曲阜师范大学

研究生学位論文

论文题目：几个基础数数论的问题研究

研究生姓名 方玉光

专　　业 数论

攻读学位级别 硕士

指导教师姓名 邵品琮

1987 年 5 月　　日

目录

第一类指数方幂和的同余问题

1985.9.15.

一 引言

设 $S_r(p^\alpha,d)$ 表示在 modp^α 的完全剩余系中具有指数 d 的元素之 r 次方幂和，其中 p 为奇素数，r,d,α 为正整数. C.F. Gauss 在其名著[3]中证明了 $S_1(p,p-1)\equiv\mu(p-1)\ (\mathrm{mod}\,p)$. 随后，这个问题引起了许多数学家的兴趣. 1830年，M.A. Stern[4] 证明了 $S_1(p,d)\equiv\mu(d)\ (\mathrm{mod}\,p)$；1883年，A.R. Forsyth[5] 讨论了 $S_r(p,p-1)$ 的同余情况，但其结果及其证明都很复杂；1952年，R.Moller[2] 证明了 $S_r(p,d)\equiv\frac{\varphi(d)}{\varphi(d_1)}\mu(d_1)\ (\mathrm{mod}\,p)$，其中 $d_1=\frac{d}{(r,d)}$，但其证明比较复杂. H. Gupta[1] 利用原根的知识对 R.Moller 的结果给出了一个简单的证明。本文目的就是把上述结果推广到了模为 p^α $(\alpha\geq1)$

的一般情况，即证明了

定理一. $S_r(p^\alpha, d) \equiv \frac{\varphi(d)}{\varphi(l_0)}\mu(l_0) \pmod{p^\alpha}$

其中 $\alpha>0$，p为奇素数，$d/(d,r) = p^m l_0$，$p\nmid l_0$，$m\geq 0$.

设 $h(d)=\frac{d}{(r,d)}$，$p(d)=\mathrm{pot}_p(h(d))$ 表示 $h(d)$中 p 因子的最高次幂. 对于 $x\mid\varphi(p^\alpha)$，定义

$$F(x,r)=\sum_{d\mid x}\frac{\varphi(d)}{\varphi(h(d)p^{-p(d)})}\mu(h(d)p^{-p(d)})$$

我们有（以下"≡"皆表示 $\mathrm{mod}\,p^\alpha$ 同余号）

定理二.

$$F(x,r)\equiv\begin{cases} x & \text{当 } p^{-\mathrm{pot}_p(x)}x\mid r \text{ 时}\\ 0 & \text{否则}\end{cases}$$

二. 引理

为得到定理的证明，需要下述引理：

引理1 存在 $\mathrm{mod}\,p^\alpha$ 的一个原根 g，使得

$$g^{p^l(p-1)}\equiv 1+\mu g^{l+1} \pmod{p^{l+2}} \quad (l\geq 0,\ p\nmid\mu).$$

证明　设 g 为 $\bmod p$ 的一个原根，不妨设 $g^{p-1}\equiv 1+up \pmod{p^2}$ $(p\nmid u)$（否则取 $g+p$ 代 g）. 对于此 g，它必为 $\bmod p^{\alpha}$ 之原根. 下面对于 l 用数学归纳法. 当 $l=0$ 时，由 g 的选取可知引理成立；假设当 $l-1$ 时引理成立. 设

$$g^{p^{l-1}(p-1)}=1+up^{l} \quad (p\nmid u).$$

两边 p 次方可得.

$$g^{p^{l}(p-1)}=1+up^{l+1}+\binom{p}{2}(up^{l})^{2}+\cdots\equiv 1+up^{l+1}\pmod{p^{l+2}}$$

于是可知引理成立.

引理2.[1] 设 $f(n)$ 为一个数论函数，则

$$S'(n)=\sum_{j<'n}f(j)=\sum_{d|n}\mu(d)\{f(d)+f(2d)+\cdots+f(n)\}$$

其中 $j<'n$ 表示 $j<n$，且 $(j,n)=1$.

引理3[1]　$\mathrm{Pot}_p\left(\binom{p^c}{r}\right)=c-\mathrm{pot}_p(r)$　$(0\le r\le p^c)$.

引理4[6] 给定 r,d,k 三个正整数，满足 $d|k$，$d>0$，$k\geq 1$ 和 $(r,d)=1$，$S=\{r+td,\ t=1,2,\cdots k/d\}$

则S中与K互素的元素的个数为 $\varphi(k)/\varphi(d)$.

三. 定理的证明

对定理一的证明：

取引理1中的原根，令 $t=g^{\varphi(p^\alpha)/d}$，于是 $t^r\equiv g^{r_1\varphi(p^\alpha)/d_1}\ (\mathrm{mod}\,p^\alpha)\equiv a\ (\mathrm{mod}\,p^\alpha)$，其中 $r_1=\frac{r}{(r,d)}$. $d_1=\frac{d}{(r,d)}$，$a=g^{\varphi(p^\alpha)r_1/d_1}$. 于是 t^r 与 a 的指数皆为 d_1，令 $T=\{t^{\lambda r}: \lambda<'d\}$. 此中关于 $\mathrm{mod}\,p^\alpha$ 互不同余的~~元素~~的元素记为 $K=\{t^{rj}: j<'d_1\}$，K中每一个元素在T中关于 $\mathrm{mod}\,p^\alpha$ 同余的意义会出现重复，任取K中一个元素 t^{rj}，它重复的次数为下面集合元素的个数：$\{t^{r\lambda}: t^{r\lambda}\equiv t^{rj}\ (\mathrm{mod}\,p^\alpha)$ 且 $\lambda<'d\}$，由于 t^r 的指数为 d_1，故上集的个数即等于下集的个数：$\{\lambda: \lambda\equiv j\ (\mathrm{mod}\,d_1)\}$（其中 $\lambda<'d$）. 由引理4可知，它的个数等于 $\varphi(d)/\varphi(d_1)$，这样

K中每一个元素关于 mod p^α 同余的意义下重复 $\varphi(d)/\varphi(d_1)$. 记 $K_a=\{a^k : k<' d_1\}$, 于是

$$Sr(p^\alpha,d)\equiv\sum_{b\in T} b\equiv\frac{\varphi(d)}{\varphi(d_1)}\sum_{b\in K_a} b \qquad (1)$$

利用引理2，有

$$\sum_{b\in K_a} b=\sum_{h|d_1}\mu(h)\{a^h+a^{2h}+\cdots+a^{d_1}\}$$
$$\equiv\sum_{h|d_1}\mu(h)\frac{a^{d_1}-1}{a^h-1}a^h \qquad (2)$$

令 $d_1=p^{r_0}l_0$, 其中 $l_0|p-1$, $\ell(n)=\begin{cases}0 & n=0\\ 1 & n>0\end{cases}$

则
$$\sum_{b\in K_a} b=\sum_{h|p^{r_0}l_0}\mu(h)\frac{a^{d_1}-1}{a^h-1}a^h=\sum_{\substack{0\le k\le r_0\\ l|l_0}}\mu(p^k l)\frac{a^{d_1}-1}{a^{p^k l}-1}a^{p^k l}$$
$$=\sum_{l|l_0}\mu(l)\frac{a^{d_1}-1}{a^l-1}a^l+\ell(r_0)\sum_{l|l_0}\mu(pl)\frac{a^{d_1}-1}{a^{pl}-1}a^{pl}$$
$$=\sum_{l|l_0}\mu(l)\frac{a^{d_1}-1}{a^l-1}a^l-\ell(r_0)\sum_{l|l_0}\mu(l)\frac{a^{d_1}-1}{a^{pl}-1}a^{pl} \qquad (3)$$

对于 l，当 $(a^l-1,p^\alpha)\neq1$ 时，则必有 $a^l\equiv1\ (\mathrm{mod}\ p)$，即 $g^{\varphi(p^\alpha)l r_1/d_1}\equiv1\ (\mathrm{mod}\ p)$，由于 g 为 mod p 的原根，故 $p-1\,\Big|\,\frac{\varphi(p^\alpha)}{d_1}r_1 l=p^{\alpha-1-r_0}r_1(p-1)l/l_0$.

又 $l_0|d_1$, $(d_1,r_1)=1$, 及 $(l_0,p)=1$, 故必有 $l_0|l$.

因此当 $0<l<l_0$ 时，必有 $(a^l-1,\ p^\alpha)=1$，进而有 $\frac{a^{d_1}-1}{a^l-1}\equiv 0 \pmod{p^\alpha}$；

同理可证明当 $0<l<l_0$ 时，$\frac{a^{d_1}-1}{a^{pl}-1}\equiv 0 \pmod{p^\alpha}$.

于是(3)变为

$$\sum_{b\in K_a} b \equiv \mu(l_0)\frac{a^{d_1}-1}{a^{l_0}-1}a^{l_0} - l(r_0)\mu(l_0)\frac{a^{d_1}-1}{a^{pl_0}-1}a^{pl_0} \pmod{p^\alpha} \quad (4)$$

由引理3可得：当 $\beta\geqslant\alpha-r$，$1\leqslant r<\alpha$，及 $2\leqslant k\leqslant p^r$ 时，必有 $\operatorname{pot}_p\left(\binom{p^r}{k}p^{k\beta}\right)\geqslant\alpha+\beta$. (5)

事实上，上式右边为：

$$\operatorname{pot}_p\binom{p^r}{k} + \operatorname{pot}_p(p^{k\beta}) = r-\operatorname{pot}_p(k)+k\beta$$

故只要证明 $r-\operatorname{pot}_p(k)+(k-1)\beta\geqslant\alpha$，又 $\beta\geqslant\alpha-r$，故只要证明 $r-\operatorname{pot}_p(k)+(k-1)(\alpha-r)\geqslant\alpha$，或证

$$(k-2)(\alpha-r)\geqslant\operatorname{pot}_p(k).$$

当 $k=2$ 时，此式两边皆为 0，显然成立；当 $k>2$ 时，只证 $k-2\geqslant\operatorname{pot}_p(k)$，即 $k\geqslant\operatorname{pot}_p(k)+2$，这是显然的结果，故(5)式成立。

再由引理1：存在 u，$p\nmid u$，使得：

$$a^{l_0}=\left(g^{\varphi(p^\alpha)r_1/d_1}\right)^{l_0}=g^{p^{\alpha-r_0-1}(p-1)r_1}=1+up^\beta \qquad (6)$$

其中 $\beta\geqslant\alpha-r_0$，于是

$$\frac{a^{d_1}-1}{a^{l_0}-1}=\frac{(a^{l_0})^{p^{r_0}}-1}{a^{l_0}-1}=\frac{(1+up^\beta)^{p^{r_0}}-1}{up^\beta}=p^{r_0}+$$

$$+l(r_0)\frac{1}{p^\beta}\sum_{k\geqslant 2}\binom{p^{r_0}}{k}u^{k-1}p^{k\beta}\equiv p^{r_0}\ (\mathrm{mod}\,p^\alpha).$$

结合(6)知：$$\frac{a^{d_1-1}}{a^{l_0}-1}a^{l_0}\equiv p^{r_0}\ (\mathrm{mod}\,p^\alpha) \qquad (7)$$

同样的讨论可得：

$$\frac{a^{d_1}-1}{a^{pl_0}-1}a^{pl_0}\equiv p^{r_0-1}\ (\mathrm{mod}\,p^\alpha)\quad(\text{若 } r_0\geqslant 1) \qquad (8)$$

将(7)和(8)代入(4)可得

$$\sum_{b\in K_a}b\equiv u(l_0)p^{r_0}-l(r_0)u(l_0)p^{r_0-1}\ (\mathrm{mod}\,p^\alpha)$$

$$\equiv u(l_0)(p^{r_0}-l(r_0)p^{r_0-1})\ (\mathrm{mod}\,p^\alpha)\equiv u(l_0)\varphi(p^{r_0})$$

代入(1)．

$$S'_r(p^\alpha,d)\equiv\frac{\varphi(d)}{\varphi(d_1)}u(l_0)\varphi(p^{r_0})\ (\mathrm{mod}\,p^\alpha)$$

$$\equiv\frac{\varphi(d)}{\varphi(l_0)}u(l_0)\ (\mathrm{mod}\,p^\alpha).$$

当 $\alpha=1$ 时，由于 $d\mid p-1$，$r_0=0$，故 $l_0=\frac{d}{(r,d)}=d_1$，

此时 $S_r(p^\alpha, d) = S_r(p, d) \equiv \frac{\varphi(d)}{\varphi(d_1)}\mu(d_1) \pmod p$.

这就是 R. Moller 的结果.　　定理一证毕

定理二的证明

注意到 $h(d)$ ~~$p(d)$~~ 为积性(multiplicative), 即可知: $\varphi(d)\mu(h(d)p^{-\rho(d)})/\varphi(h(d)p^{-\rho(d)})$ 为一积性函数, 进而推得: $F(x, r)$ 为 x 的积性函数.

设 q 为一个素数, 当 $(q, p) = 1$ 时,

$$F(q^{\alpha_1}, r) = \sum_{d \mid q^{\alpha_1}} \frac{\varphi(d)}{\varphi(h(d))}\mu(h(d)) = \sum_{k=0}^{\alpha_1} \varphi(q^k)\mu\left(\frac{q^k}{(q^k, r)}\right) \Big/ \varphi\left(\frac{q^k}{(q^k, r)}\right)$$

当 $(q^{\alpha_1}, r) = q^\beta$, $0 < \beta < \alpha_1$ 时, 有

$$F(q^{\alpha_1}, r) = \sum_{i=0}^{\beta} \frac{\varphi(q^i)}{\varphi(1)}\mu(1) + \frac{\varphi(q^{\beta+1})}{\varphi(q)}\mu(q)$$

$$= \sum_{i=0}^{\beta} \varphi(q^i) - \frac{\varphi(q^{\beta+1})}{\varphi(q)} = q^\beta - q^\beta = 0.$$

当 $(q^{\alpha_1}, r) = q^{\alpha_1}$ 时, $F(q^{\alpha_1}, r) = \sum_{d \mid q^{\alpha_1}} \varphi(d_1) = q^{\alpha_1}$,

当 $q = p$ 时,

$$F(p^\beta, r) = \sum_{d \mid p^\beta} \frac{\varphi(d)}{\varphi(h(d)p^{-\rho(d)})}\mu(h(d)p^{-\rho(d)})$$

$$= \sum_{d \mid p^\beta} \varphi(d) = p^\beta.$$

设 $x=p^{\beta}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 为 x 的典型分解式，则

$$F(x,r)=F(p^{\beta},r)F(p^{\alpha_1},r)\cdots\cdots F(p_k^{\alpha_k},r)$$

$$=\begin{cases} p^{\beta}p_1^{\alpha_1}\cdots p_k^{\alpha_k}=x & \text{当 } p\text{-}pot_p(x)\,x\mid r \text{ 时} \\ 0 & \text{当 } p\text{-}pot_p(x)\,x\nmid r \text{ 时.} \end{cases}$$

定理二证毕.

对于偶素数 $p=2$ 的情况，我们也获得了一个较简单的结果

$$S_r(2^{\alpha},2^{n_0})\equiv(-1)^r\Delta(n_0)+[1+(-1)^r]\varphi(2^{n_0})\pmod{2^{\alpha}}.$$

其中 $\alpha\geqslant3$, $0\leq n_0\leq n-2$, $\Delta(n_0)=\left[\frac{1}{n_0}\right]=\begin{cases}1 & n=1\\ 0 & n>1\end{cases}$

$$S_r(2,1)\equiv1\pmod{2}.\qquad S_r(4,2)\equiv(-1)^r\pmod{4}.$$

这个结果将另文讨论.

在本文的写作过程中，我的指导老师邵品琮教授一直给予热情的指导，在此我表示深深的感谢。

参考文献

[1] H. Gupta, Selected Topics in Number Theory, ABACUS Press, 1980. PP. 55-57

[2] R. MoLLer, Sums of Powers of Numbers Having a Given Exponent ModuLo a Prime. Amer. Math. Monthly 59 (1952).

