+(-1)^{\lambda}p(n-\frac{1}{2}\lambda(3\lambda-1))+(-1)^{\lambda}p(n-\frac{1}{2}\lambda(3\lambda+1))+\cdots=0$$

MacMahon은 따름정리 3.6을 이용하여 $n=200$까지 $p(n)$을 계산했고 $p(200)=3972999029388$임을 밝혔다.

4. 새로운 분할공식들과 항등식

$p(n)$에 대하여 순환 공식이 있다. 우리는 4.1절에서 행렬식으로 이 공식을 표현하고, $d_m(n)$의 순환공식도 행렬식에 의하여 얻는다. 4.2절에서는 $p_m(n)$의 공식을 얻는 방법을 소개한다.

4.1. $p(n)$과 $d_m(n)$의 표현

정리 3.5와 (2.1)식을 이용하면 다음의 식을 얻을 수 있다 :

$$t(n)=\begin{cases}(-1)^{\lambda}, & n=\dfrac{3\lambda^2\pm\lambda}{2}\text{ 일 때,}\\ 0, & n\neq\dfrac{3\lambda^2\pm\lambda}{2}\text{ 일 때,}\end{cases}$$

이면

$$\prod_{n=0}^{\infty}t(n)x^n\prod_{n=0}^{\infty}p(n)x^n=1\ . \tag{4.1}$$

(4.1)식의 양쪽 계수를 비교하면

$$\begin{aligned}&p(0)=1,\\ &t(1)+p(1)=0,\\ &t(2)+t(1)p(1)+p(2)=0,\\ &\quad\vdots\\ &t(n-1)+t(n-2)p(1)+\cdots+t(1)p(n-2)+p(n-1)=0,\\ &t(n)+t(n-1)p(1)+\cdots\cdots+t(1)p(n-1)+p(n)=0.\end{aligned}$$

행렬 형식으로 나타내면

$$\begin{pmatrix}1&&&&&&\\ t(1)&1&&&&&\\ t(2)&t(1)&1&&&&\\ \vdots&\vdots&\vdots&\ddots&&&\\ t(n-1)&t(n-2)&t(n-3)&\cdots&t(1)&1&\\ t(n)&t(n-1)&t(n-2)&\cdots&t(2)&t(1)&1\end{pmatrix}\begin{pmatrix}p(0)\\ p(1)\\ p(2)\\ \vdots\\ p(n-1)\\ p(n)\end{pmatrix}=\begin{pmatrix}1\\ 0\\ 0\\ \vdots\\ 0\\ 0\end{pmatrix}.$$

p(n)은 역행렬의 (n+1, 1)원이다. 따라서

$$p(n)=(-1)^n\begin{vmatrix}t(1)&1&&&&\\ t(2)&t(1)&1&&&\\ \vdots&\vdots&\vdots&\ddots&&\\ t(n-1)&t(n-2)&t(n-3)&\cdots&t(1)&1\\ t(n)&t(n-1)&t(n-2)&\cdots&t(2)&t(1)\end{vmatrix}. \tag{4.2}$$

이 행렬식을 n번째 행으로 전개한다면

$$p(n)=\sum_{p_1+2p_2+\cdots+np_n}(-1)^{p_1+p_2+\cdots+p_n}\frac{(p_1+p_2+\cdots+p_n)!}{p_1!p_2!\cdots p_n!}\,t(1)^{p_1}t(2)^{p_2}\cdots t(n)^{p_n}$$

이 공식은 다음 정리로 이끌어진다.

