命题：任意大于 6 的偶数可表示为两个质数之和
（哥德巴赫猜想证明的一种新方法）

一.预备知识

1.常用集合符号

自然数集 N；正整数集 N^+；质数集 $P=\{x\in N^+\mid x为质数\}$。

设 $x\in N$，集合 $N(X)=\{r\mid r\in N且r\le X\}$, 比如：$N(6)=\{0,1,2,3,4,5,6\}$

集合 $P(X)=\{r\mid r\in P且r\le X\}$, 比如：$P(16)=\{2,3,5,7,11,13\}$

2.定义：

函数 $\Phi(X):N\to N,$

$\Phi(X)=Card(P(X)),(X\in N),\ \Phi(X)$称为质数位置函数.

1）$\Phi(X)$ 表示不大于 X 的质数个数。

2）给集合 P 中元素赋予右下标进行排序。

如果 $r\in P$ 且 $\Phi(r)=k$，则元素 r 记作 $p_k(k\in N^+)$, 即

$$p_1=2,p_2=3,p_3=5,p_4=7,\cdots\cdots$$

3.设 $n\in N$，$m\in N^+$,集合 $\{x\in N\mid x\equiv n(\bmod m)\}$ 记作 E_n^m, E_n^m 为余数为 n 的关于 m 的同余类。集合 $E_n^m\cap N(X)$, 记作 $E_n^m(X)$。集合 $\{0,1,2,\cdots，m\text{-}1\}$ 记作 Γ_m, Γ_m 是 m 的一个完全剩余系。

4.集合列 $E_0^m,E_1^m,\cdots\cdots,E_{m-1}^m(m\ge 2)$ 满足：

1）当 $i,j\in\Gamma_m且i\ne j时E_i^m\cap E_j^m=\varphi;$

2）$\bigcup_{i\in\Gamma_m}E_i^m=N$

$\therefore E_i^m,i\in\Gamma_m$为集合$N$的一个$m$组剖分,

同理$E_i^m(X)$ $i\in\Gamma_m$为集合$N(X)$的一个m组剖分。

二　孙子定理及其推论

1.**定理（孙子定理）**假设$m_1, m_2, \cdots\cdots, m_k$两两互质，则同余方程组

$$\begin{cases} x \equiv a_1 (\bmod m_1) \\ \quad\cdots\cdots \\ x \equiv a_k (\bmod m_k) \end{cases} \qquad (1)$$

对于模$m = m_1 \cdots\cdots m_k$有唯一解：

$$x \equiv \frac{m}{m_1} x_1 a_1 + \cdots + \frac{m}{m_k} x_k a_k (\bmod m)$$

这里$\frac{m}{m_i} x_i \equiv 1 (\bmod m_i) \quad i = 1, \cdots, k.$　当$x \in \Gamma_m$时，x记作μ（$a_1, \cdots, a_k$）

2.**推论:**如果$a_i \in \Gamma_{m_i}, i = 1, \cdots, k$取两组不完全相同的值,则同余方程组(1)的解关于

m不同余。

证明：假设方程组$\begin{cases} x \equiv b_1 (\bmod m_1) \\ \quad\cdots\cdots \\ x \equiv b_k (\bmod m_k) \end{cases}$和$\begin{cases} x \equiv c_1 (\bmod m_1) \\ \quad\cdots\cdots \\ x \equiv c_k (\bmod m_k) \end{cases}$的解为

$$x_1 \equiv \frac{m}{m_1} x_1 b_1 + \cdots + \frac{m}{m_k} x_k b_k (\bmod m)$$ 与

$$x_2 \equiv \frac{m}{m_1} x_1 c_1 + \cdots + \frac{m}{m_k} x_k c_k (\bmod m)$$ 相同

即$\frac{m}{m_1} x_1 b_1 + \cdots + \frac{m}{m_k} x_k b_k \equiv \frac{m}{m_1} x_1 c_1 + \cdots + \frac{m}{m_k} x_k c_k$（mod$m$）　(2)

$$\because (m_i, \frac{m}{m_j}) = \begin{cases} 1, & 当 i = j 时 \\ m_i, & 当 i \neq j 时 \end{cases} \qquad i, j = 1, \cdots k.$$

则由(2)式知:$\frac{m}{m_1} x_1 (b_1 - c_1) + \cdots + \frac{m}{m_k} x_k (b_k - c_k) \equiv 0 (\bmod m_i)$

$$\therefore \frac{m}{m_i} x_i (b_i - c_i) \equiv 0 (\bmod m_i)$$

由于$\frac{m}{m_i}x_i \equiv 1(\bmod m_i)$，　　$\therefore b_i - c_i \equiv 0(\bmod m_i), i = 1, 2, \cdots, k$矛盾。