[3] Gauss. C.F. Disquisitions Arithmeticae, Arts. 80-81.

[4] Stern. M.A. Bemerkungen über hohere Arithmetik. Journal für Mathematik. Vol. VI (1830) PP. 147-153.

[5] Forsyth. A.R. Primitive Roots of Primes and Their Residues, Messenger of Mathematics. Vol. XIII (1883-4) PP. 180-185.

[6] Apostal. T. An Introduction to Analytic Number Theory, Springer-Verlag, 1976, PP. 124.

On Sums of Powers of Numbers Having a Given Exponent Modulo a Power of a Prime

FANG Yuguang

§1. Introduction

Let $S_r(p^\alpha, d)$ denote the sum of r-powers of numbers having given order (or exponent) d modulo a p^α, where p is odd prime, r, d, α are positive integers and $d \mid \varphi(p^\alpha)$. C.F. Gauss have proved in his masterpiece [3] that $S_1(p, p-1) \equiv \mu(p-1) \pmod{p}$. Afterward, this problem was considered by many mathematician. In 1830, M.A. Stern[4] proved that $S_1(p, d) \equiv \mu(d) \pmod{p}$, where $d \mid \varphi(p)$. In 1883, A.R. Forsyth[5] discussed the congruence of $S_r(p, p-1)$, but his results and proofs are too complicated ; In 1952, R. Moller[2] proved $S_r(p, d) \equiv \frac{\varphi(d)}{\varphi(d_1)} \mu(d_1) \pmod{p}$, where $d_1 = \frac{d}{(r,d)}$, but his method is not helpful for generalization. H. Gupta[1] have a simple proof given for R. Moller's result by means of primitive roots.

In this paper, we shall give a generalization on above result to the case that modulo is a power of prime p^α $(\alpha \geq 1)$, that is, we have proved the following

Theorem 1. $S_r(p^\alpha, d) \equiv \frac{\varphi(d)}{\varphi(l_0)} \mu(l_0) \pmod{p^\alpha}$

where $\alpha > 0$, p is odd prime and $d/(r,d) = p^m l_0$, $p \nmid l_0$, $m \geq 0$.

Let $h(d) = \frac{d}{(r,d)}$ · $p(d) = \mathrm{pot}_p(h(d))$, the highest power of p in $h(d)$. For $x \mid \varphi(p^\alpha)$, define

$$F(x,r) = \sum_{d \mid x} \frac{\varphi(d)}{\varphi(h(d)p^{-p(d)})} \mu(h(d)p^{-p(d)})$$

We have (From then on, $\equiv$ denote the congruence modulo p^α)

Theorem 2

$$F(x,r) \equiv \begin{cases} x & \text{If } p^{-\mathrm{pot}_p(x)} x \mid r \\ 0 & \text{otherwise} \end{cases}$$

§2 Lemmas

To obtain the proofs of theorem 1 and 2, we need

Lemma 1 There exsits a primitive root g mod p^α such that $g^{p^l(p-1)} \equiv 1 + \mu g^{l+1} \pmod{p^{l+2}}$ where $l \geqslant 0$, $p \nmid \mu$.

Proof Suppose g is a primitive root mod p. without lasing generality, assume $g^{p-1} \equiv 1 + \mu p \pmod{p^2}$, where $p \nmid \mu$. It is well known that g is a primitive root mod p^α. When $l = 0$, from the choice of g, we know the lemma 1 is true. Suppose Lemma 1 is true for $l-1$, that is,

$$g^{p^{l-1}(p-1)} \equiv 1 + \mu p^l \quad (p \nmid \mu)$$

then $g^{p^l(p-1)} = (1 + \mu p^l)^p = 1 + \mu p^{l+1} + \binom{p}{2}(\mu p^l)^2 + \cdots$

$$\equiv 1 + \mu p^{l+1} \pmod{p^{l+2}}.$$

By induction, we complete the proof.

Lemma 2 [1] Let $f(n)$ denote an arithmetical function, then

$$S'(n) \triangleq \sum_{j<'n} f(j) = \sum_{d|n} \mu(d)\{f(d)+f(2d)+\cdots+f(n)\}$$

Where $j<'n$ ~~denote~~ represents $j<n$ and $(j,n)=1$.

Lemma 3[1] $\mathrm{Pot}_p\left(\binom{p^c}{r}\right) = c-\mathrm{pot}_p(r)$ $(0\leq r\leq p^c)$.

Lemma 4[6] Given integers r, d and K such that $d|K$, $d>0$, $K\geq 1$ and $(r,d)=1$. Then the number of elements in the set $S=\{r+td;\ t=1,2,\cdots K/d\}$ which are relatively prime to K is $\varphi(K)/\varphi(d)$.

§3 Proofs of theorems

Proof of theorem~~s~~ 1 g is the one in Lemma1, set $t = g^{\varphi(p^\alpha)/d}$, then $t^r \equiv g^{\varphi(p^\alpha)r_1/d_1} \pmod{p^\alpha} \equiv a \pmod{p^\alpha}$. where $r_1=\frac{r}{(r,d)}$, $d_1=\frac{d}{(r,d)}$ and $a=g^{\varphi(p^\alpha)r_1/d_1}$. Then both t^r and a have order d_1. Set $T=\{t^{\lambda r},\ \lambda<'d\}$ and $K=\{t^{rj}: j<'d_1\}$ are all elements of T not congruent with each other. Every element in K will reappear many ~~bt~~ times in T in the sense that if $a \equiv b \pmod{p^\alpha}$ then we regard a and b as the same element. Let t^{rj} be an arbitary element in K, for t^r has an order d_1, the number of the set $\{t^{r\lambda} : t^{r\lambda} \equiv t^{rj} \pmod{p^\alpha}, \lambda <' d\}$ is equal to the number of the set $\{\lambda : \lambda \equiv j \pmod{d_1}, \lambda <' d\}$ and equals to $\varphi(d)/\varphi(d_1)$ by means of Lemma 4. Thus every element in K will reappear $\varphi(d)/\varphi(d_1)$ times in T.

Set $K_a = \{a^k : k <' d_1\}$, then

$$S_r(p^\alpha, d) \equiv \sum_{b \in T} b \equiv \frac{\varphi(d)}{\varphi(d_1)} \sum_{b \in K} b \equiv \frac{\varphi(d)}{\varphi(d_1)} \sum_{b \in K_a} b \qquad (1)$$

From Lemma 2, we have

$$\sum_{b \in K_a} b = \sum_{h \mid d_1} \mu(h) \{a^h + a^{2h} + \cdots + a^{d_1}\} \equiv \sum_{h \mid d_1} \mu(h) \frac{a^{d_1} - 1}{a^h - 1} a^h \qquad (2)$$

Set $d_1 = p^{r_0} l_0$, $l_0 \mid p-1$, $l(n) = \begin{cases} 0 & n = 0 \\ 1 & n > 0 \end{cases}$, then

$$\sum_{b \in K_a} b = \sum_{h \mid p^{r_0} l_0} \mu(h) \frac{a^{d_1}-1}{a^h - 1} a^h = \sum_{\substack{0 \le k \le r_0 \\ l \mid l_0}} \mu(p^k l) \frac{a^{d_1}-1}{a^{p^k l} - 1} a^{p^k l}$$

$$= \sum_{l \mid l_0} \mu(l) \frac{a^{d_1}-1}{a^l - 1} a^l + l(r_0) \sum_{l \mid l_0} \mu(pl) \frac{a^{d_1}-1}{a^{pl}-1} a^{pl}$$

$$= \sum_{l \mid l_0} \mu(l) \frac{a^{d_1}-1}{a^l - 1} a^l - l(r_0) \sum_{l \mid l_0} \mu(l) \frac{a^{d_1}-1}{a^{pl}-1} a^{pl} \qquad (3)$$

For l. if $(a^l-1, p^\alpha)\neq 1$, then we have $a^l\equiv 1 \pmod p$, that is, $g^{\varphi(p^\alpha) l r_1/d_1}\equiv 1 \pmod p$. Because g is a primitive root of mod p, then $p-1 \mid \varphi(p^\alpha) l r_0/d_1$ that is, $p-1 \mid p^{\alpha-1-r_0} r_1 (p-1) l/l_0$. But $l_0 \mid d_1$, $(d_1, r_1)=1$ and $(l_0, p)=1$, we have $l_0 \mid l$.

Therefore, when $0<l<l_0$, we must have $(a^l-1, p^\alpha)=1$, then $\frac{a^{d_1}-1}{a^l-1}\equiv 0 \pmod{p^\alpha}$.

With the same derivation, we have $\frac{a^{d_1}-1}{a^{pl}-1}\equiv 0 \pmod{p^\alpha}$ for $0<l<l_0$.

From (3), we obtain

$$\sum_{b\in K_a} b \equiv \mu(l_0)\frac{a^{d_1}-1}{a^{l_0}-1}a^{l_0} - l(r_0)\,\mu(l_0)\frac{a^{d_1}-1}{a^{pl_0}-1}a^{pl_0} \pmod{p^\alpha} \quad (4)$$

Using Lemma 3, we arrive at the following

$$\mathrm{pot}_p\left(\binom{p^r}{k}p^{k\beta}\right) \geqslant \alpha+\beta \text{, when } \beta\geqslant \alpha-r \text{, } 1\leq r<\alpha \text{ and } 2\leq k\leq p^r. \quad (5)$$

In fact, we only need to prove

$$\mathrm{pot}_p\left(\binom{p^r}{k}p^{k\beta}\right) = \mathrm{pot}_p\left(\binom{p^r}{k}\right) + \mathrm{pot}_p(p^{k\beta}) = r - \mathrm{pot}_p(k) + k\beta$$

$\geqslant \alpha+\beta$. or. $r - \mathrm{pot}_p(k) + (k-1)\beta \geqslant \alpha$. Because $\beta \geqslant \alpha - r$, we only prove $r - \mathrm{pot}_p(k) + (k-1)(\alpha - r) \geqslant 0$ or $(k-2)(\alpha-r) \geqslant \mathrm{pot}_p(k)$. But this is easy to see, so we get the conclusion.

By means of Lemma1, there exsits μ, $p \nmid \mu$, such that

$$a^{l_0} = \left(g^{\varphi(p^\alpha) r_1/d_1} \right)^{l_0} = g^{p^{\alpha - r_0 - 1}(p-1)} = 1 + \mu p^\beta \qquad (6)$$

where $\beta \geqslant \alpha - r_0$. Then

$$\frac{a^{d_1}-1}{a^{l_0}-1} = \frac{(a^{l_0})^{p^{r_0}}-1}{a^{l_0}-1} = \frac{(1+\mu p^\beta)^{p^{r_0}}-1}{\mu p^\beta} = p^{r_0} +$$

$$+ \, l(r_0) \frac{1}{p^\beta} \sum_{k \geqslant 2} \binom{p^{r_0}}{k} \mu^{k-1} p^{k\beta} \equiv p^{r_0} \pmod{p^\alpha}$$

Reminding of (6), we obtain

$$\frac{a^{d_1}-1}{a^{l_0}-1} a^{l_0} \equiv p^{r_0} \pmod{p^\alpha} \qquad (7)$$

We can also derive by the same method that

$$\frac{a^{d_1}-1}{a^{pl_0}-1} a^{pl_0} \equiv p^{r_0 - 1} \pmod{p^\alpha} \quad (\text{if } r_0 \geqslant 1) \qquad (8)$$

Combining (7) and (8) with (4), we finally get

$$\sum_{btka} b \equiv \mu(l_0) p^{r_0} - l(r_0) \mu(l_0) p^{r_0 - 1} \pmod{p^\alpha}$$

$$\equiv \mu(l_0)\left(p^{r_0} - l(r_0)\, p^{r_0-1}\right) \pmod{p^\alpha} \equiv \mu(l_0)\,\varphi(p^{r_0}) \pmod{p^\alpha}$$

Put this into (1), we obtain

$$S_r(p^\alpha, d) \equiv \frac{\varphi(d)}{\varphi(d_1)}\, \mu(l_0)\,\varphi(p^{r_0}) \pmod{p^\alpha}$$

$$\equiv \frac{\varphi(d)}{\varphi(l_0)}\, \mu(l_0) \pmod{p^\alpha}.$$

This complete the proof of theorem1.

When $\alpha = 1$, $d \mid p-1$. $r_0 = 0$, and $l_0 = \frac{d}{(r,d)} = d_1$, then $S_r(p, d) \equiv \frac{\varphi(d)}{\varphi(d_1)}\, \mu(d_1) \pmod{p}$. This is what R. Moller obtained in 1952.

Proof of theorem 2. Notice that $h(d)$ is multiplicative and $p(d)$ is additive, therefore $\varphi(d)\mu(h(d)p^{-p(d)})/\varphi(h(d)p^{-p(d)})$ is multiplicative, too. Moreover, we obtain $F(x, r)$ is multiplitive for x.

Suppose that q is a prime, when $(q, p) = 1$,

$$F(q^{\alpha_1}, r) = \sum_{d \mid q^{\alpha_1}} \frac{\varphi(d)}{\varphi(h(d))}\, \mu(h(d)) = \sum_{k=0}^{\alpha_1} \varphi(q^k)\,\mu\!\left(\frac{q^k}{(q^k, r)}\right) \Big/ \varphi\!\left(\frac{q^k}{(r, q^k)}\right)$$

If $(q^{\alpha_1}, r) = q^\beta$, $0 < \beta < \alpha_1$, then

$$F(q^{\alpha_1}, r) = \sum_{i=0}^{\beta} \frac{\varphi(q^i)}{\varphi(1)} \mu(1) + \frac{\varphi(q^{\beta+1})}{\varphi(q)} \mu(q)$$

$$= \sum_{i=0}^{\beta} \varphi(q^i) - \frac{\varphi(q^{\beta+1})}{\varphi(q)} = q^\beta - q^\beta = 0$$

If $(q^{\alpha_1}, r) = q^{\alpha_1}$, then $F(q^{\alpha_1}, r) = \sum_{d \mid q^{\alpha_1}} \varphi(d_1) = q^{\alpha_1}$.

when $q = p$, $F(p^\beta, r) = \sum_{d \mid p^\beta} \frac{\varphi(d)}{\varphi(h(d) p^{-\gamma(d)})} \mu(h(d) p^{-\gamma(d)})$

$= \sum_{d \mid p^\beta} \varphi(d) = p^\beta$.

Therefore, if $x = p^\beta \gamma_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is canonical decomposition of x, then

$$F(x, r) = F(p^\beta, r) F(p^{\alpha_1}, r) \cdots F(p_k^{\alpha_k}, r)$$

$$= \begin{cases} p^\beta p_1^{\alpha_1} \cdots p_k^{\alpha_k} = x & \text{when } p^{-pot_p(x)} x \mid r \\ 0 & \text{otherwise} \end{cases}$$

This completes the proof.

When $p = 2$, we have also obtain an interesting result, that is,

$$S_r(2^\alpha, 2^{n_0}) \equiv (-1)^r \Delta(n_0) + [1 + (-1)^r] \varphi(2^{n_0}) \pmod{2^\alpha}$$

where $\alpha \geq 3$, $0 \leq n_0 \leq n-2$, $\Delta(n_0) = \left[\frac{1}{n_0}\right]$.

$S_r(2,1) \equiv 1 \pmod 2$ $S_r(4,2) \equiv (-1)^r \pmod 4$.

This will be discussed in anther paper.

In writting thepaper, I have got a Lot of instruction from my tutor, Professor SHAO, Pinzong. I am greatly indebted to him.

References

[1] H. Gupta, Selected Topics in Number Theory, ABACUS Press, 1980 pp. 55-57.

[2] R. Moller, Sums of powers of Numbers Having Given Exponent Modulo a prime. Amer. Math. Monthly 59 (1952)

[3] Gauss, C.F. Disquisitions Arithmeticae, Arts. 80-81.

[4] Stern, M.A. Bemerkungen über hohere Arithmetik.

Journal für Mathematik . Vol.VI (1830) pp.147-153.

[5] Forsyth . A.R. Primitive Roots of Primes and their Residues , Messenger of Mathematics , Vol. XIII (1883-4) pp. 180-185.