정리 4.1. : Euler 항등식의 계수들로 이루어진 부분들

$$\overbrace{1,\cdots,1}^{p_1},\ \overbrace{2,\cdots,2}^{p_2},\ \cdots,\ \overbrace{n,\cdots,n}^{p_n}$$

에 의하여 만들어진 $\frac{(p_1+p_2+\cdots+p_n)!}{p_1!p_2!\cdots p_n!}$ 개의 각 분할에 주어진 부호 $(-1)^{p_1+p_2+\cdots+p_n}t(1)^{p_1}t(2)^{p_2}\cdots t(n)^{p_n}$의 대수합은 n의 분할 수와 같다. 만일 우리가 1열로 행렬식 (4.2)를 전개한다면 $p(n)$의 순환식(따름정리 3.6)을 얻는다. 또한, 항등식

$$\prod_{k=1}^{m}\frac{1}{1-x^k}=\sum_{n=0}^{\infty}p_m(n)x^n=\sum_{n=0}^{\infty}d_m(n+m)x^n \quad [1]$$

을 택한다면 항등식

$$(1-x)(1-x^2)\cdots(1-x^m)\sum_{n=0}^{\infty}d_m(n+m)x^n=1 \qquad (4.3)$$

를 얻는다. 따라서,

$a_k(m)$으로 $\sum_{\substack{p_1+2p_2+\cdots+mp_m=k\\ 0\le p_1,\,p_2,\,\cdots,\,p_m\le 1}}(-1)^{p_1+p_2+\cdots+p_m}$를 나타내면 (4.3)식은

$$\left(1+\sum_{k=1}^{\frac{m(m+1)}{2}}\alpha_k(m)x^k\right)\sum_{n=0}^{\infty}d_m(n+m)x^n=1$$

로 표현된다. 양변의 x의 계수들을 비교하면

$$d_m(n+m)+d_m(n+m-1)\alpha_1(m)+d_m(n+m-2)\alpha_2(m)+\cdots+d_m\left(n+m-\frac{m(m+1)}{2}\right)\alpha_{\frac{m(m+1)}{2}}(m)=0$$

이 된다. $n=0,1,2,\cdots$일때

$$\begin{aligned}
&d_m(m)=1\\
&d_m(m+1)+d_m(m)\alpha_1(m)=0\\
&d_m(m+2)+d_m(m+1)\alpha_1(m)+d_m(m)\alpha_2(m)=0\\
&\quad\vdots\\
&d_m\left(m+\frac{m(m+1)}{2}\right)+d_m\left(m+\frac{m(m+1)}{2}-1\right)\alpha_1(m)+\cdots+d_m(m)\,\alpha_{\frac{m(m+1)}{2}}(m)=0
\end{aligned}$$

을 얻는다. 행렬 형식으로 표현하고 $d_m(n)$을 행렬식으로 표현하면

$$d_m(n)=(-1)^{n-m}\begin{vmatrix}
\alpha_1(m) & 1 & & & & & & \\
\alpha_2(m) & \alpha_1(m) & 1 & & & & & \\
\cdot & & \cdot & & & & & \\
\cdot & & & \cdot & & & & \\
\cdot & & & & \cdot & & & \\
\alpha_{\frac{m(m+1)}{2}} & \cdots & & \alpha_1(m) & 1 & & & \\
0 & & & & \cdot & & & \\
\cdot & & & & & \cdot & & \\
\cdot & & & & & & \cdot & \\
0 & \cdots & \cdots & \cdots & \cdots & \alpha_1(m) & 1 & \\
0 & \cdots & 0 & \alpha_{\frac{m(m+1)}{2}} & \cdots & \cdots & \alpha_1(m) &
\end{vmatrix} \qquad (4.4)$$

$$\left(n-m>\frac{m(m+1)}{2}\right).$$

로 된다. (4.4)의 행렬식을 $\Delta(n-m)$으로 표시하고 1열을 택하여 전개하면

$$d_m(n) = (-1)^{n-m}\{\alpha_1(m)\Delta(n-m-1) - \alpha_2(m)\Delta(n-m-2)+\alpha_3(m)\Delta(n-m-3)+\cdots + (-1)^{\frac{m(m+1)}{2}-1}\alpha_{\frac{m(m+1)}{2}}(m) \times \Delta\left(n-m-\frac{m(m+1)}{2}\right)\}$$
$$= -\alpha_1(m)d_m(n-1) - \alpha_2(m)d_m(n-2)-\cdots -\alpha_{\frac{m(m+1)}{2}}(m)\, d_m\left(n-\frac{m(m+1)}{2}\right)$$

을 얻는다.