3.**引理** 设$m_1, m_2, \cdots\cdots, m_k$两两互质，$E_{n_i}^{m_i}(n_i \in \Gamma_{m_i})\quad i = 1,2,\cdots,k$都为集合$N$的剖分，

则$\bigcap_{i=1}^{k} E_{n_i}^{m_i}(n_i \in \Gamma_{m_i}\quad i = 1,2,\cdots,k)$为集合$N$的一个$m = m_1 \cdots m_k$组剖分。

比如：$m_1 = 2, m_2 = 3$时，如图1

$E_0^2 \cap E_0^3 = E_0^6, E_0^2 \cap E_1^3 = E_4^6, E_0^2 \cap E_2^3 = E_2^6$

$E_1^2 \cap E_0^3 = E_3^6, E_1^2 \cap E_1^3 = E_1^6, E_1^2 \cap E_2^3 = E_5^6$

	E_0^3	E_1^3	E_2^3
E_0^2			
E_1^2			

图 1

事实上，$\bigcap_{i=1}^{k} E_{n_i}^{m_i} = E_{\mu(n_1,\cdots,n_k)}^{m}$

$\mu(n_1, \cdots, n_k) \equiv \frac{m}{m_1}x_1 n_1 + \cdots + \frac{m}{m_k}x_k n_k(\bmod m)$，这里$\frac{m}{m_i}x_i \equiv 1(\bmod m_i)\quad i = 1, 2, \cdots, k$

$\because n_i \in \Gamma_{m_i}(i = 1, 2, \cdots, k)$有$m$组不同取值，$\mu(n_1, \cdots, n_k)$也有$m$个不同取值，

$\therefore E_{\mu(n_1,\cdots,n_k)}^{m}(\mu(n_1, \cdots, n_k) \in \Gamma_m)$为$N$的$m$组剖分

$\therefore \bigcap_{i=1}^{k} E_{n_i}^{m_i}(n_i \in \Gamma_{m_i}\quad i = 1, 2, \cdots, k)$为$N$的$m$组剖分。

同理，引理结论对于有限集合$N(X)$也成立，即若$m_1, m_2, \cdots, m_k$两两互质，则

$\bigcap_{i=1}^{k} E_{n_i}^{m_i}(X)(n_i \in \Gamma_{m_i}\quad i = 1,2,\cdots,k)$为集合$N(X)$的一个$m = m_1 \cdots m_k$组剖分。

三.有关集合元素个数的结论（一）

对于有限集合A，其元素个数$Card(A)$记作$|A|$

1.$|N(X)| = X+1$

2.设$X \equiv e \pmod{m}, e \in \Gamma_m$,集合$E_n^m(X)$的补集$\ell_{N(X)}(E_n^m(X))$记作$B_n^m(X), n \in \Gamma_m$

则$|E_n^m(X)|$和$|B_n^m(X)|$分两种情形。

①当$0 \le n \le e$时,$|E_n^m(X)| = [\frac{X}{m}]+1 = \frac{X-e}{m}+1$

这里符号[]为高斯最大取整符号，且$[\frac{X}{m}] = \frac{X-e}{m}$

$$|B_n^m(X)| = |N_{(X)}| - |E_n^m(X)|$$

$$= X(1-\frac{1}{m}) + \frac{e}{m}$$ (3

②当$e < n \le m-1$时,$|E_n^m(X)| = [\frac{X}{m}] = \frac{X-e}{m}$

$$|B_n^m(X)| = |N(X)| - |E_n^m(X)|$$

$$= X+1-\frac{X-e}{m} = X(1-\frac{1}{m}) + \frac{e}{m} +$$

3. 设$m_1, m_2 \in N^+$,且m_1, m_2互质，$X \equiv e_2 \pmod{m_1 m_2}, e_2 \in \Gamma_{m_1 m_2}, X \equiv e' \pmod{m_1}, X \equiv e'' \pmod{m_2}$

比如$X=34$，$m_1=3, m_2=5$,这时$e_2=4$,如图2

$B_0^5(X)$（$E_1^5(X)$ 至 $E_4^5(X)$ 列）

	$E_0^5(X)$	$E_1^5(X)$	$E_2^5(X)$	$E_3^5(X)$	$E_4^5(X)$
$E_0^3(X)$	0 15 30	6 21	12 27	3 18 33	9 24
$E_1^3(X)$	10 25	1 16 31	7 22	13 28	4 19 34
$E_2^3(X)$	5 20	11 26	2 17 32	8 23	14 29