[6] Apostal . T. An Introduction to Analytic Number Theory , Springer-Verlag , New York Heidelberg Berlin , 1976 , pp. 124.

关于某一类指数方幂和的再讨论

1985. 9. 15.

设 $S_r(p^\alpha,d)$ 表示在 $\bmod p^\alpha$ 的中一个完全剩余系中指数为 d 的元素之方幂和。1985年，本文作者[1]证明了当 p 为奇素数，r, α, d 为正整数，$d|\varphi(p^\alpha)$ 的情况下

$$S_r(p^\alpha,d)\equiv\frac{\varphi(d)}{\varphi(l_0)}\mu(l_0)\ \ (\bmod p^\alpha)$$

其中 $d/(r,d) = p^{r_0}l_0$. $p\nmid l_0$.

本文的目的在于证明模为 2^α 的情况，即

定理 $S_r(2^\alpha,2^{n_0})\equiv(-1)^r\Delta(n_0)+[1+(-1)^r]\varphi(2^{n_0})\ (\bmod 2^\alpha)$

其中 $\alpha\geqslant3$，$0<n_0\leqslant\alpha-2$ $\Delta(n_0)=[\frac{1}{n_0}]$

$$S_r(2,1)\equiv1\ (\bmod 2),\quad S_r(4,2)\equiv(-1)^r(\bmod 4).$$

证明 当 $\alpha\geqslant3$ 时，$\pm5^0$, $\pm5^1$, …… $\pm5^{2^{\alpha-2}-1}$ 构成 $\bmod 2^\alpha$ 的一个简化剩余系([2])。

下面分两种情况证明

(i) 当 $n_0=1$ 时，若 n 的指数为 2，设

$n\equiv(-1)^{v}5^{v_0}\pmod{2^\alpha}$，则由

$n^2\equiv[(-1)^{v}5^{v_0}]^2\equiv5^{2v_0}\equiv1\pmod{2^\alpha}$，必有 $2^{\alpha-3}|v_0$

这样指数为 2 的元素只有 -1，$\pm5^{2^{\alpha-3}}$，故有

$$S_r(2^\alpha,2)=(-1)^r+[1+(-1)^r]5^{2^{\alpha-3}r}$$

$$\equiv\begin{cases}-1\pmod{2^\alpha} & \text{当 } 2\nmid r \text{ 时}\\ 3\pmod{2^\alpha} & \text{当 } 2|r \text{ 时}\end{cases}$$

$$\equiv1+2(-1)^r\pmod{2^\alpha}\equiv(-1)^r\Delta(1)+[1+(-1)^r]\varphi(2^1)\pmod{2^\alpha}$$

(ii) 当 $n_0>1$ 时，设 n 的指数为 2^{n_0}，$n\equiv(-1)^{v}5^{v_0}\pmod{2^\alpha}$

由 $n^{2^{n_0}}\equiv1\pmod{2^\alpha}$，得到 $5^{v_02^{n_0}}\equiv1\pmod{2^\alpha}$

从而 $2^{\alpha-2}|2^{n_0}v_0$，即 $2^{\alpha-n_0-2}|v_0$．设

$$v_0=2^{\alpha-n_0-2}n_1$$

下证明 $(n_1,2)=1$．否则，若 $2|n_1$ 时，必有

$n^{2^{v_0-1}}\equiv[(-1)^{v}5^{v_0}]^{2^{n_0-1}}\equiv5^{2^{\alpha-3}n_1}\equiv1\pmod{2^\alpha}$，

这与 n 的指数为 2^{n_0} 相矛盾．

反之，若 $v_0 = 2^{\alpha-2-n_0} n_1$，$2\nmid n_1$，则 $(-1)^v 5^{v_0}$ 的指数为 2^{n_0}。因为 $\{(-1)^v 5^{v_0} \mid v=0,1,\ 2^{\alpha-n_0-2} \| v_0\}$ 构成 mod 2^α 中的某个简化剩余系中指数为 2^{n_0} 的全体元素（$2^k \| n$ 表示 $2^k | n$，但 $2^{k+1} \nmid n$）。

所以（$j<'n$ 表示 $j<n$，且 $(j,n)=1$）

$$S_r(2^\alpha, 2^{n_0}) \equiv \sum_{\substack{v_0:\ 2^{\alpha-n_0-2} \\ v=0,1}} [(-1)^v 5^{v_0}]^r$$

$$= [1+(-1)^r] \sum_{v_0:\ 2^{\alpha-n_0-2} \| v_0} 5^{rv_0}$$

$$= [1+(-1)^r] \sum_{k<'2^{n_0}} \left(5^{r 2^{\alpha-n_0-2}}\right)^k$$

$$= [1+(-1)^r] \sum_{k<'2^{n_0}} (5^l)^k \quad (记\ l = r2^{\alpha-n_0-2})$$

应用下述结果（见[3]）

$$S'(n) = \sum_{j<'n} f(j) = \sum_{d|n} \mu(d)\{f(d)+f(2d)+\cdots+f(n))$$

便有

$$S_r(2^\alpha, 2^{n_0}) \equiv [(-1)^r+1] \sum_{d|2^{n_0}} \mu(d)\Big[\sum_{k=1}^{2^{n_0}/d} (5^l)^{kd}\Big]$$

$$\equiv [1+(-1)^r] \sum_{d|2^{n_0}} \mu(d) \frac{5^{l\cdot 2^{n_0}}-1}{5^{ld}-1} \cdot 5^{ld}$$

$$\equiv [1+(-1)^r]\left(\mu(1)\frac{5^{l\cdot 2^{n_0}}-1}{5^l-1}+\mu(2)\frac{5^{l\cdot 2^{n_0}}-1}{5^{2l}-1}\cdot 5^{2l}\right)$$

$$\equiv (1+(-1)^r)\frac{5^{l\cdot 2^{n_0}}-1}{5^{2l}-1}\cdot 5^l \qquad (1)$$

当 $2\nmid r$ 时，$S_r(2^\alpha, 2^{n_0}) \equiv 0 \pmod{2^\alpha}$

当 $2|r$ 时，讨论其同余情况.

很容易由数学归纳法证明

$$5^{2^{l-2}} \equiv 1+2^l \pmod{2^{l+1}}$$

其中 $2\leq l\leq \alpha-1$. 故必有

$$5^{2^{\alpha-n_0-2}} \equiv 1+2^{\alpha-n_0} \pmod{2^{\alpha+1-n_0}}$$

当 $2|r$ 时，$5^{r\cdot 2^{\alpha-n_0-2}} \equiv 1+2^{r_0} \pmod{2^{r_0+1}}$

即 $5^l \equiv 1+2^{r_0} \pmod{2^{r_0+1}}$ (2)

其中 $r_0 \geq \alpha-n_0+1$.

设 $5^l = 1+\mu 2^{r_0}$，其中 $2\nmid\mu$. 这样必有

$$5^{2l} = 1+\mu_1 2^{r_0+1} \qquad (2\nmid\mu_1)$$

于是

$$\frac{5^{l\cdot 2^{n_0}}-1}{5^{2l}-1} = \frac{(1+\mu_1 2^{r_0+1})^{2^{n_0-1}}-1}{\mu_1 2^{r_0+1}} = 2^{n_0-1} +$$

$$+\frac{1}{2^{r_0+1}}\sum_{k\geq 2}\binom{2^{n_0-1}}{k}\mu_1^{k-1}2^{k(r_0+1)}$$

$$\equiv 2^{n_0-1} \pmod{2^\alpha}.$$

其中用到 $pot_2\left(\binom{2^{n_0-1}}{k}2^{k(r_0+1)}\right)\geq \alpha+r_0+1$ $(k\geq 2)$

而结合(2) 及 $r_0\geq \alpha-n_0+1$ 可得:

$$\frac{5^{l\cdot 2^{n_0}}-1}{5^{2l}-1}\cdot 5^{l}\equiv 2^{n_0-1} \pmod{2^\alpha}$$

代入(1)可得

$$S_r(2^\alpha, 2^{n_0})\equiv[1+(-1)^r]\,2^{n_0-1} \pmod{2^\alpha}$$

$$\equiv[1+(-1)^r]\,\varphi(2^{n_0}) \pmod{2^\alpha}$$

若定义

$$\Delta(n)=\left[\frac{1}{n}\right]=\begin{cases}1 & n=1\\ 0 & n>1\end{cases}$$

综合(i)(ii)可得:

$$S_r(2^\alpha, 2^{n_0})\equiv\Delta(n_0)(-1)^r+[1+(-1)^r]\varphi(2^{n_0}) \pmod{2^\alpha}.$$

易知 $S_r(2,1)\equiv 1 \pmod 2$ $S_r(4,2)\equiv(-1)^r \pmod 4$.

这就完成了定理的证明.

参 考 文 献

[1] 方玉光. 某一类指数方幂和的同余问题.

[2] K. Ireland & M. Rosen. A Classical Introduction to Modern Number Theory. Springer-Verlag New York Heidelberg BerLin (1980) 43-45.

[3] H. Gupta, Selected Topics in Number Theory. ABACUS Press, 1980. PP. 55-57

关于某一类指数方幂和一个定理的简证明

1986. 3. 17.

设 $S_n(p^\alpha, d)$ 表示 modp^α 的完全剩余系中指数为 d 元素的 n 次方幂和，其中 p 为奇素数，α. d, n 为正整数. 1952 年，R. Moller[2] 证明了

$$S_n(p^\alpha, d) \equiv \frac{\varphi(d)}{\varphi(d_1)} \mu(d_1) \pmod p .$$

其中 $d_1 = \frac{d}{(n,d)}$. 1985 年，本作者[1]证明了

$$S_n(p^\alpha, d) \equiv \frac{\varphi(d)}{\varphi(l_0)} \mu(l_0) \pmod{p^\alpha} .$$

其中 $\alpha \geq 0$. p 为奇素数, $d/(n,d) = p^{r_0} l_0$, $(p \nmid l_0)$.

本文改进了 H. S, Zukurman[1] 的方法，给出了上述结果的另一个证明。

设 $h(d) = \frac{d}{(n,d)}$. $p(d) = \mathrm{pot}_p(h(d))$, 对于 $x \mid \varphi(p^\alpha)$.

定义

$$F(x,n) = \sum_{d \mid x} \frac{\varphi(d)}{\varphi(h(d)p^{-p(d)})} \mu(h(d)p^{-p(d)})$$

对于此 $F(x,n)$，我们得到类似 Zukerman 的同样类似的结果（注：以下 $\equiv$ 都表示 $\bmod p^{\alpha}$ 的同余号）

定理一

$$F(x,n)=\begin{cases} x & \text{当 } p^{-pot_p(x)}x \mid n \text{ 时} \\ 0 & \text{否则} \end{cases}$$

证明　注意到 $h(d)$ 为积性函数，$P(d)$ 为可加性函数，即可知：$\varphi(d)\mu(h(d)p^{-P(d)})/\varphi(h(d)p^{-pot_p(dh(d))})$ 为积性函数，进而推知 $F(x,n)$ 关于 x 为积性的。

设 q 为一个素数，当 $(q,p)=1$ 时，

$$F(x,n)=\sum_{d\mid q^{\alpha_1}}\frac{\varphi(d)}{\varphi(h(d))}\mu(h(d))=\sum_{k=0}^{\alpha_1}\frac{\varphi(q^{k})}{\varphi\left(\frac{q^{k}}{(q^{k},n)}\right)}\mu\left(\frac{q^{k}}{(q^{k},n)}\right)$$

当 $(q^{\alpha_1},n)=q^{\beta}$，$0\le\beta<\alpha_1$ 时，我们有

$$F(q^{\alpha_1},n)=\sum_{i=0}^{\beta}\frac{\varphi(q^{i})}{\varphi(1)}\mu(1)+\frac{\varphi(q^{\beta+1})}{\varphi(q)}\mu(q)$$

$$=\sum_{i=0}^{\beta}\varphi(q^{i})-\frac{\varphi(q^{\beta+1})}{\varphi(q)}=q^{\beta}-q^{\beta}=0.$$

当 ~~q=~~ $(q^{\alpha_1},n)=q^{\alpha_1}$ 时，

$$F(q^{\alpha_1},n)=\sum_{d\mid q^{\alpha_1}}\varphi(d)=q^{\alpha_1},$$

当 $q=p$ 时，

$$F(p^{\beta},n)=\sum_{d\mid p^{\beta}}\frac{\varphi(d)}{\varphi(h(d)p^{-P(d)})}\mu(h(d)p^{-P(d)})$$

$$=\sum_{d\mid p^{\beta}}\varphi(d)=p^{\beta}$$

设 $x=p^{\beta}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 为 x 的典型分解式，则

$$F(x,n)=F(p^{\beta},n)F(p_1^{\alpha_1},n)\cdots F(p_k^{\alpha_k},n)$$

$$=\begin{cases}p^{\beta}p_1^{\alpha_1}\cdots p_k^{\alpha_k}=x & \text{当 } p^{-\mathrm{pot}_p(x)}x\mid n \text{ 时}\\ 0 & \text{否则}\end{cases}$$

定理一证毕.

H. S. Zukurman 在 $\alpha=1$ 时曾对 R. Moller 结果给出了一个简单证明（见 [2] Additional Remark）. 它是先证明了类似于定理一的一个结果，然后给出证明的. 下面我们使用定理一的类似形式去证明 [1] 中的结果.

定理二 $S_n(p^{\alpha},d)\equiv\frac{\varphi(d)}{\varphi(l_0)}\mu(l_0)\pmod{p^{\alpha}}$，

其中 $\alpha\geq0$，p 为素数，$d/(n,d)=p^{\gamma_0}l_0$. $(p\nmid l_0)$.

首证明几个引理

设 $x|\varphi(p^\alpha)$，定义

$$F_1(x,n)=\sum_{d|x}f(d,n)\text{，}f(d,n)=\sum g_d^n$$

其中求和号是对一切具有指数为 d 的元素 g_d 取的.

引理1　$F_1(x,n)\equiv\sum_{u^x\equiv1(p^\alpha)}u^n$，其中$\Sigma$是对一切 $u^x\equiv1\ (p^\alpha)$ 的不同余的根取的.

证明　只要比较 $\sum_{d|x}\sum g_d^n$ 与 $\sum_{u^x\equiv1(p^\alpha)}u^n$ 的对应项，立即得证.