4.2. $p_m(n)$에 대하여

이 절에서는 $p_m(n)$의 상계와 $p_m(n)$의 공식을 유도하자. 모든 n에 대하여 $1\le m\le n$이면

$$\binom{n-1}{m-1} \le m!\,p_m(n) \le \binom{n+\frac{m(m+1)}{2}-1}{m-1}.$$

따라서,

$$p_m(n) \le \frac{n^{m-1}}{m!\,(m-1)!}\left(1+\frac{m^2}{2n}\right)^{m-1} \le \frac{n^m}{(m!)^2}\left(1+\frac{m^2}{2n}\right)^m$$

을 이끌어 낼 수 있다. Stirling의 공식 [8]에 의하여

$$p_m(n) \le \exp\{m^3/2n + m(\log n + 2 - 2\log m)\}$$

를 얻는다. 따라서 $\alpha \ge 0$이고 $m \le \alpha\sqrt{n}$이면

$$p_m(n) \le \exp\left(\frac{\alpha^3}{2} + 2\alpha(1-\log\alpha)\right)\sqrt{n}$$

이므로 $p_m(n)$의 상계를 찾게 된다.
이제 $p_m(n)$의 공식을 만들어 보자.
$m = 1, 2, 3, \cdots$, $n = 0, 1, 2, \cdots$에 대하여

$$\begin{cases} A(m, n) = 1 & (m \mid n\text{일때}) \\ A(m, n) = 0 & (m \nmid n\text{일때}) \end{cases},$$

특히, $A(m, 0) = 1$로 나타내자.

$n = mq + r$ $(0 \le r < m)$일때

$$p_m(n) = p_m(mq+r) = \sum_{\nu=0}^{m-1} a(\nu, r)q^\nu = F(mq+r, q) \quad (0\le r<m)$$

라 하면

$p_m(mq) = F(mq, q)$, $p_m(mq+1) = F(mq+1, q), \cdots,$
$p_m(mq+m-1) = F(mq+m-1, q)$

이므로 $A(m, n)$의 정의에 의하여

$$p_m(n) = F(mq, \frac{n}{m})A(m, n) + F(mq+1, \frac{n-1}{m})A(m, n+m-1) + \cdots + F(mq+m-1, \frac{n-m+1}{m})A(m, n+1) \tag{4.5}$$

이고

$$\sum_{\nu=0}^{m-1} A(m, n+\nu) = 1\ . \tag{4.6}$$

(4.5)식을 이용하여 $p_2(n)$과 $p_3(n)$의 공식을 찾아보자. $u = 0, 1, 2, \cdots$에 대하여 $p_2(2u) = u+1$, $p_2(2u+1) = u+1$임을 쉽게 알 수 있다. 따라서

$$p_2(n) = \frac{1}{2}(n+1+A(2, n))\ . \tag{4.7}$$

$m = 3$에 대하여 $n = 3u$, $3u+1$, $3u+2$로 나타내면

$$\begin{cases} p_3(3u) = \sum_{\nu=0}^{u} p_2(3\nu), \\ p_3(3u+1) = \sum_{\nu=0}^{u} p_2(3\nu+1), \\ p_3(3u+2) = \sum_{\nu=0}^{u} p_2(3\nu+2), \end{cases}$$

$u = 0, 1, 2, \cdots$이다. $A(2, 3u) = A(2, u)$,
$A(2, 3u+1) = A(2, u+1)$이므로 (4.7)식에 의하여

$$\begin{cases} p_3(3u) = \frac{1}{2}\sum_{\nu=0}^{u}(3\nu+1+A(2, \nu)), \\ p_3(3u+1) = \frac{1}{2}\sum_{\nu=0}^{u}(3\nu+1+1+A(2, \nu+1)), \\ p_3(3u+2) = \frac{1}{2}\sum_{\nu=0}^{u}(3\nu+2+1+A(2, \nu)) \end{cases} \tag{4.8}$$