$B_0^3(X)$（$E_1^3(X)$、$E_2^3(X)$ 行）

图 2

对于集合 $N(X)$ 中任意 x ,及性质

$$H_1: x \equiv 0 (\bmod m_1)$$

$$H_2: x \equiv 0 (\bmod m_2)$$

显然 x 要么有性质 H_i ，要么没有性质 $H_i (i=1.2)$

$N(X)$ 中有性质 H_i 的所有元素组成的集合记作 $E_0^{m_i}(X) \qquad i=1,2$

没有性质 H_i 的所有元素组成的集合记作 $B_0^{m_i}(X) \qquad i=1,2$

则同时有性质 H_1, H_2 的所有元素组成的集合为 $E_0^{m_1}(X) \cap E_0^{m_2}(X) = E_0^{m_1 m_2}(X)$

$$\left| E_0^{m_1 m_2}(X) \right| = [\frac{X}{m_1 m_2}] + 1 = \frac{X - e_2}{m_1 m_2} + 1$$

同时没有性质 H_1, H_2 的所有元素组成的集合为 $B_0^{m_1}(X) \cap B_0^{m_2}(X)$

$$\left| B_0^{m_1}(X) \cap B_0^{m_2}(X) \right| = (X+1) - \left| E_0^{m_1}(X) \right| - \left| E_0^{m_2}(X) \right| + \left| E_0^{m_1 m_2}(X) \right|$$

$$= X(1 - \frac{1}{m_1} - \frac{1}{m_2} + \frac{1}{m_1 m_2}) + \frac{m_2 e' + m_1 e'' - e_2}{m_1 m_2}$$

$$= X(1 - \frac{1}{m_1})(1 - \frac{1}{m_2}) + \frac{m_2 e' + m_1 e'' - e_2}{m_1 m_2} \qquad (4)$$

4.设 $m_1 \ldots m_k$ 两两互质，

$x \equiv e_k (\bmod m_1 \ldots m_k) \quad e_k \in \Gamma m_1 \ldots m_k, X \equiv b_i (\bmod m_i), b_i \in \Gamma m_i, i = 1, 2, \cdots, k$

1）对于集合 $N(X)$ 和 $N(e_k)$ 中任意元素 x 及性质 H： $x \neq 0 (\bmod m_i), i = 1, \ldots k$

显然 x 要么有性质 H ，要么没有性质 H ，则 $N(X)$ 和 $N(e_k)$ 中

满足性质 H 的所有元素组成的的集合分别为 $\bigcap_{i=1}^{k} B_0^{m_1}(X)$ 和 $\bigcap_{i=1}^{k} B_0^{m_1}(e_k)$

因为集合 $\bigcap_{i=1}^{k} B_0^{m_1}(X) = \bigcup_{a_i \in \Gamma_{mi} 且 a_i \neq 0, i=1,2,\ldots k} E_{\mu(a_1,\ldots,a_{10})}^{m_1 \ldots m_k}(X)$ 中每组为 $E_{\mu(a_1,\ldots,a_k)}^{m_1 \ldots m_k}$

共有 $t = \prod_{i=1}^{k} (m_i - 1)$ 组，每组元素个数差异由 $\{0, 1, \ldots, e_k\}$ 中元素

是否有性质 H 成立确定，共有 $\left|\bigcap_{i=1}^{k} B_0^{m_i}(e_k)\right|$ 组的元素个数多 1.

$$\therefore \left|\bigcap_{i=1}^{k} B_0^{m_i}(X)\right| = t[\frac{X}{m_1\cdots m_k}] + \left|\bigcap_{i=1}^{k} B_0^{m_i}(e_k)\right| = \frac{X-e_k}{m_1\cdots m_k}\cdot t + \left|\bigcap_{i=1}^{k} B_0^{m_i}(e_k)\right|$$

$$= X\cdot\prod_{i=1}^{k}\alpha_i + \left|\bigcap_{i=1}^{k} B_0^{m_i}(e_k)\right| - e_k\cdot\prod_{i=1}^{k}\alpha_i$$