引理2　$F_1(x,n)$ 对于 $\varphi(p^\alpha)$ 的因子关于 $\bmod p^\alpha$ 为积性的，即 $d_1d_2|\varphi(p^\alpha)$，$(d_1,d_2)=1$，则

$$F_1(d_1,n)F_1(d_2,n)\equiv F_1(d_1d_2,n)\quad(\bmod p^\alpha).$$

证明　由引理1，

$$F_1(d_1,n)F_2(d_2,n)=\Big(\sum_{u_1^{d_1}\equiv1(p^\alpha)}u_1^n\Big)\Big(\sum_{u_2^{d_2}\equiv1(p^\alpha)}u_2^n\Big)$$
$$=\sum_{\substack{u_i^{d_i}\equiv1(p^\alpha)\\ i=1,2}}(u_1u_2)^n$$

我们断言当 u_1, u_2 分别通过 $u^{d_1}\equiv1\ (\bmod p^\alpha)$

$u_2^{d_2}\equiv 1 \pmod{p^\alpha}$ 的解系时，$\{u_1u_2\}$ 也通过 $u^{d_1d_2}\equiv 1 \pmod{p^\alpha}$ 的解系。事实上，当 $(a,m)=1$ 则 $x^n\equiv a \pmod{p^\alpha}$ 的解数为 $(n,\varphi(p^\alpha))$（参看[4]）因此 $u_1^{d_1}\equiv 1 \pmod{p^\alpha}$ 与 $u_2^{d_2}\equiv 1 \pmod{p^\alpha}$ 各有 d_1, d_2 个解，而 $u^{d_1d_2}\equiv 1 \pmod{p^\alpha}$ 有 d_1d_2 个解。又当 u_1,u_2 分别为前二方程的解时，u_1u_2 必为后一方程的解。反之，当 u 为 $u^{d_1d_2}\equiv 1 \pmod{p^\alpha}$ 的解时，设其指数为 l，设 $l=l_1l_2$，其中 $l_1|d_1$，$l_2=d_2$。由于 $(d_1,d_2)=1$，故存在 g_1,g_2，使得 $g_1l_1+g_2l_2=1$，于是 $u=u^{g_1l_1}\cdot u^{g_2l_2}$，但 $u^{g_1l_1}$ 为 $u^{d_2}\equiv 1 \pmod{p^\alpha}$ 的解，$u^{g_2l_2}$ 为 $u^{d_1}\equiv 1 \pmod{p^\alpha}$ 的解，此即表明 $u^{d_1d_2}\equiv 1 \pmod{p^\alpha}$ 的解可分解成 $u^{d_1}\equiv 1 \pmod{p^\alpha}$ 与 $u^{d_2}\equiv 1 \pmod{p^\alpha}$ 的乘积。故所断言证明。

这样，$F_1(d_1,n)F_2(d_2,n)\equiv \sum_{u^{d_1d_2}\equiv 1(p^\alpha)} u^n$
$\equiv F_1(d_1d_2,n) \pmod{p^\alpha}$，引理证毕

引理3[3] 若p为奇素数，且$p \nmid b$，n为正整数，则 $a^{p^s} \equiv b^{p^s} \pmod{p^{n+s}}$ 之充分必要条件为 $a \equiv b \pmod{p\alpha}$

定理三

$$F_1(x,n) = \begin{cases} x & \text{当 } p^{-pot_p(x)}x \mid n \text{ 时} \\ 0 & \text{否则} \end{cases}$$

证明：令 $x = p^l x_1$ $(p \nmid x_1)$ 则由引理2可知 $F_1(x,n) \equiv F_1(p^l, n) F_1(x_1, n) \pmod{p^\alpha}$

设u_0为一指数为x_1的元素，于是当$\{u_0 u\}$当u通过 $u^{x_1} \equiv 1 \pmod{p^\alpha}$ 的解组时，亦通过其解组，故

$$F_1(x_1,n) \equiv \sum_{u^{x_1} \equiv 1 (p^\alpha)} u^n \equiv \sum_{u^{x_1} \equiv 1} (u_0 u)^n = u_0^n \sum_{u^{x_1} \equiv 1} u^n$$

$$\equiv u_0^n F_1(x_1, n) \pmod{p\alpha}$$

因此 $(u_0^n - 1) F_1(x_1, n) \equiv 0 \pmod{p^\alpha}$

当 $x_1 \nmid n$ 时，则 $(u_0^n - 1, p) = 1$ （否则 $u_0^n \equiv 1 \pmod{p}$ 则易证 $u_0^{p^{\alpha-1}n} \equiv 1 \pmod{p^\alpha}$，故 $x_1 \mid p^{\alpha-1}n$，矛

$(x_1, p)=1$，故 $x_1 | n$. 矛盾)

于是有 $F_1(x_1, n) \equiv 0 \pmod{p^\alpha}$.

当 $x_1 | n$ 时，$F_1(x_1, n) \equiv \sum\limits_{u^{x_1}\equiv 1} 1 \equiv x_1 \pmod{p^\alpha}$.

这样，我们有

$$F_1(x_1, n) = \begin{cases} x_1 & \text{当 } x_1 | n \text{ 时} \\ 0 & \text{否则} \end{cases}.$$

设 u_0 为关于指数为 p^β 的元素. 由于 $\{u : u^{p^\beta} \equiv 1 \pmod{p^\alpha}\}$ 构成一个以 u_0 为生成元的循环群，故必有

$$F_1(p^\beta, n) \equiv \sum_{r=1}^{p^\beta} u_0^{n\lambda} \equiv \frac{u_0^{np^\beta}-1}{u_0^n-1} \pmod{p^\alpha}.$$

易知：u_0^n 的指数为 p^β 的因子，记为 p^r. 由引理 3 可知：存在 a，$p \nmid a$，使得 $u_0^n = 1 + ap^{\alpha-r}$ $(r \leq \beta)$. 从而有

$$\frac{u_0^{np^\beta}-1}{u_0^n-1} = \frac{1}{ap^{\alpha-1}}\left[(1+ap^{\alpha-r})^{p^\beta}-1\right]$$

$$= p^\beta + \frac{1}{p^{\alpha-r}} \sum_{k\geq 2} \binom{p^\beta}{k} a^{k-1} p^{k(\alpha-r)}$$

$$\equiv p^{\beta} \pmod{p^{\alpha}}$$

(最后一步用到了 $\operatorname{pot}_p\left(\binom{p^{\beta}}{\kappa} p^{\kappa(\alpha-r)}\right) = \beta - \operatorname{pot}_p(\kappa) + \kappa(\alpha-r)$

$\geq 2\alpha - r$)

即: $F_1(p^{\beta}, n) \equiv p^{\beta} \pmod{p^{\alpha}}$

综上所述可知

$$F_1(x,n) \equiv \begin{cases} p^l x_1 = x & 当\ p^{-\operatorname{pot}_p(x)} x \mid n\ 时 \\ 0 & 否则 \end{cases}$$

完成定理的证明.

定理二的证明 由定理三可知:

$$\sum_{d \mid x} f(d,n) \equiv \begin{cases} x \pmod{p^{\alpha}} & 当\ p^{-\operatorname{pot}_p(x)} x \mid n\ 时 \\ 0 & 否则 \end{cases}$$

由 Möbius 逆转公式可得 ($x = p^l x_1$, $p \nmid x_1$)

$$f(x,n) \equiv \sum_{d \mid x} F_1(d,n) \mu\left(\frac{x}{d}\right) \equiv \sum_{\substack{d \mid x \\ p^{-\operatorname{pot}_p(d)} d \mid n}} d\, \mu\left(\frac{x}{d}\right)$$

$$\equiv \sum_{\substack{p^r d_1 \mid p^l x_1 \\ d_1 \mid n}} p^r d_1\, \mu\left(\frac{x_1}{d_1} \cdot \frac{p^l}{p^r}\right) \equiv \left(\sum_{p^r \mid p^l} p^r \mu\left(\frac{p^l}{p^r}\right)\right)\left(\sum_{\substack{d_1 \mid x_1 \\ d_1 \mid n}} d_1 \mu\left(\frac{x_1}{d_1}\right)\right)$$

$$=\varphi(p^{l})\frac{\varphi(x_1)}{\varphi\left(\frac{x_1}{(x_1,n)}\right)}\mu\left(\frac{x_1}{(x_1,n)}\right)=\frac{\varphi(x)}{\varphi\left(\frac{x_1}{(x_1,n)}\right)}\mu\left(\frac{x_1}{(x_1,n)}\right) \quad *)$$

设 $\frac{x}{(x,n)}=p^{r_0}l_0$，其中 $p\nmid l_0$，易知 $\frac{x_1}{(x_1,n)}=l_0$.

因此，$S_n(p^{\alpha},x)\equiv f(x,n)\equiv\frac{\varphi(x)}{\varphi(l_0)}\mu(l_0)\pmod{p^{\alpha}}$

这就是定理二的结果.

*) 这里用到 H.S. Zukurman 的结果[2].

对于模为一般正整数的情况，有待研究.

著名的 Ramanujan 和已引起许多数学家的注意，它是这样定义：

$$C_k(n)=\sum_{\substack{m \bmod k\\(m,k)=1}}e^{2\pi imn/k}$$

已知[5]：$C_k(n)=\frac{\varphi(k)}{\varphi\left(\frac{k}{(n,k)}\right)}\mu\left(\frac{k}{(n,k)}\right)$，这正好与定理二当 $\alpha=1$ 的结果中等式的右边相等. 那么定理二究竟与 Ramanujan 和有何联系呢？这也是一个有待探讨的问题！

参 考 文 献

[1] 方玉光．某一类指数方幂和的同余问题．

[2] R. Moller, Sums of Powers of Numbers Having a Given Exponent Modulo a Prime. Amer. Math. Monthly 59(1952) 226-230.

[3] W. J. LeVeque. Topics in Number Theory Vol I. Addison-Wesley Publ. Co., Reading, Mass. 1955.

[4] K. Ireland & M. Rosen. A Classical Introduction to Modern Number Theory, Springer-Verlag. New York Heidelberg Berlin. (1980) 45-46.

[5] T. Apostal. An Introduction to Analytic Number Theory ~~The~~ Springer-Verlag New York Heidelberg Berlin (1976) 160-164.

关于正整数k进位表示中的一个定理

1985. 9. 20.

设 $k \geq 1$ 为一个固定整数，则任意正整数 x 可以唯一表示成下述形式

$$x = a_1 k^{n_1} + a_2 k^{n_2} + \cdots + a_t k^{n_t} .$$

其中 $n_1 > n_2 > \cdots > n_t \geq 0$ 是整数，$a_1, a_2, \cdots a_t$ 为不超过 $k-1$ 的非负整数．定义

$$\alpha(x) = \sum_{i=1}^{t} a_i \;,\quad A(x) = \sum_{y \leq x} \alpha(y)$$

在1940年，Bush[1] 证明了

$$A(x) \sim \frac{k-1}{2\log k}\, x \log x$$

在1948年，Bellman 和 Shapiro[2] 证明了

$$A(x) = \frac{k-1}{2\log k}\, x \log x + O(x \log\log x)$$

对于 $k=2$ 的情况．

在1949年，Mirsky[3] 把 O 下的项改进成 $O(x)$．但是用他的方法，我们不能给出 $O(x)$ 中

所含常数的估计，而且也不能断定可把 O(x) 中改进成更低阶的形式。

在 1955 年，周伯壎和严士健[4] 也证明了

$$A(x)=\frac{k-1}{2\log k}x\log x + O(x) \qquad (1)$$

并没指出 O(x) 不能再改进成更低阶无穷大量的形式。但利用他们的方法，我只能给出 O(x) 中所含常数的一个粗糙估计，而且他们的证明也较烦琐。

本文利用 Lagrange 的一个恒等式，不仅给出了 O(x) 中所含常数的一个较好的估计，而且同时给出了 (1) 的一个简单证明。即我们证明

定理： $A(x)=\frac{k-1}{2}\frac{x\log x}{\log k} + \theta(x)x \quad (k\geq 2)$

其中 $-\frac{5k-4}{8}\leq\theta(x)\leq\frac{k+1}{2}$.

先给 Lagrange 恒等式一个证明

引理[5] (J. L. Lagrange) $\frac{n-\alpha(n)}{k-1}=\sum_{r=1}^{\infty}\left[\frac{n}{k^r}\right]$

证明　设 $n = a_0 + a_1 k + \cdots + a_h k^h$，则

$$\frac{n-\alpha(n)}{k-1} = \frac{1}{k-1}\sum_{r=1}^{h} a_r(k^r-1) = \sum_{r=1}^{k} a_r(k^{r-1}+k^{r-2}+\cdots+1)$$

$$= \sum_{r=1}^{h}(a_h k^{h-r} + a_{h-1}k^{h-r-1} + \cdots + a_r)$$

$$= \sum_{r=1}^{h}\left[\frac{n}{k^r}\right] = \sum_{r=1}^{\infty}\left[\frac{n}{k^r}\right]$$

证毕

定理的证明　由引理，我们有

$$A(x) = \sum_{n\le x}\left(n-(k-1)\sum_{r=1}^{h}\left[\frac{n}{k^r}\right]\right)$$

$$= \frac{1}{2}x(x+1) - (k-1)\sum_{i=1}^{\infty}\sum_{n\le x}\left[\frac{n}{k^i}\right]$$

$$= \frac{1}{2}x(x+1) - (k-1)\sum_{1\le i\le \log_k x}\left(\frac{1}{2}\left[\frac{x}{k^i}\right]\left(\left[\frac{x}{k^i}\right]-1\right)k^i + \right.$$

$$\left. + \left[\frac{x}{k^i}\right]\left(x-\left[\frac{x}{k^i}\right]x+1\right)\right)$$

$$= \frac{1}{2}x(x+1) + \frac{1}{2}(k-1)\sum_{1\le i\le \log_k x} k^i\left[\frac{x}{k^i}\right] - (k-1)\sum_{1\le i\le \log_k x}\left[\frac{x}{k^i}\right]$$

$$-(k-1)\sum_{1\le i\le \log_k x}\left(x\left[\frac{x}{k^i}\right] - \frac{1}{2}\left[\frac{x}{k^i}\right]^2 k^i\right) \qquad (2)$$

由于

$$\sum_{1\le i\le \log_k x} k^i\left[\frac{x}{k^i}\right] = x[\log_k x] + \sum_{1\le i\le \log_k x} k^i\left(\left[\frac{x}{k^i}\right]-\frac{x}{k^i}\right)$$

$$= x\log_k x - \theta_1 x + \sum_{1\le i\le \log_k x} k^i\left(\left[\frac{x}{k^i}\right]-\frac{x}{k^i}\right) \quad (0\le\theta_1\le 1).$$

$$\sum_{1\le i\le \log_k x}\left(x\left[\frac{x}{k^i}\right] - \frac{1}{2}\left[\frac{x}{k^i}\right]^2 k^i\right) = \sum_{1\le i\le \log_k x}\left(\frac{1}{2}\frac{x^2}{k^i} - \frac{1}{2}k^i\left(\left[\frac{x}{k^i}\right]-\frac{x}{k^i}\right)^2\right)$$

$$= \frac{1}{2}x^2\sum_{1\le i\le \log_k x}\frac{1}{k^i} - \frac{1}{2}\sum_{1\le i\le \log_k x}k^i\left(\left[\frac{x}{k^i}\right]-\frac{x}{k^i}\right)^2$$

故代入(2)可知

$$A(x) = \frac{1}{2}x(x+1) + \frac{k-1}{2}x\log_k x - \frac{k-1}{2}\theta_1 x - (k-1)\sum_{1\le i\le \log_k x}\left[\frac{x}{k^i}\right]$$

$$-\frac{1}{2}(k-1)\sum_{1\le i\le \log_k x}\left(\left\{\frac{x}{k^i}\right\}-\left\{\frac{x}{k^i}\right\}^2\right)k^i$$

$$-\frac{k-1}{2}x^2\sum_{1\le i\le \log_k x}\frac{1}{k^i} \qquad (3)$$

其中$\{y\}$表示y的小数部分.

易推证

$$\sum_{1\le i\le \log_k x}\left[\frac{x}{k^i}\right] = \theta_2\frac{x}{k-1} \qquad (0\le\theta_2\le 1)$$

$$\sum_{1\le i\le \log_k x}\left(\left\{\frac{x}{k^i}\right\}-\left\{\frac{x}{k^i}\right\}^2\right)k^i = \theta_3\frac{kx}{4(k-1)} \qquad (0\le\theta_3\le 1)$$

（这里用到了 $0\le x-x^2\le\frac{1}{4}$ $(0\le x\le 1)$）

$$x^2\sum_{1\le i\le \log_k x}\frac{1}{k^i} = \frac{x^2}{k-1} - \frac{1}{k-1}\frac{x^2}{k^{[\log_k x]}}$$

因此代入(3)，我们有

$$A(x) = \frac{k-1}{2}x\log_k x - \left(\frac{k-1}{2}\theta_1 + \theta_2 - \frac{1}{2} + \frac{k}{8}\theta_3 - \frac{1}{2}\frac{x}{k^{[\log_k x]}}\right)x$$

$$\triangleq \frac{k-1}{2}\frac{x\log x}{\log k} + \theta(x)x$$

其中$-\frac{5k-4}{8}\le\theta(x)\le\frac{k+1}{2}$. 这就便完成了定理之证明.

参考文献

[1] L. E. Bush. An Asymptotic formula for the average sums of the digits of integers, Amer. Math. Monthly 47 (1940) 154-156.

[2] R. Bellman & H. N. Shapiro, On a problem in additive number theory, Ann. Math. Princeton II 49 (1948) 333-340.