를 얻게 된다.

$$\sum_{\nu=0}^{u} A(2,\nu) = \frac{1}{2}\{(u+2)A(2,u) + (u+1)A(2,u+1)\}$$

$$\sum_{\nu=0}^{u} A(2,\nu+1) = \frac{1}{2}\{(u+1)A(2,u+1) + uA(2,u)\}$$

이므로 (4.7), (4.8)식에 의하여

$$\begin{cases} p_3(3u) &= \frac{1}{4}(3u^2+6u+3+A(2,u)), \\ p_3(3u+1) &= \frac{1}{4}(3u^2+8u+4+A(2,u+1)), \\ p_3(3u) &= \frac{1}{4}(3u^2+10u+7+A(2,u)). \end{cases} \quad (4.9)$$

이제 (4.9)식의 세개의 방정식에 있는 $3u$, $3u+1$, $3u+2$를 n으로 바꾸면

$$\begin{cases} p_3(3u)=p_3(n) = \frac{1}{12}(n^2+6n+9+3A(2,n)), \\ p_3(3u+1)=p_3(n) = \frac{1}{12}(n^2+6n+5+3A(2,n)), \\ p_3(3u+2)=p_3(n) = \frac{1}{12}(n^2+6n+5+3A(2,n)) \end{cases}$$

가 되므로 $n=0, 1, 2, \cdots$에 대하여

$$p_3(n) = \frac{1}{12}\{(n^2+6n+9+3A(2,n))\ A(3,n) + (n^2+6n+5+3A(2,n))\ A(3,n+2) + (n^2+6n+5+3A(2,n))\ A(3,n+1)\}.$$

따라서, $n=0, 1, 2, \cdots$에 대하여 $A(2,n) = \frac{1}{2}(1+(-1)^n)$이므로

$$p_3(n) = \frac{1}{24}\{2n^2+12n+13+3(-1)^n+8A(3,n)\}.$$

이와같은 방법으로 $n=0, 1, 2, \cdots$에 대하여 $p_4(n)$, $p_5(n)$, …의 공식들을 얻을 수 있다.

참 고 문 헌

1. H.L. Alder, Partition identities-from Euler to the present, amer. Math. Monthly76(1969), pp.733-746.

2. P. Erdös and J. Lehner, The distribution of number of summands in the partitions of positive integer, Duke. Math. J 8(1941), pp.335-345.

3. H. Gupta, Table of partitions, Indian Math. Soc(1939), Madras.

4. H. Gupta, C.E. Gwyther and J.C.P. Miller, Table of partitions, cambridge Univ. Press(1962).

5. G.H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, Proc. London Math. Soc.(2) (1918), pp.75-115.

6. H. Rademacher, On the partition function p(n), Proc. London Math. Soc.(2) 43(1937), pp.241-254.

7. I.J. Schur, Vorlesungen über Invariantentheorie satz 2.22, Grundlehren der Mathematicschen Wissenschaften Vol.143, pp.76.

8. J. Stirling, Methodus differentialis : sive tractatus de summantione et interpolatione, 1730.

□ 著者紹介

오 정 환(정회원)

연세대학교 이과대학 수학과(학사)
연세대학교 수학과(석사)
연세대학교 수학과(박사)
미국 팬실바니아 주립대학 객원교수
미국 일리노이 대학교 객원교수
현재 : 연세대학교 이과대학 수학과 교수

김 경 희

연세대학교 이과대학 수학과(학사)
미국 신시내티 대학교 수학과(Ph.D)
현재 : 연세대학교 문리대학 수학과 조교수

류 송 분

연세대학교 이과대학 수학과(학사)
연세대학교 수학과(석사)
연세대학교 수학과(박사)
현재 : 연세대학교 강사

김 영 희

연세대학교 이과대학 수학과(학사)
연세대학교 수학과(석사)
연세대학교 수학과(박사)
미국 웨스트 버지니아 대학교 객원교수
현재 : 충북대학교 수학과 부교수