这里 $\alpha_i = 1-\frac{1}{m_i}, i=1,2,\ldots k.$

令 $F_k(X) = \left|\bigcap_{i=0}^{k} B_0^{m_i}(X)\right| - X\cdot\prod_{i=1}^{k}\alpha_i$

则 $F_k(X) = F_k(e_k)$ (5

2）集合 $N(X)$ 和 $N([\frac{X}{m_k}])$ 中任意元素 x 及性质 H'： $x \not\equiv 0(\bmod m_i), i=1,..,k-1,$

对于 x 要么 H' 成立，要么没有性质 H'

则 $N(X)$ 和 $N(\frac{X}{m_k})$ 中满足性质 H'：的所有元素组成的集合分别

为 $\bigcap_{i=1}^{k-1} B_0^{m_i}(X)$ 和 $\bigcap_{i=1}^{k-1} B_0^{m_i}([\frac{X}{m_k}])$。

$$\text{则} \bigcap_{i=1}^{k} B_0^{m_i}(X) = \bigcap_{i=1}^{k-1} B_0^{m_i}(X) \cap B_0^{m_k}(X)$$

$$= \bigcap_{i=1}^{k-1} B_0^{m_i}(X) \Big/ \left(\bigcap_{i=1}^{k-1} B_0^{m_i}(X) \cap E_0^{m_k}(X)\right)$$

由于 $E_0^{m_k}(X) = \left\{0, m_k, \ldots, \lambda m_k, \ldots, [\frac{X}{m_k}]\cdot m_k\right\}$，这些元素是否在集合

$\bigcap_{i=1}^{k-1} B_0^{m_i}(X)$ 中，就看 $\lambda m_k\left(\lambda = 0,1,\ldots,[\frac{X}{m_k}]\right)$，是否满足 $\lambda\cdot m_k \not\equiv 0(\bmod m_i)$

$i=1,2,\ldots,k-1$，由于 m_k 与 $m_i(i=1,\ldots,k-1)$ 互质，$\therefore \lambda \not\equiv 0(\bmod m_i)$

$i=1,2,\ldots,k-1$，即 $N([\frac{X}{m_k}])$ 中的元素是否有性质 H' 成立确定，

而$N([\frac{X}{m_k}])$中满足性质H'的元素组成的集合为$\bigcap_{i=1}^{k-1} B_0^{m_i}([\frac{X}{m_k}])$

$$\therefore \left|\bigcap_{i=1}^{k-1} B_0^{m_i}(X)\cap E_0^{m_k}(X)\right| = \left|\bigcap_{i=1}^{k-1} B_0^{m_i}([\frac{X}{m_k}])\right|$$

$$\therefore \left|\bigcap_{i=1}^{k} B_0^{m_i}(X)\right| = \left|\bigcap_{i=1}^{k-1} B_0^{m_i}(X)\right| - \left|\bigcap_{i=1}^{k-1} B_0^{m_i}([\frac{X}{m_k}])\right| \qquad (6)$$

$$F_k(X) = \left|\bigcap_{i=1}^{k} B_0^{m_i}(X)\right| - X\cdot\prod_{i=1}^{k}\alpha_i$$

$$F_{k-1}(X) = \left|\bigcap_{i=1}^{k-1} B_0^{m_i}(X)\right| - X\cdot\prod_{i=1}^{k-1}\alpha_i$$

$$F_{\text{k-1}}([\frac{X}{m_k}]) = \left|\bigcap_{i=1}^{k-1} B_0^{m_i}([\frac{X}{m_k}])\right| - [\frac{X}{m_k}]\cdot\prod_{i=1}^{k\text{-}1}\alpha_i$$

$$\therefore F_k(X) = F_{k\text{-}1}(X) - F_{k\text{-}1}([\frac{X}{m_k}]) + X\cdot\prod_{i=1}^{k-1}\alpha_i - X\cdot\prod_{i=1}^{k}\alpha_i - [\frac{X}{m_k}]\prod_{i=1}^{k-1}\alpha_i$$

$$= F_{k\text{-}1}(X) - F_{k\text{-}1}([\frac{X}{m_k}]) + \Delta_{k\text{-}1}(X)$$

这里$\Delta_{k\text{-}1}(X) = (\frac{X}{m_k} - [\frac{X}{m_k}])\cdot\prod_{i=1}^{k\text{-}1}\alpha_i = \frac{b_k}{m_k}\cdot\prod_{i=1}^{k\text{-}1}\alpha_i$