[3] L. Mirsky, A theorem on representations of integers in the scale of r. Scripta Math. New York 15 (1949) 11-12.

[4] 周伯壎与严士健，关于K进位表示法的一个问题，数学学报 Vol 5 No. 4 1955. 12.

[5] H. Gupta, Selected topics in number theory. ABACUS Press. 1980.

On a theorem in the K-adic representation of positive integers

FANG Yuguang

Let $K\geqslant 1$ be a fixed integers, then any positive integer x can be uniquely represented by the following form

$$x = a_1K^{n_1}+a_2K^{n_2}+\cdots+a_tK^{n_t}$$

where $n_1>n_2>\cdots>n_t\geqslant 0$ are integers, and $a_1, a_2, \cdots a_t$ are also positive integers not exceeding $K-1$. Define

$$\alpha(x)=\sum_{i=1}^{t} a_i, \text{ and } A(x)=\sum_{y\leq x}\alpha(y)$$

In 1940, Bush[1] has shown $A(x)\sim\frac{K-1}{2\log K}x\log x$

In 1948, Bellman and Shapiro[2] has proved

$A(x)=\frac{K-1}{2\log K}x\log x+O(x\log\log x)$ for $K=2$; In 1949, Mirsky[3] improved the O-term to $O(x)$ for any $K\geqslant 2$, but using his method, we can't give the estimation of the implied constant in $O(x)$.

In 1955. Cheo Peh-Hsiün and Yien Sze-Chien[4] also proved $A(x) = \frac{k-1}{2\log k} x\log x + O(x)$. (1)

Although by means of their method, we can estimate the implied constant in $O(x)$, it is too unaccurate and more importantly, their method is too complicated.

In this paper, we shall give a Linear inequality on k for the estimation of the implied constant and give a very simple proof of (1) as the same time, that is, we have proved

Theorem $A(x) = \frac{k-1}{2}\frac{x\log x}{\log k} + \theta(x)\, x \quad (k \geqslant 2)$

where $-\frac{5k-4}{8} \leqslant \theta(x) \leqslant \frac{k+1}{2}$.

Lemma[5] (J.L. Lagrange) $\frac{n-\alpha(n)}{k-1} = \sum_{r=1}^{\infty}\left[\frac{n}{k^r}\right]$

Proof Set $n = a_0 + a_1 k + \cdots + a_h k^h$, then

$$\frac{n-\alpha(n)}{k-1} = \frac{1}{k-1}\sum_{r=1}^{h} a_r(k^r-1) = \sum_{r=1}^{h} a_r(k^{r-1}+k^{r-2}+\cdots+1)$$

$$= \sum_{r=1}^{h} \left(a_n k^{h-r} + a_{n-1} k^{h-r-1} + \cdots + a_r \right) = \sum_{r=1}^{h} \left[\frac{n}{k^r} \right] \qquad \|$$

Proof of Theorem Using the Lemma, we have

$$A(x) = \sum_{n \le x} \left(n - (k-1) \sum_{r=1}^{h} \left[\frac{n}{k^r} \right] \right)$$

$$= \frac{1}{2} x(x+1) - (k-1) \sum_{r=1}^{\infty} \sum_{n \le x} \left[\frac{n}{k^r} \right]$$

$$= \frac{1}{2} x(x+1) - (k-1) \sum_{1 \le r \le \log_k x} \left(\frac{1}{2} \left[\frac{x}{k^r} \right] \left(\left[\frac{x}{k^r} \right] - 1 \right) k^r + \left[\frac{x}{k^r} \right] \left(x - \left[\frac{x}{k^r} \right] k^r + 1 \right) \right)$$

$$= \frac{1}{2} x(x+1) + \frac{1}{2}(k-1) \sum_{1 \le r \le \log_k x} k^r \left[\frac{x}{k^r} \right] - (k-1) \sum_{1 \le r \le \log_k x} \left[\frac{x}{k^r} \right]$$

$$- (k-1) \sum_{1 \le r \le \log_k x} \left(x \left[\frac{x}{k^r} \right] - \frac{1}{2} \left[\frac{x}{k^r} \right]^2 k^r \right) \qquad (2)$$

Since

$$\sum_{1 \le r \le \log_k x} k^r \left[\frac{x}{k^r} \right] = x \left[\log_k x \right] + \sum_{1 \le r \le \log_k x} k^r \left(\left[\frac{x}{k^r} \right] - \frac{x}{k^r} \right)$$

$$= x \log_k x - \theta_1 x + \sum_{1 \le r \le \log_k x} k^r \left(\left[\frac{x}{k^r} \right] - \frac{x}{k^r} \right) \quad (0 \le \theta_1 \le 1)$$

$$\sum_{1 \le r \le \log_k x} \left(x \left[\frac{x}{k^r} \right] - \frac{1}{2} \left[\frac{x}{k^r} \right]^2 k^r \right) = \sum_{1 \le r \le \log_k x} \left(\frac{1}{2} \frac{x^2}{k^r} - \frac{1}{2} k^r \left(\left[\frac{x}{k^r} \right] - \frac{x}{k^r} \right)^2 \right)$$

$$= \frac{1}{2} x^2 \sum_{1 \le r \le \log_k x} \frac{1}{k^r} - \frac{1}{2} \sum_{1 \le r \le \log_k x} k^r \left(\left[\frac{x}{k^r} \right] - \frac{x}{k^r} \right)^2$$

(2) Change into the following

$$A(x) = \frac{1}{2} x(x+1) + \frac{k-1}{2} x \log_k x - \frac{k-1}{2} \theta_1 x - (k-1) \sum_{1 \le r \le \log_k x} \left[\frac{x}{k^r} \right]$$

$$- \frac{1}{2} \sum_{1 \le r \le \log_k x} \left(\left\{ \frac{x}{k^r} \right\} - \left\{ \frac{x}{k^r} \right\}^2 \right) k^r - \frac{k-1}{2} x^2 \sum_{1 \le r \le \log_k x} \frac{1}{k^r} \qquad (3)$$

It's easy to derive

$$\sum_{1\le r\le \log_K x}\left[\frac{x}{K^i}\right] = \theta_2\frac{x}{K-1} \qquad (0\le\theta_2\le 1)$$

$$\sum_{1\le r\le \log_K x}\left(\left\{\frac{x}{K^r}\right\}-\left\{\frac{x}{K^r}\right\}^2\right)K^i = \theta_3\frac{Kx}{4(K-1)} \qquad (0\le\theta_3\le 1)$$

Here we use the following: $0\le x-x^2\le\frac{1}{4}$ for $0\le x\le 1$.

$$x^2\sum_{1\le r\le \log_K x}\frac{1}{K^r} = \frac{x^2}{K-1} - \frac{1}{K-1}\frac{x^2}{K^{[\log_K x]}}$$

Therefore, notice (3), we obtain

$$A(x)=\frac{K-1}{2}\frac{x\log x}{\log K} - \left(\frac{K-1}{2}\theta_1+\theta_2-\frac{1}{2}+\frac{K}{8}\theta_3-\frac{1}{2}\frac{x}{K^{[\log_K x]}}\right)x$$

$$\triangleq \frac{K-1}{2}\frac{x\log x}{\log K}+\theta(x)\,x$$

where $-\frac{5K-4}{8}\le\theta(x)\le\frac{K+1}{2}$

I am greatly indebted to my tutor, Professor SHAO. Pingzong for instruction and suppling references.

References

[1] L. E. Bush. An asymptotic formula for the average sum of the digits of integers. Amer. Math. Monthly

47(1940) 154-156

[2] R. Bellman & H.N. Shapiro, On a problem in additive number theory, Ann. Math. Princeton II 49(1949) 333-340.

[3] L. Mirsky, A theorem on representations of integers in the scale of r. Scripta. Math. New York 15(1949) 11-12.

[4] CHEO Peh-Hsuin & Yien Sze-Chien, A problem on the k-adic representation of positive integers Acta Mathematia (Chinese edition) Vol 5 No. 4 (1955).

[5] H. Gupta. Selected topics in number theory. ABACUS Press (1980).

二项式系数中恰被某素数幂整除的个数

1985. 8. 10.

设 $\theta_j(n)$ 表示 $\binom{n}{0}\binom{n}{1}\cdots\binom{n}{n}$ 中恰被 p^j 整除的个数，p 为素数．又设 $n=c_0+c_1p+\cdots+c_rp^r$ $(0\le c_i<p)$．

1947 年 N. J. Fine 证明了

$$\theta_0(n)=(c_0+1)(c_1+1)\cdots(c_r+1).$$

其中 $\theta_0(n)$ 表示不能被 p 整除的 $\binom{n}{k}$ 的个数．

1967 年，L. Carlitz 证明了

$$\theta_1(n)=\sum_{k=0}^{r-1}(c_0+1)\cdots(c_{k-1}+1)(p-c_k-1)c_{k+1}(c_{k+2}+1)\cdots(c_r+1).$$

并对 $n=ap^r+bp^{r+1}$ $(0\le a<p,\ 0\le b<p)$

$$n=b+ap+ap^2+\cdots+ap^{r+j}\quad(0<a<p\text{，}b=a\text{ 或 }a-1)$$

给出了相应的公式．

1971 年，F. T. Harward 考虑了 $p=2$ 的情况，得出了相应的公式；

1973年，Harward又证明了

$$\theta_2(n)=\sum_{k=0}^{r-2}(p-c_k-1)(p-c_{k+1})c_{k+2}A_k +$$

$$+\sum_{m=k+2}^{r-1}\sum_{k=0}^{r-3}(p-c_k-1)c_{k+1}(p-c_m-1)c_{m+1}B_{k,m}.$$

其中 $A_k=\left[\prod_{i=1}^{r}(c_i+1)\right]/(c_k+1)(c_{k+1}+1)(c_{k+2}+1).$

$$B_{k,m}=\left[\prod_{i=1}^{r}(c_i+1)\right]/(c_k+1)(c_{k+1}+1)(c_m+1)(c_{m+1}+1)$$

同时对于 $n=ap^k+bp^r$ $(0<a<p,\ 0<b<p,\ k<r)$

$$n=c_1p^k+\cdots+c_mp^{k_m}\quad(0<c_i<p,\ j\le k_1,\ j\le k_{i+1}-k_i)$$

给出了计算公式。

本文考虑了一般的情况，给出了 $\theta_j(n)$ 的一般求法公式，并对于 $\theta_j(n)$ 的平均值给出了一个下界估计。

引理（Kummer）[5] 设 (1) $s=a_0+a_1p+\cdots+a_rp^r$, $(0\le a_i<p)$, (2) $n-s=b_0+b_1p+\cdots+b_rp^r$, $(0\le b_i<p)$.

(3) $a+b=c_0+\varepsilon_0p$, $\varepsilon_0+a_1+b_1=c_1+\varepsilon_1$, $\cdots$

$\varepsilon_{r-1}+a_r+b_r=c_r+\varepsilon_rp.$

其中 $\varepsilon_0=0$ 或 1，则 $\binom{n}{s}$ 中 p 的最高次幂

$\mathrm{pot}_p\left(\binom{n}{s}\right)=\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_r$. 易知 $\varepsilon_r=0$.

一. $\theta_j(n)$ 的求法

欲使 $\mathrm{pot}_p\left(\binom{n}{s}\right)=j$ 充分必要条件为 $\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_r=j$. 即 $\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_{r-1}=j$，这表明 $\varepsilon_0,\varepsilon_1,\cdots\varepsilon_{r-1}$ 中正好有 j 个取 1 而其余取 0. 设 $\varepsilon_{n_1}=\varepsilon_{n_2}=\cdots=\varepsilon_{n_j}=1$，设 $B(n_1,n_2,\cdots n_j)$ 表示 $\binom{n}{s}$ $(s=0,1,\cdots n)$ 中通过引理 (1)(2)(3) 过程得到的 $\varepsilon_0,\varepsilon_1,\cdots\varepsilon_{r-1}$ 中 $\varepsilon_{n_1}=\varepsilon_{n_2}=\cdots=\varepsilon_{n_j}=1$，而其余为 0 的 $\binom{n}{s}$ 的个数，则易知

$$\theta_j(n)=\sum_{0\le n_1<n_2<\cdots<n_j\le r-1}B(n_1,n_2,\cdots n_j) \qquad (1)$$

故只要求出 $B(n_1,n_2,\cdots n_j)$ 即可. 把 $n_1,n_2\cdots n_j$ 按相邻关系分成下列的组（不妨设为 k 组）

$n_1=m_1,m_1+1,\cdots m_1+l_1$；$m_2,m_2+1,\cdots,m_2+l_2$；$\cdots m_k,m_k+1,\cdots m_k+l_k=n_j$.

其中 $m_i > m_{i-1}+1$ $(2 \leq i \leq k)$

将 $\varepsilon_{n_1}=\varepsilon_{n_2}=\cdots=\varepsilon_{n_j}=1$，与其余 $\varepsilon_i=0$ 代入引理中(3)式即得一个方程

$$a_0+b_0=c_0 \qquad (1)'$$

$$\vdots \qquad \vdots$$

$$a_{m_1}+b_{m_1}=c_{m_1}+p \qquad (m_1)'$$

$$1+a_{m_1+1}+b_{m_1+1}=c_{m_1+1}+p \qquad (m_1+1)'$$

$$\vdots \qquad \vdots$$

$$1+a_{m_1+l_1+1}+b_{m_1+l_1+1}=c_{m_1+l_1+1} \qquad (m_1+l_1+1)'$$

$$a_{m_1+l_1+2}+b_{m_1+l_1+2}=c_{m_1+l_1+2} \qquad (m_1+l_1+2)'$$

$$\vdots \qquad \vdots$$

$$a_{m_2-1}+b_{m_2-1}=c_{m_2}-1 \qquad (m_2-1)'$$

$$a_{m_2}+b_{m_2}=c_{m_2}+p \qquad (m_2)'$$

$$\vdots \qquad \vdots$$

$$1+a_{m_2+l_2}+b_{m_2+l_2}=c_{m_2+l_2} \qquad (m_2+l_2)'$$

$$\vdots \qquad \vdots$$

$$a_{m_k}+b_{m_k}=c_{m_k}+p \qquad (m_k)'$$

$$1+a_{m_k+1}+b_{m_k+1}=c_{m_k+1}+p \qquad (m_k+1)'$$

$$\vdots \qquad \vdots$$

$$1+a_{m_k+l_k+1}+b_{m_k+l_k+1}=c_{m_k+l_k+1} \qquad (m_k+l_k+1)'$$

$$a_{m_k+l_k+2}+b_{m_k+l_k+2}=c_{m_k+l_k+2} \qquad (m_k+l_k+2)'$$

$$\vdots \qquad\qquad\qquad\qquad \vdots$$

$$a_{r-1} + b_{r-1} = c_{r-1} \qquad (r-1)'$$

$$a_r + b_r = c_r \qquad (r)'$$

易知这个方程组的解 $(a_0, a_1, \cdots a_r)$ 的个数即是 $\binom{n}{s}$ $(s=0,1,2,\cdots n)$ 中所求之个数 $B(n_1, n_2, \cdots n_j)$. 由方程组可以看出 $(a_0, a_1, \cdots a_r)$ 作为解时 $a_0, a_1, \cdots a_r$ 的取值是相互独立的。故由 $(1)'-(r')$ 中 $(1)'$ 易可得 a_0 有 (c_0+1) 种取法，由 $(2)'$ 知 a_1 有 (c_1+1) 种取法，… 由 $(m_1-1)'$ 知 a_{m_1-1} 有 $(c_{m_1-1}+1)$ 种取法，~~a_{m_1}~~ 由 $(m_1)'$ 知 a_{m_1} 有 $(p-c_{m_1}-1)$ 种取法，由 $(m_1+1)'$ 知 a_{m_1+1} 有 $(p-c_{m_1})$ 种取法，由 $(m_1+2)'$ 知 a_{m_1+2} 有 $(p-c_{m_1+2})$ 种取法，…… 由 $(m_1+l_1)'$ 知 $a_{m_1+l_1}$ 有 $(p-c_{m_1+l_1})$ 种取法，由 $(m_1+l_1+1)'$ 知，$a_{m_1+l_1+1}$ 有 $c_{m_1+l_1+1}$ 种取法，由 $(m_1+l_1+2)'$ 知 $a_{m_1+l_1+2}$ 有 $(c_{m_1+l_1+2}+1)$ 种取法（若 $m_2 \neq m_1+l_1+2$），…… a_{m_2-1} 有 $(c_{m_2-1}+1)$ 种取