由此$F_{k\text{-}1}(X) = F_{k\text{-}2}(X) - F_{k\text{-}2}([\frac{X}{m_k}]) + \Delta_{k\text{-}2}(X)$

$$\vdots$$

$$F_2(X) = F_1(X) - F_1([\frac{X}{m_k}]) + \Delta_1(X)$$

而$F_1(X) = |B_0^{m_1}(X)| - X\cdot\alpha_1 = \frac{b_1}{m_1}$

$$\Delta_s(X) = \frac{b_{s+1}}{m_{s+1}}\cdot\prod_{i=1}^{s}\alpha_i,\ s = 1,2,\cdots,k-1$$

$$\therefore F_k(X) = -(F_1([\frac{X}{m_2}]) + F_2([\frac{X}{m_3}]) + \cdots + F_{k-1}([\frac{X}{m_k}])) + \sum_{s=1}^{k-1}(\frac{b_{s+1}}{m_{s+1}}\cdot\prod_{i=1}^{s}\alpha_i) + \frac{b_1}{m_1} \qquad (8)$$

又$\because X \equiv e_{s+1}\left(\bmod m_1\cdots m_{s+1}\right), e_{s+1}\in\Gamma_{m_1\cdots m_{s+1}}$

$$\therefore [\frac{X}{m_{s+1}}]-[\frac{e_{s+1}}{m_{s+1}}]\equiv 0\left(\bmod m_1\cdots m_s\right)$$

由公式(5)有：

$$F_s([\frac{X}{m_{s+1}}])=F_s([\frac{e_{s+1}}{m_{s+1}}]), s=1,2,\cdots,k-1$$

$$\therefore F_k(X)=-(F_1([\frac{e_2}{m_2}])+F_2([\frac{e_3}{m_3}])+\cdots+F_{k-1}([\frac{e_k}{m_k}]))+\sum_{s=1}^{k-1}(\frac{b_{s+1}}{m_{s+1}}\cdot\prod_{i=1}^{s}\alpha_i)+\frac{b_1}{m_1} \qquad (9)$$

四　有关集合元素个数的结论(二)

1.$X\in N, m\in N^{+}, X\equiv e(\bmod m), e\in\Gamma_{m}$且$e\neq 0$，$\forall x\in N(X)$

$N(X)$的有关性质，$H_1: x\not\equiv 0(\bmod m)$

$H_2: x\not\equiv e(\bmod m)$

则：

有性质 H_1 成立的所有元素组成的集合为$\ell_{N(X)}(E_0^m(X))=B_0^m(X)$

有性质 H_2 成立的所有元素组成的集合为$\ell_{N(X)}(E_e^m(X))=B_e^m(X)$

则$N(X)$中有关性质H_1，H_2都成立的所有元素组成的集合记为$D^m(X)=B_0^m(X)\cap B_e^m(X)$

比如　X =26，　m=5，　e=1，如图 3

$B_1^5(X)$（$E_0^5(X)$ 至 $E_4^5(X)$ 列）；$B_0^5(X)$（$E_1^5(X)$ 至 $E_4^5(X)$ 行）

	$E_1^5(X)$	$E_0^5(X)$	$E_2^5(X)$	$E_3^5(X)$	$E_4^5(X)$
$E_0^5(X)$		///			
$E_1^5(X)$	///				
$E_2^5(X)$			///		
$E_3^5(X)$				///	
$E_4^5(X)$					///

图 3

$E_0^5(X)=\{0,5,10,15,20,25\}$, $E_1^5(X)=\{1,6,11,16,21,26\}$, $E_2^5(X)=\{2,7,12,17,22\}$,

$E_3^5(X)=\{3,8.13,18,23\}$, $E_4^5(X)=\{4,9,14,15,24\}$

同时满足性质 H_1, H_2 的共有(5−2)组，而每组元素个数之差异由集合

$\{0,1,\cdots,e\}$ 中是否有性质 H_1, H_2 同时成立确定。又$D^m(X)=\ell_{N(X)}(E_0^m(X)\cup E_e^m(X))$

$$\therefore |D^m(X)|=(X+1)-2(\frac{X}{m}-\frac{e}{m}+1)=X(1-\frac{2}{m})+\frac{2e}{m}-1 \qquad (10)$$