法，a_{m_1} 有 $(p-c_{m_2}-1)$ 种取法，… $a_{m_2+l_2}$ 有 $(p-c_{m_2+l_2})$ 种取法，… 这样继续下去，当上述 $a_0, a_1, \cdots a_r$ 中各自选一个值构成的一组值乃组成之方程组的解. 于是

$$B(n_1,n_2,\cdots n_j)=(c_0+1)(c_1+1)\cdots(c_{m_1-1}+1)(p-c_{m_1}-1)\cdots$$

$$(p-c_{m_1}+1)\cdots(p-c_{m_1+l_1})c_{m_1+l_1+1}(c_{m_1+l_1+2}+1)\cdots(c_{m_2-1}+1)$$

$$(p-c_{m_2}-1)(p-c_{m_2})\cdots(p-c_{m_2+l_2})c_{m_2+l_2+1}(c_{m_2+l_2+2}+1)$$

$$\cdots(p-m_k-1)(p-c_{m_k+1})\cdots(p-c_{m_k+l_k})c_{m_k+l_k+1}\times$$

$$(c_{m_k+l_k+2}+1)\cdots(c_r+1)$$

$$=\left[\prod_{i=0}^{K}(c_i+1)\right]\left[\prod_{i=1}^{K}\frac{(p-c_{m_i}-1)(p-c_{m_i+1})\cdots(p-c_{m_i+l_i})c_{m_i+l_i+1}}{(c_{m_i}+1)(c_{m_i+1}+1)\cdots\cdots(c_{m_i+l_i}+1)(c_{m_i+l_i+1})}\right]$$

于是我们有

定理一

$$\theta_j(n)=\left[\prod_{i=0}^{K}(c_i+1)\right]\sum_{0\le n_1<n_2<\cdots<n_j\le r-1}\prod_{i=1}^{K}\frac{(p-c_{m_i}-1)(p-c_{m_i+1})\cdots(p-c_{m_i+l_i})c_{m_i+l_i+1}}{(c_{m_i}+1)(c_{m_i+1}+1)\cdots(c_{m_i+l_i}+1)(c_{m_i+l_i+1}+1)}.$$

其中 $(n_1,n_2\cdots n_j)=(m_1,m_1+1,\cdots m_1+l_1;\ m_2,m_2+1,\cdots m_2+l_2;\ \cdots$

$m_k,m_k+1,\cdots m_k+l_k)$， $m_{i+1}-m_i>1$ $(i=1,2,\cdots k-1)$.

推论 $$\theta_3(n)=\prod_{i=0}^{r}(c_i+1)\Big(\sum_{k=0}^{r-3}\frac{(p-c_k-1)(p-c_{k+1})(p-c_{k+2})c_{k+3}}{(c_k+1)(c_{k+1}+1)(c_{k+2}+1)(c_{k+3}+1)}$$

$$+\sum_{k=2}^{r-1}\sum_{m=0}^{k-2}\frac{(p-c_m-1)c_{m+1}(p-c_k-1)(p-c_{k+1})c_{k+2}}{(c_m+1)(c_{m+1}+1)(c_k+1)(c_{k+1}+1)(c_{k+2}+1)}+$$

$$+\sum_{k=2}^{r-4}\sum_{m=k+2}^{r-1}\frac{(p-c_k)(p-c_{k+1})c_{k+2}(p-c_m)c_{m+1}}{(c_k+1)(c_{k+1}+1)(c_{k+2}+1)(c_m+1)(c_{m+1}+1)}+$$

$$\sum_{2\le i+2<j+1<m\le r-1}\frac{(p-c_i-1)c_{i+1}(p-c_j-1)c_{j+1}(p-c_m-1)c_{m+1}}{(c_i+1)(c_{i+1}+1)(c_j+1)(c_{j+1}+1)(c_m+1)(c_{m+1}+1)}\Big).$$

注意，这些公式对于充分大的 n 与 p 是有效的，而且根据其规律性，可以在计算机上加以实现.（见二递推公式）.

二. $\theta_j(n)$ 的均值估计

命题 1. $\theta_j(p^n)=\varphi(p^j)$ $(n\geq j>0)$ $\theta_0(p^n)=2.$

证明. $j>0$ 欲使 $\mathrm{pot}_p\left(\binom{p^n}{l}\right)=n-\mathrm{pot}_p(l)=j \Longleftrightarrow$ $\mathrm{pot}_p(l)=n-j \Longleftrightarrow l=p^{n-j}r$，$p\nmid r$，故 l 的个数为 $\varphi(p^j)$ 个（$\Leftrightarrow$ 表示充分必要条件） 证毕.

对于 $\theta_j(n)$，我们有一个递推公式.

仍从一中的方程组出发，由 $(r)'$ 式，当

$\varepsilon_{r-1}=0$ 时，a_r 有(c_r+1)种取法．而$(a_0,\cdots a_{r-1})$有$\theta_j(n-c_rp^r)$种取法；故当$\varepsilon_{r-1}=0$时，$(a_0,a_1,\cdots a_r)$共有$(c_r+1)\theta_j(n-c_rp^r)$种取法；当$\varepsilon_{r-1}=0$时．而$\varepsilon_{r-2}=0$时，$a_r$有$c_r$种取法，$a_{r-1}$有$(p-c_{r-1}-1)$种取法，而$(a_0,a_1,\cdots a_{r-2})$共有$\theta_{j-1}(n-c_rp^r-c_{r-1}p^{r-1})$种取法，这样$(a_0,\cdots a_r)$共有

$$c_r(p-c_{r-1}-1)\theta_{j-1}(n-c_rp^r-c_{r-1}p^{r-1}),\cdots$$

这个步骤继续下去，便有

命题 2. $\theta_j(n)=(c_r+1)\theta_j(n-c_rp^r)$

$$+c_r(p-c_{r-1}-1)\theta_{j-1}(n-c_rp^r-c_{r-1}p^{r-1})+$$

$$+c_r(p-c_{r-1})(p-c_{r-2}-1)\theta_{j-2}(n-c_rp^r-c_{r-1}p^{r-1}-c_{r-2}p^{r-2})$$

$$+\cdots+c_r(p-c_{r-1})\cdots(p-c_{r-j+1})(p-c_{r-j}-1)\theta_0(n-c_rp^r$$

$$-\cdots-c_{r-j}p^{r-j}).$$

定义 $\Delta_j(x)=\sum_{n\leq x}\theta_j(n)$．我们有

定理二. $\lim_{n\to\infty}\frac{\Delta_j(x)}{x^{\log_p(p(p+1)/2)}}\geq\frac{\varphi(p^j)}{[\frac{p(p+1)}{2}]^{j+1}}$.

证明. 由命题二可知, 当 $n>j$ 时.

$$\theta_j(ap^n+b) \geqslant (a+1)\theta_j(b) \quad (0<a\leqslant p,\ b<p^n).$$

于是 $(n>j)$

$$\Delta_j(p^n) = \sum_{0\leq l<p^{n-1}} \theta_j(l) + \sum_{p^{n-1}\leq l<2p^{n-1}} \theta_j(l) + \cdots$$

$$+\sum_{(p-1)p^{n-1}\leq l<p^n} \theta_j(l) + \theta_j(p^n)$$

$$= \sum_{0\leq l<p^{n-1}} \theta_j(l) + \sum_{0\leq l<p^{n-1}} \theta_j(p^{n-1}+l) + \cdots$$

$$+ \sum_{0\leq l<p^{n-1}} \theta_j((p-1)p^{n-1}+l) + \theta_j(p^n)$$

$$\geqslant \sum_{0\leq l<p^{n-1}} + 2\sum_{0\leq l<p^{n-1}} \theta_j(l) + \cdots + p\sum_{0\leq l<p^{n-1}} \theta_j(l)$$

$$+ \theta_j(p^n)$$

$$= \frac{p(p+1)}{2} \sum_{0\leq l\leq p^{n-1}} \theta_j(l) + \theta_j(p^n)$$

$$\geqslant \frac{p(p+1)}{2} \sum_{0\leq l\leq p^{n-1}} \theta_j(l) - \frac{p(p+1)}{2}\theta_j(p^{n-1}).$$

由命题1 可证: $\theta_j(p^n) = \varphi(p^j) \quad (n\geqslant j)$

于是我们有

$$\Delta_j(p^n) \geqslant \frac{p(p+1)}{2} \sum_{0\leq l\leq p^{n-1}} \theta_j(l) - \frac{p(p+1)}{2}\varphi(p^j)$$

$$= \frac{p(p+1)}{2} \Delta_j(p^{n-1}) - \frac{p(p+1)}{2}\varphi(p^j).$$

当 $p^n \leq x < p^{n+1}$ 时 则 $n \leq \log_p x \leq n+1$

因而

$$\Delta_j(x) \geqslant \Delta_j(p^n) \geqslant \frac{p(p+1)}{2} \Delta_j(p^{n-1}) - \frac{p(p+1)}{2} \varphi(p^j)$$

$$\geqslant \cdots \geqslant \left[\frac{p(p+1)}{2}\right]^{n-j} \Delta_j(p^j) - (n-j) \frac{p(p+1)}{2} \varphi(p^j)$$

$$= \left[\frac{p(p+1)}{2}\right]^{n+1} \frac{\Delta_j(p^j)}{\left(\frac{p(p+1)}{2}\right)^{j+1}} - (n-j) \frac{p(p+1)}{2} \varphi(p^j)$$

$$\geqslant \left(\frac{p(p+1)}{2}\right)^{\log_p x} \frac{\Delta_j(p^j)}{\left(\frac{p(p+1)}{2}\right)^{j+1}} - (\log_p x - (j+1)) \frac{p(p+1)}{2} \varphi(p^j)$$

$$\geqslant x^{\log_p\left(\frac{p(p+1)}{2}\right)} \frac{\Delta_j(p^j)}{\left(\frac{p(p+1)}{2}\right)^{j+1}} - (\log_p x - (j+1)) \frac{p(p+1)}{2} \varphi(p^j) \qquad (*)$$

于是有

$$\underline{\lim}_{x \to \infty} \frac{\Delta_j(x)}{\left(\frac{p(p+1)}{2}\right)^{\log_p x}} \geqslant \frac{\Delta_j(p^j)}{\left(\frac{p(p+1)}{2}\right)^{j+1}} \geqslant \frac{\theta_j(p^j)}{\left(\frac{p(p+1)}{2}\right)^{j+1}} = \frac{\varphi(p^j)}{\left(\frac{p(p+1)}{2}\right)^{j+1}}$$

事实上，我们得到的是比此极限不等式更好的 $\Delta_j(x)$ 的估计式(*).

我猜测 $\Delta_j(x) = O\left(x^{\log_p\left(\frac{p(p+1)}{2}\right)}\right)$，其中所含的常数与 p, j 有关. 在[6]中，对 $j=0$, $p=2$ 时，本文已证明这是对的，实际上得到是 $\Delta_0(x) \leq 3x^{\log_2 3}$. 对于 $j=0$, p 为素数时，由[1]很容易推知猜测成立.

下面的结果更使我们的猜测是成立.

定理三. $\overline{\lim_{x\to\infty}} \Delta_1(x)/x^{\log_p\frac{p(p+1)}{2}}\log_p x \leq \left(\frac{p-1}{p+1}\right)^2\left(\frac{p(p+1)}{2}+2\right)$.

证明 由命题已可知

$$\theta_1(n)=(C_r+1)\theta_1(n-C_rp^r)+C_r(p-C_{r-1}-1)\theta_0(n-C_rp^r-C_{r-1}p$$

于是 当 $n>2$ 时

$$\Delta_1(p^n)=\sum_{j\leq p^n}\theta_1(j)=\sum_{j<p^{n-1}}(\theta_1(j)+\theta_1(p^{n-1}+j)+\cdots+\theta_1((p-1)p^{n-1}+j)$$

$$+\theta_1(p^n)$$

$$\leq\frac{p(p+1)}{2}\Delta_1(p^{n-1})+\theta_1(p^n)+\frac{p(p-1)}{2}\sum_{\substack{j<p^{n-1}\\ j=lp^{n-2}+k\\ 0\leq l\leq p-1,\,k<p^{n-2}}}(p-l-1)\theta_0(k)$$

$$\leq\frac{p(p+1)}{2}\Delta_1(p^{n-1})+\theta_1(p^n)+\frac{p(p-1)}{2}\left(\sum_{l=0}^{p-1}(p-l-1)\right)\left(\sum_{k\leq p^{n-2}}\theta_0(k)\right)$$

$$=\frac{p(p+1)}{2}\Delta_1(p^{n-1})+\varphi(p)+\left(\frac{p(p-1)}{2}\right)^2\Delta_0(p^{n-2})$$

由此递推公式可得

$$\Delta_1(p^n)\leq\left(\frac{p(p+1)}{2}\right)^{n-2}\Delta_1(p^2)+\left(\frac{p(p+1)}{2}\right)^{n-3}\varphi(p)$$

$$+\left(\frac{p(p+1)}{2}\right)^{n-4}\varphi(p)+\cdots+\varphi(p)$$

$$+\left(\frac{p(p+1)}{2}\right)^{n-3}\left(\frac{p(p-1)}{2}\right)^2\Delta_0(p)+\left(\frac{p(p+1)}{2}\right)^{n-4}\left(\frac{p(p-1)}{2}\right)^2\Delta_0(p^2)$$

$$+\cdots+\left(\frac{p(p+1)}{2}\right)\left(\frac{p(p-1)}{2}\right)^2\Delta_0(p^{n-3})+\left(\frac{p(p-1)}{2}\right)^2\Delta_0(p^{n-2}). \qquad (2)$$

同上述处理方法，可得

$$\Delta_{\varphi}(p^2)=\sum_{j<p}\left(\theta_1(j)+\theta_1(p+j)+\cdots+\theta_1((p-1)p+j)\right)+\theta_1(p^2)$$

$$=\sum_{j<p}\left(1\cdot(p-j-1)+2(p-j-1)+\cdots+(p-1)(p-j-1)\right]+\varphi(p)$$

$$=\frac{p(p-1)}{2}\sum_{j<p}(p-j-1)+\varphi(p)=\left(\frac{p(p-1)}{2}\right)^2+\varphi(p)$$

注意上面用到了 $\theta_1(lp+j)=l(p-j-1)$（其中 $0<l\leq p-1$，$0\leq j\leq p-1$），这可由一中方程组推知.

$$\Delta_0(p^n)=\sum_{j<p^{n-1}}\left(\theta_0(j)+\theta_0(p^{n-1}+j)+\cdots+\theta_0((p-1)p^{n-1}+j)\right)$$

$$+\theta_0(p^n)$$

$$=\sum_{j<p^{n-1}}\theta_0(j)(1+2+\cdots+p)+2$$

$$=\frac{p(p+1)}{2}\sum_{j\leq p^{n-1}}\theta_0(j)-p(p+1)+2$$

$$\leq\frac{p(p+1)}{2}\Delta_0(p^{n-1}) \qquad (n>1)$$

故 $\Delta_0(p^n)\leq\left(\frac{p(p+1)}{2}\right)^{n-1}\Delta_0(p)$.

代入(2)可知

$$\Delta_1(p^n)\leq\left(\frac{p(p+1)}{2}\right)^{n-2}\left(\frac{p(p-1)}{2}\right)^2+\varphi(p)\left(\left(\frac{p(p+1)}{2}\right)^{n-2}+\left(\frac{p(p+1)}{2}\right)^{n-3}+\right.$$

$$+\cdots+\frac{p(p+1)}{2}+1\Big)+\left(\frac{p(p-1)}{2}\right)^2\Big[\Delta_0(p)\left(\frac{p(p+1)}{2}\right)^{n-3}+\left(\frac{p(p+1)}{2}\right)^{n-4}\Delta_0(p^2)$$

$$+\cdots+\Delta_0(p^{n-2})\Big]$$

$$\leqslant\left(\frac{p(p+1)}{2}\right)^{n-2}\left(\frac{p(p-1)}{2}\right)^2+\varphi(p)\left[\left(\frac{p(p+1)}{2}\right)^{n-1}-1\right]\Big/\frac{p(p+1)}{2}-1$$

$$+\left(\frac{p(p-1)}{2}\right)^2(n-2)\,\Delta_0(p)\left(\frac{p(p+1)}{2}\right)^{n-3}\qquad(3)$$

设 $p^n\leqslant x<p^{n+1}$，则 $n\leqslant\log_p x$．由 (3) 可知．

$$\Delta_1(x)\leqslant\Delta_1(p^{n+1})\leqslant\left(\frac{p(p+1)}{2}\right)^{n-1}\left(\frac{p(p-1)}{2}\right)^2$$

$$+\varphi(p)\left[\left(\frac{p(p+1)}{2}\right)^{n}-1\right]\Big/\frac{p(p+1)}{2}-1$$

$$+\left(\frac{p(p-1)}{2}\right)^2(n-1)\;\Delta_0(p)\left(\frac{p(p+1)}{2}\right)^{n-2}$$

$$\leqslant\left(\frac{p(p+1)}{2}\right)^{n-1}\left(\frac{p(p-1)}{2}\right)^2+\varphi(p)\left[\left(\frac{p(p+1)}{2}\right)^{n}-1\right]\Big/\frac{p(p+1)}{2}-1$$

$$+\left(\frac{p-1}{p+1}\right)^2\Delta_0(p)\left(\frac{p(p+1)}{2}\right)^{\cancel{\log x}\log_p x}$$

$$=\left(\frac{p(p+1)}{2}\right)^{n-1}\left(\frac{p(p-1)}{2}\right)^2+\varphi(p)\left[\left(\frac{p(p+1)}{2}\right)^{n}-1\right]\Big/\frac{p(p+1)}{2}-1$$

$$+\left(\frac{p-1}{p+1}\right)^2\Delta_0(p)\;x^{\log_p\frac{p(p+1)}{2}}\log_p x$$

于是

$$\overline{\lim_{x\to\infty}}\ \Delta_1(x)\Big/x^{\log_p\frac{p(p+1)}{2}}\log_p x \leqslant \left(\frac{p-1}{p+1}\right)^2\Delta_0(p)$$

$$=\left(\frac{p-1}{p+1}\right)^2\left(\frac{p(p+1)}{2}+2\right).$$

这就完成了定理三的证明.

上定理说明，$\Delta_1(x)=O\left(x^{\log_p\left(\frac{p(p+1)}{2}\right)}\log_p x\right)$，若能把 $\log_p x$ 去掉，则也说明猜测在 $j=1$ 的情况下成立. 对于 $j\geq 2$ 的情况，应用上述方法似乎不实用，由此而出的估计并不能逼近到此猜测的程度.

记 $A_0=\log_p\left(\left(\frac{p(p+1)}{2}\right)\right)$，$A_j(n)=\Delta_j(n)/n^{A_0}$，则有

$$\left|A_j(n)-A_j(n+1)\right|\leqslant\frac{\Delta_j(n+1)-\Delta_j(n)}{n^{A_0}}+\Delta_j(n+1)\left(\frac{1}{n^{A_0}}-\frac{1}{(n+1)^{A_0}}\right)$$

$$\leqslant\frac{n}{n^{A_0}}+\Delta_j(n+1)\cdot\frac{1}{(n+1)^{A_0}}\left[\left(1+\frac{1}{n}\right)^{A_0}-1\right]$$

$$=\frac{1}{n^{A_0-1}}+\frac{(n+1)(n+2)}{2}\cdot\frac{1}{(n+1)^{A_0}}\left(\frac{A_0}{n}+O\left(\frac{1}{n^2}\right)\right)$$

$$=\frac{1}{n^{A_0-1}}+\frac{(n+1)(n+2)}{2}\cdot O\left(\frac{1}{n^{1+A_0}}\right)\longrightarrow 0\ (n\to\infty).\ (\because A_0>1).$$

这说明 $\{A_j(n)\}$ 与其上极限与下极限的关系.

等.

记 $\alpha = \varliminf_{x\to\infty} \Delta_j(x) / x^{\log_p(\frac{p(p+1)}{2})}$

$\beta = \varlimsup_{x\to\infty} \Delta_j(x) / x^{\log_p(\frac{p(p+1)}{2})}$.

又怎样对 α, β 作出估计呢？有待研究.

参考文献

[1] N. J. Fine, Binomial cofficients modulo a prime, Amer. Math. Monthly. 54(1947).

[2] L. Carlitz. The number of binomial cofficients divisible by a fixed power of a prime. Rend. Circ. Mat. Palermo (2) 16(1967) 299-320 MR. 40 # 2554

[3] F. T. Harward. The number of binomial cofficients divisible by a fixed power of 2. Proc. Amer.

Math. Soc. 29(1971) 236-242.

[4] F. T. Harward, Formulas for the number of binomial coefficients divisible by a fixed power of a prime. Proc. Amer. Math. Soc. 37(1973).

[5] L. E. Dickson, History of the theory of numbers Vol. 1. Publication no. 256, Carnegie Institution of Washington, D.C. 1919.

[6] 方玉光，杨辉三角形中奇数的分布。

杨辉三角形中奇数的分布

1985. 4. 25.

在文献[1]中，R. Honsberger 把下述结果称为组合与数论中三个奇妙结果之一：$\binom{n}{0},\binom{n}{1},\cdots\binom{n}{n}$ 中有 2 的某个幂次个奇数，并指出其证明比较复杂。文[2]中虽然给出了其证明用到了 Lucas 恒等式及同余式的知识，本文只用整数的整除性的知识不仅给出更强的结果且证明比较简单，而且对于杨辉三角形中奇数的分布作出了估计。

§1 $\binom{n}{0}$ $\binom{n}{1},\cdots\binom{n}{n}$ 中奇数的个数

定理一 设 $n=2^{n_1}+2^{n_2}+\cdots+2^{n_t}$，其中 $n_1>n_2>n_3>\cdots>n_t\geq 0$. 则 $\binom{n}{0},\binom{n}{1},\cdots\binom{n}{n}$ 中有 2^t 个奇数.

先证明两个引理，而其本身也具有其趣味性.

引理1. 设 p 为素数，$0\leq m<p^r$，则有

$\mathrm{pot}_p\left(\binom{p^r+m}{l}\right) = \mathrm{pot}_p\left(\binom{m}{l}\right)$ 对一切 $0\le l\le m$ 成立. 其中 $\mathrm{pot}_p(x)$ 表示 $p^{\mathrm{pot}_p(x)} \mid x$, 但 $p^{\mathrm{pot}_p(x)+1} \nmid x$.

证明 $\mathrm{pot}_p\left(\binom{p^r+m}{l}\right) = \sum_{k=1}^{r}\left(\left[\frac{p^r+m}{p^k}\right] - \left[\frac{l}{p^k}\right] - \left[\frac{p^r+m-l}{p^k}\right]\right)$

$= \sum_{k=1}^{r}\left(p^{r-k} + \left[\frac{m}{p^k}\right] - \left[\frac{l}{p^k}\right] - p^{r-k} - \left[\frac{m-l}{p^k}\right]\right)$

$= \sum_{k=1}^{r}\left(\left[\frac{m}{p^k}\right] - \left[\frac{l}{p^k}\right] - \left[\frac{m-l}{p^k}\right]\right) = \mathrm{pot}_p\left(\binom{m}{l}\right)$

引理2. 当 $m<l<2^k$ 时, $2 \mid \binom{2^k+m}{l}$ $(0\le m<2^k)$

证明 $\mathrm{pot}_p\left(\binom{2^k+m}{l}\right) = \sum_{r=1}^{k}\left(\left[\frac{2^k+m}{2^r}\right] - \left[\frac{l}{2^r}\right] - \left[\frac{2^k+m-l}{2^r}\right]\right)$

$\geqslant \left[\frac{2^k+m}{2^k}\right] - \left[\frac{l}{2^k}\right] - \left[\frac{2^k+m-l}{2^k}\right] = 1$, 只要注意到 $l<2^k$, $2^k+m-l<2^k$ 即可得证. 故 $2 \mid \binom{2^k+m}{l}$

这就完成了引理证明.

设 $\delta(n) = \begin{cases} 0 & 2\mid n \\ 1 & 2\nmid n \end{cases}$ $\Delta(n) = \sum_{k\le n}\delta\left(\binom{n}{k}\right)$

定理一的证明 注意到 $\Delta(n)$ 即 $\binom{n}{0}, \binom{n}{1}, \cdots \binom{n}{n}$ 中奇数的个数, 且由引理一知:

$\delta\left(\binom{2^k+m}{l}\right) = \delta\left(\binom{m}{l}\right)$ 对一切 $0\le m<2^k$, $0\le l\le m$ 成

立，即有

$$\Delta(2^k+m) = \sum_{l\le m}\delta\left(\left(\binom{2^k+m}{l}\right)\right) + \sum_{l\ge 2^k}\delta\left(\left(\binom{2^k+m}{l}\right)\right)$$

$$+\sum_{m<l<2^k}\delta\left(\left(\binom{2^k+m}{l}\right)\right)$$

$$= 2\sum_{l\le m}\delta\left(\left(\binom{m}{l}\right)\right) = 2\Delta(m)$$

对于 $n=2^{n_1}+2^{n_2}+\cdots+2^{n_t}$，$n_1>n_2>\cdots>n_t\ge 0.$，有

$$\Delta(n) = 2\Delta(2^{n_2}+\cdots+2^{n_t}) = \cdots = 2^{t-1}\Delta(2^{n_t}) = 2^t.$$

§2. 定理 = 设 $f(x)=\sum_{n\le x}\Delta(n)$ 则

$$\frac{1}{3} < f(x)/x^{\log_2 3} \le 3.$$

证明 对于 $k\ge 1$，$f(2^k-1) = f(2^{k-1}+2^{k-2}+\cdots+1)$

$$= f(2^{k-2}+2^{k-3}+\cdots+1) + \sum_{n\le 2^{k-1}-1}\Delta(2^{k-1}+n)$$

$$= f(2^{k-2}+2^{k-3}+\cdots+1) + 2\sum_{n\le 2^{k-1}-1}\Delta(n)$$

$$= 3f(2^{k-1}+1) = \cdots = 3^k f(0) = 3^k.$$

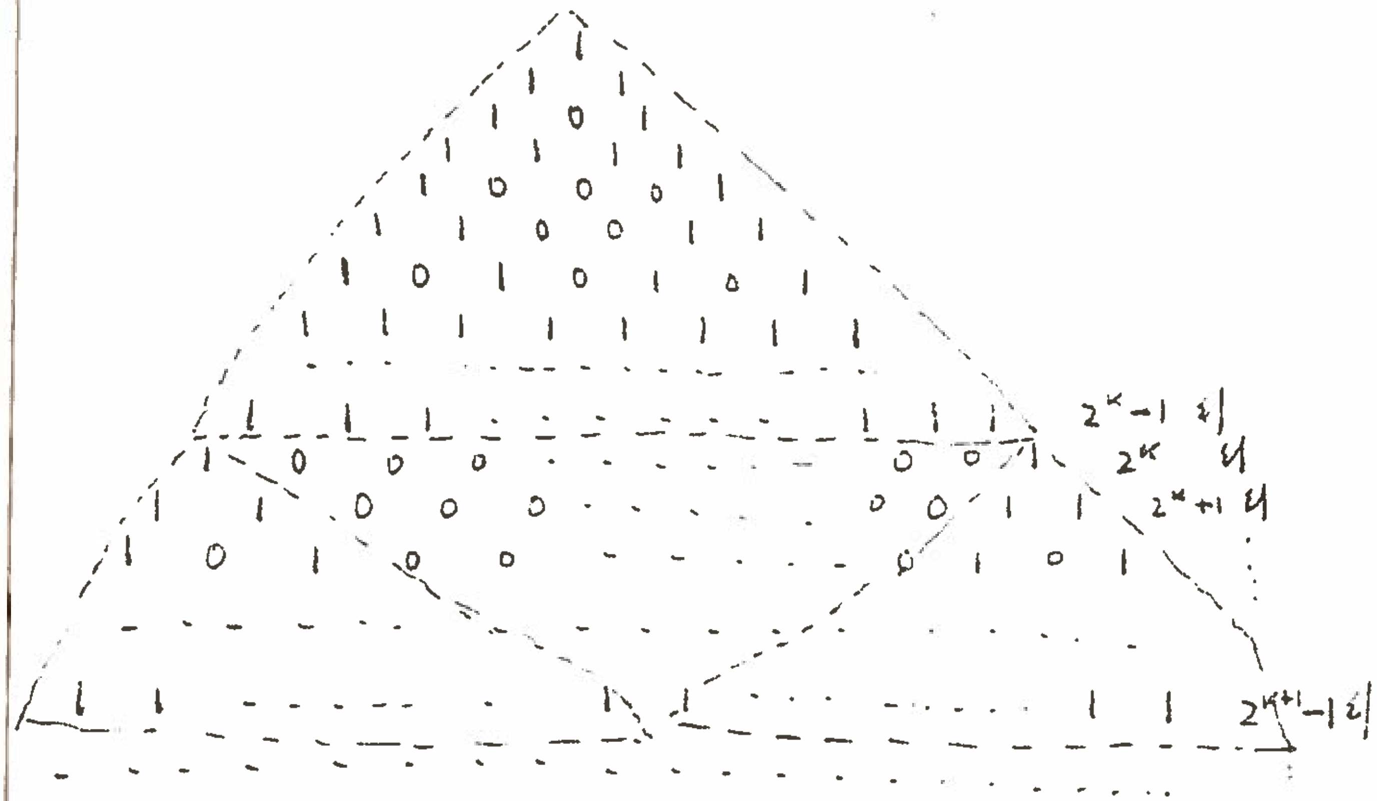
假设 $2^k\le x<2^{k+1}$ (*)

则有 $k\le \log_2 x<k+1$，$f(2^k-1)\le f(x)\le f(2^{k+1}-1)$，

即 $3^k\le f(x)\le 3^{k+1}$.

再由用(*)即得 $\frac{1}{3}\le f(x)/x^{\log_2 3}\le 3$.

定理一与定理二有一个几何说明，而使得上述证明明朗化。在杨辉三角形中关于 mod 2 作出相应的一个三角形，凡同余于 0 的数记为 0，凡余 1 的数记为 1，从并且利用 $\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k}$ 记 0+1=1，0+0=0，1+1=0 之运算法则即为：



从图中可以看出：当 $n=2^k-1$ 时，$\binom{n}{0},\binom{n}{1},\cdots\binom{n}{n}$

全部为1，在 $2^{k}-1$ 与 2^{k+1} 之间有两个全等三角形，故由生成规律可知它与 2^k-1 以上的三角形是完全相等的。因此才有定理二中的 $f(2^k-1)=3f(2^{k-1}-1)$ 等式的存在。而又由其对称性，故有定理一之2的第次的出现。

另由 $m_k=2^k$ 与 $m_k=3\cdot 2^{k-1}-2$ 知 $f(m)/m^{\log_2 3}$ 在 $m\to\infty$ 时极限不存在。设 $\alpha=\varliminf\limits_{n\to\infty} f(n)/n^{\log_2 3}$.

$\beta=\varlimsup\limits_{n\to\infty} f(n)/n^{\log_2 3}$.

我们有

定理三. 序列 $\{f(n)/n^{\log_2 3}\}$ 在 $[\alpha,\beta]$ 之间稠密的.

证明. 记 $A(n)=f(n)/n^{\log_2 3}$，只要证明 $A(n)-A(n+1)\to 0$ $(n\to\infty)$. 由 $f(n)$ 的定义可知 $f(n+1)-f(n)\le n+1$，于是

$$|A(n)-A(n+1)| = \left|\frac{f(n)}{n^{\log_2 3}} - \frac{f(n+1)}{n^{\log_2 3}}\right| \le$$

$$\leq f(n)\left|\frac{1}{n^{\log_2 3}}-\frac{1}{(n+1)^{\log_2 3}}\right|+\frac{f(n+1)-f(n)}{(n+1)^{\log_2 3}}$$

$$\leq 3\left[\left(1+\frac{1}{n}\right)^{\log_2 3}-1\right]+\frac{1}{(n+1)^{\log_2 3}}\longrightarrow 0 \quad (n\to\infty).$$

因此 $A(n)$ 在 $[\alpha,\beta]$ 内稠密. ||

另由定理二可知 $\alpha\geq\frac{1}{3}$，及 $\beta\leq 3$，现在的问题是怎样去得到 α,β 的更好的估计，尚待研究！

对于 $\Delta(n)$ 的均值不易研究，现在考其对数均值的情况，我们有：

定理四 $\sum\limits_{n\leq x}\log\Delta(n)=\frac{1}{2}x\log x+\theta(x)x$，其中 $-\frac{3}{4}\log 2\leq\theta(x)\leq\frac{3}{2}\log 2$.

我们在[3]已证明：

引理3 设 $x=a_1k^{n_1}+a_2k^{n_2}+\cdots+a_tk^{n_t}$，其中 $n_1>n_2>\cdots>n_t\geq 0$，k为不小于1的自然数，$a_1,a_2\cdots a_t$ 为不大于 $k-1$ 的非负整数，记 $\alpha(x)=\sum\limits_{i=1}^{t}a_i$，$A(x)=\sum\limits_{n\leq x}\alpha(n)$，则 $A(x)=\frac{k-1}{2}\frac{x\log x}{\log k}+\theta(x)x$

其中 $-\frac{5k-4}{8} \le \theta(x) \le \frac{k+1}{2}$.

定理的证明　若 $n = 2^{n_1} + 2^{n_2} + \cdots + 2^{n_t}$, $n_1 > n_2 > \cdots > n_t \ge 0$

则 $\alpha(n) = t$. 从而 $\Delta(n) = 2^{\alpha(n)}$. 故

$$\sum_{n \le x} \log \Delta(n) = \log 2 \sum_{n \le x} \alpha(n) = \log 2 \cdot A(x)$$

由引理3中 $k=2$ 的情况可知

$$\sum_{n \le x} \log \Delta(n) = \log 2 \left(\frac{x \log x}{2 \log 2} + \theta_1(x)\, x \right)$$

$$= \frac{1}{2} x \log x + (\theta_1(x) \log 2)\, x \triangleq \frac{1}{2} x \log x + \theta(x)\, x.$$

其中　$-\frac{3}{4}\log 2 \le \theta(x) \le \frac{3}{2} \log 2$.　完成定理四的证明.

对于 $f(x)$, 我们还有

定理五　设 $x = 2^{x_1} + 2^{x_2} + \cdots + 2^{x_k}$, 其中

$x_1 > x_2 > \cdots > x_k \ge 0$. $B_i(x)$ 表示不大于 x 的 $\alpha(n) = i$ 的解的个数. 则 $f(x) = \sum_{i=0}^{x_1} 2^i B_i(x)$, 且 $x_1 = \left[\frac{\log x}{\log 2} \right]$.

证明　$f(x) = \sum_{n \le x} \Delta(n) = \sum_{n \le x} 2^{\alpha(n)} = \sum_{i=0}^{x_1} \sum_{\alpha(n)=i} 2^i$

$= \sum_{i=0}^{x_1} 2^i \sum_{\alpha(n)=i} 1 = \sum_{i=0}^{x_1} 2^i B_i(x)$. 由 $x = 2^{x_1} + 2^{x_2} + \cdots + 2^{x_k}$

知　$x_1 = \left[\frac{\log x}{\log 2} \right]$.

参考文献

[1] R. Honsberger, Three surprising results in combinatorial analysis and number theory, Mathematical Germs II.

[2] N. J. Fine, Binomial confficients modulo a prime. Amer. Math. Monthly. 54(1947) 589-592.

[3] 方玉光. 关于正整数k进位表示中的一个定理.

[4] 周伯壎与尹士健. 关于k进位表示中数的一个问题. 数学学报. 第五卷第四期, 1955年12月.

[5] 华罗庚. 数论导引 pp.15. 科学出版社 (1975).

整数分拆中一个条件极值问题

1985. 3.

设n为一个正整数，若 $n=a_1+a_2+\cdots+a_k$，其中 $a_1,a_2\cdots a_k$ 皆为正整数，则称 $\{a_1,a_2\ldots a_k\}$ 为n的一个分拆(partition)。数论中一个饶有风趣的问题就是处理分拆函数 $p(n)$ 及 $P_r(n)$ 问题。周知：

$$\lim_{n\to\infty}\frac{\log p(n)}{n^{\frac{1}{2}}}=\pi\sqrt{\frac{2}{3}}$$ （见[1]）。这说明当n充分大时，n的分拆数变得很大。即下集合

$$A(n)=\{(a_1,a_2\cdots a_k):\ n=a_1+a_2+\cdots+a_k,\ a_i>0,\ i=1,2\cdots k;\ k=1,2,\cdots\}$$

的元素有很多。记 $p(a_1\cdots a_k)=a_1a_2\cdots a_k$，现在要问 $p(A(n))\triangleq\max\limits_{a\in A(n)}p(a)$ 为多少呢？又当 $A(n)$ 中当k为固定值时，它的元素各分量乘积的最大与最小值又为多少？本文就是处理这一类问题。

首先，我们有下述结果：

定理一. 把n进行任意分拆，得到 $A(n)$，则

$$P(A(n))=\max_{(a_1,\cdots a_k)\in A(n)} a_1a_2\cdots a_k=\begin{cases}3^l & \text{当 } n=3l \text{ 时}\\ 4\times 3^{l-1} & \text{当 } n=3l+1 \text{ 时}\\ 2\cdot 3^l & \text{当 } n=3l+2\end{cases}$$

证明：设 $n=a_1+a_2+\cdots+a_k$ 是使得 $P(A(n))=a_1a_2\cdots a_k$ 的一个分拆.

若 a_i 中有一个大于4，不妨设 $a_1>4$，作这样一个分拆 $n=2+(a_1-2)+a_2+\cdots+a_k$，于是

$P(2, a_1-2, a_2,\cdots a_k)=2(a_1-2)a_2\cdots a_k=2a_1a_2\cdots a_k-4a_2\cdots a_k$

$=P(A(n))+(a_1-4)a_2\cdots a_k>P(A(n))$，这与 $P(A(n))$ 定义矛盾。

若 a_i 中有一个取1，不妨设 $a_1=1$. 则作下述分拆 $n=(1+a_2)+a_3+\cdots+a_k$，于是

$P(1+a_2, a_3,\cdots a_k)=(1+a_2)a_3\cdots a_k=P(A(n))+a_2a_3\cdots a_k>P(A(n))$

又产生矛盾.

因此欲使 $P(A(n))=a_1a_2\cdots a_k$ 最大，$\{a_i\}$ 必取2或3.

令 $P(A(n))=2^m3^l$.

又若 $\{a_i\}$ 中含有不少于 3 个 2 即 $m\geq 3$，则由 $2+2+2=3+3$ 可知，$2\times2\times2<3\times3$ 可知 $a_1\cdots a_k$ 亦不会达最大，因此必有 $m=0,1,2$.

因此，当 $n=3l$ 时，$m=0$，故 $p(A(n))=3^l$.

当 $n=3l+1$ 时，$m=2$，故 $p(A(n))=4\times3^{l-1}$.

当 $n=3l+2$ 时，$m=1$，故 $p(A(n))=2\cdot3^l$. 证毕.

下面我们着重考虑那些具有 k 个元素的分析（k 为固定的整数）. 记 $P(k,n)$ 表示下列集合的元素的个数（k 暂时固定）.

$$A(k,n)=\{(a_1,\cdots a_k):n=a_1+a_2+\cdots+a_k\ ,\ a_i>0.\ i=1,2\cdots k\}.$$

显然 当 $n>k$ 时，$p(k,n)\geq 2$.

记
$$p_M(A(k,n))=\max_{(a_1,\cdots a_k)\in A(k,n)} a_1a_2\cdots a_k$$

$$P_m(A(k,m))=\min_{(a_1,\cdots a_k)\in A(k,n)} a_1a_2\cdots a_k$$

$$d=\left[\frac{n}{k}\right]\ ,\ n=dk+r\ ,\qquad 0\leq r<k.$$

对于 P_M 与 P_m，我们有.

定理二. $P_M(A(k,n)) = d^{k-r}(d+1)^r$. (1)

$P_m(A(k,n)) = n-k$. (2)

证明. 先证明 (1):

设 $n = a_1+a_2+\cdots+a_k = kd+r$，使得 $P_M(A(k,n)) = a_1a_2\cdots a_k$

若 $\{a_i\}$ 中有一个小于 d，不妨 $a_1<d$，又若 $a_2, a_3, \cdots a_n$ 皆不大于 $d+1$. 则不妨设 $a_2, a_3, \cdots a_l$ 皆小于 d，于是

$$p((a_1,a_2,\cdots a_k)) = a_1a_2\cdots a_k = a_1a_2\cdots a_l\, d^i (d+1)^j$$

记 $a_1 = d-p_1$，$\cdots$ $a_l = d-p_l$，则由于

$$a_1+a_2+\cdots+a_k = (d-p_1)+\cdots+(d-p_l)+id+j(d+1) = kd+r$$

即: $(l+j+i)d+j-p_1-\cdots-p_l = kd+r$

而 $l+j+i=k$. 故 $p_1+p_2+\cdots+p_l = j-r>0$

又对于 $m>0$，有 $(d-m)(d+1)<(d-m+1)d$. 于是 $p(a_1,\cdots a_k) = (d-p_1)(d-p_2)\cdots(d-p_l)\,d^i(d+1)^j$

$$= (d-p_1)(d-p_2)\cdots(d-p_l)\,d^i\,(d+1)^{p_1+p_2+\cdots+p_l}(d+1)^r$$

$$=[(d-p_1)(d+1)^{p_1}]\cdots[(d-p_l)(d+1)^{p_l}]\,d^i(d+1)^r \qquad (3)$$

由于 $(d-p_i)(d+1)^{p_i} < (d-p_i+1)(d+1)^{p_i-1}d$

$$< \cdots < d^{p_i} \qquad (i=1,2,\cdots l)$$

将其代入(3)可得

$$p(a_1,\cdots a_n) < d^{p_1+p_2+\cdots+p_l+i}(d+1)^r = d^{j-r+i}(d+1)^r$$

$$= d^{k-r+-l}(d+1)^r \leqslant d^{k-r}(d+1)^r = p(\overbrace{d,d,\cdots d}^{k-r},\overbrace{d+1,\cdots d+1}^{r})$$

这与 $p(a_1\cdots a_n)$ 为最大值矛盾．此即说 $a_1,\cdots a_n$ 中任一个均不大于 $d+1$。是不正确的。

若 $a_2,\cdots a_k$ 中有一个大于 $d+1$，不妨设 $a_2>d+1$，设 $a_2=a_1+1+q$ ，由 $a_1<d$，故 $q>0$。作 n 个一个分拆 $n=(a_1+q)+(a_2-q)+a_3+\cdots+a_k=kd+r$．

则 $p(a_1+q,\ a_2-q,a_3\cdots a_n)=(a_1+q)(a_2-q)a_3\cdots a_k$

$$=(a_1a_2+(a_2-a_1-q)q)a_3a_4\cdots a_k$$

$$=(a_1a_2+q)a_3a_4\cdots a_k > a_1a_2\cdots a_k = p_M(A(k,n)),$$

这又产生矛盾．上述两矛盾，即说 $a_i \geq d\ (1\leq i\leq k)$．

若 $a_1,a_2,\cdots a_k$ 中有一个大于 $d+1$，不妨 $a_1>d+1$.

设 $a_{l+1}=\cdots=a_k=d$，$a_{j+1}=a_{j+2}=\cdots=a_l=d+1$，

$a_1,a_2,\cdots a_l$ 皆大于 $d+1$，$a_m=d+p_m$. $p_m>1$ $(1\le m\le j)$

则 $p(a_1,\cdots a_k)=(d+p_1)\cdots(d+p_j)(d+1)^{l-j}d^{k-l}$

因知：$(d+p_1)+\cdots+(d+p_j)+(l-j)(d+1)+(k-l)d=kd+r$

从而 $p_1+p_2+\cdots+p_j+l-j=r$. 令 $i=l-j$，则

$$p_1+p_2+\cdots+p_j=r-i.$$

由于对于 $m\ge1$，有 $(d+m)d\le(d+m-1)(d+1)$.

故 $p(a_1,a_2,\cdots a_k)\le(d+1)^{p_1+\cdots+p_j}d^{-(p_1+p_2+\cdots+p_j)}(d+1)^i d^{k-l}$

$=(d+1)^{p_1+\cdots+p_j+i}d^{k-l-(p_1+\cdots+p_j)}=(d+1)^r d^{k-l-r+i}$

$=(d+1)^r d^{k-r-j}<(d+1)^r d^{k-r}$ （因为 $j\ge1$）

这又是一个矛盾. 故 $a_1,a_2,\cdots a_n$ 中皆不大于 $d+1$.

于是 a_i 只取 d 或 $d+1$ $(1\le i\le k)$.

设 $P_M(A(k,n))=d^{k-j}(d+1)^j$

因 $(k-j)d+j(d+1)=kd+r$，故 $j=r$.

这说明：$P_m(A(k,n)) = d^{k-r}(d+1)^r$.

下证(2)式．先证明 $k=2$ 的情况．

$p(x,n-x) = x(n-x) = nx-x^2 \triangleq f(x)$，由于 $f'(x)=n-2x$ 故当 $x \leq \frac{n}{2}$ 时 $f(x)$ 递增而当 $x \geq \frac{n}{2}$ 时递减，故

$$P_m(A(2,n)) = \min\{n\times1-1^2, n(n-1)-(n-1)^2\} = n-1.$$

对于一般的 k，可利用 R. Bellman[2] 动态规划的思想，当 $n = x_1+x_2+\cdots+x_k$ 时，

$$P_m(A(k,n)) = \min_{(x_1,\cdots x_k)\in A(k,n)} x_1 x_2 \cdots x_k$$

$$= \min_{x_1}\Big(x_1 \min_{x_2}\Big(\cdots\Big(\min_{x_{k-1}} x_{k-1}(n-x_1-\cdots-x_{k-2}-x_{k-1})\cdots\Big)$$

$$= \min_{x_1}\Big(x_1 \min_{x_2}\Big(\cdots\Big(\min_{x_{k-2}} x_{k-2}(n-x_1-\cdots-x_{k-3}-1-x_{k-2})$$

$$= \cdots = \min_{x_1} x_1(n-k+1-x_1) = n-k.$$

上列各式中充分利用了 $k=2$ 的结果．

利用上述方法，我们还可讨论当 n 分解成素数的分析以及分解成四个平方数之和的分析的情况，对于其它一些具有限定条件的情况．

我们能说些什么呢？这是值得考虑的问题。

正如上面所讨论的，我们引入了数论函数 $p(k,n)$，易知 $p(1,n)=1$，$p(2,n)=\left[\frac{n}{2}\right]$，但当 $k\geqslant 3$ 的情况比较复杂。另外易知，$p(n)=\sum_{k=1}^{\infty} p(k,n)$。因此对于 $p(k,n)$ 的研究将会比 $p(n)$ 复杂。能否给出 $p(k,n)$ 的阶的估计呢？能否找到其生成函数呢？与此对应的椭圆函数又是什么？尚待研究。

参考文献

[1] 华罗庚，数论导引．科学出版社，1975.

[2] R.E. Bellman & S.E. Dreyfus, Applied Dynamic Programming. Princeton University Press 1–15.