2.设m_1, m_2互质，$X\equiv b_i(\bmod m_i)$　$b_i\neq 0$且$b_i\in\Gamma_{m_i}(i=1,2)$

$$X \equiv e_2 (\bmod m_1 m_2), e_2 \in \Gamma_{m_1 m_2}$$

$\forall x \in N(X)$及与$N(X)$有关的性质：

$$H_1' : x \not\equiv 0 且 x - b_1 \not\equiv 0 (\bmod m_1)$$

$$H_2' : x \not\equiv 0 且 x - b_2 \not\equiv 0 (\bmod m_2)$$

满足H_1'的所有元素组成的集合为$D^{m_1}(X) = \ell_{N(X)}(E_0^{m_1}(X) \cup E_{b_1}^{m_1}(X))$

满足H_2'所有元素组成的集合为$D^{m_2}(X) = \ell_{N(X)}(E_0^{m_2}(X) \cup E_{b_2}^{m_2}(X))$

则$N(X)$中同时有关性质H_1'，H_2'都成立的所有元素组成的集合记为$D^{m_1}(X) \cap D^{m_2}(X)$

比如X=52，$m_1 = 3, m_2 = 5,$这时$b_1 = 1, b_2 = 2, e_2 = 7,$如图4

$D^5(X)$

	14 29 44	13 28 43	11 26 41	9 24 39	8 23 38	6 21 36 51	4 19 34 49	3 18 33 48	1 16 31 46	12 27 42	10 25 40	7 22 37 52	5 20 35 50	2 17 32 47	0 15 30 45
0 15 30 45															///
1 16 31 46									///						
3 18 33 48								///							
4 19 34 49							///								
6 21 36 51						///									
7 22 37 52												///			
9 24 39				///											
10 25 40											///				
12 27 42										///					
13 38 43		///													
2 17 32 47															
5 20 35 50					///									///	
8 23 38			///										///		
11 26 41															
14 29 44	///														

$D^3(X)$

图 4

同时满足性质H_1'，H_2'的元素共有(3-1)•(5-2)组，而每组元素个数之差异由集合$\{0,1,\cdots,e_2\}$中是否满足H_1'，H_2'来确定。

也可以这样描述与$N(X)$有关的性质：

$H_1'': x \not\equiv 0(\bmod m_i), i=1,2$

$H_2'': x \not\equiv b_i(\bmod m_i), i=1,2$

$N(X)$中满足H_1''的所有元素组成的集合为$B_0^{m_1}(X)\cap B_0^{m_2}(X)$

$N(X)$中满足H_2''的所有元素组成的集合为$B_{b_1}^{m_1}(X)\cap B_{b_2}^{m_2}(X)$

比如X=52，$m_1=3, m_2=5$,这时$b_1=1, b_2=2, e_2=7$,如图5

$B_1^3(X)\cap B_2^5(X)$

	0 15 30 45	3 18 33 48	5 20 35 50	6 21 36 51	8 23 38	9 24 39	11 26 41	14 29 44	13 38 43	12 27 42	7 22 37 52	4 19 34 49	1 16 31 46	2 17 32 47	10 25 40
0 15 30 45	///														
3 18 33 48		///													
5 20 35 50			///												
6 21 36 51				///											
9 24 39						///									
10 25 40															///
12 27 42										///					
1 16 31 46															
2 17 32 47														///	
4 19 34 49												///			
7 22 37 52											///				
8 23 38					///										
11 26 41							///								
13 38 43									///						
14 29 44								///							

$B_1^3(X)$
$\cap B_2^5(X)$

图 5

因此：（$B_0^{m_1}(X)\cap B_0^{m_2}(X)$)$\cap$（$B_{b_1}^{m_1}(X)\cap B_{b_2}^{m_2}(X)$）=$\mathrm{D}^{m_1}(X)\cap \mathrm{D}^{m_2}(X)$ 表示 $N(X)$ 中同时满足性质 H_1''，H_2'' 的元素共有$((m_1-2)\cdot(m_2-2))$组，每组元素个数之差异由集合$\{0,1,\cdots,e_2\}$是否满足H_1''，H_2''来确定。

$$\therefore \left|D^{m_1}(X)\cap D^{m_2}(X)\right| = (m_1-2)(m_2-2)\cdot[\frac{X}{m_1m_2}] + |B_0^{m_1}(e_2)\cap B_0^{m_2}(e_2)\cap(B_{b_1}^{m_1}(e_2)\cap B_{b_2}^{m_2}(e_2)|$$

$$= X\beta_1\beta_2 - e_0\beta_1\beta_2 + \left|D^{m_1}(e_2)\cap D^{m_2}(e_2)\right|$$

又 $\left|D^{m_1}(X)\cap D^{m_2}(X)\right| = \left|N(X)\right| - \left|D^{m_1}(X)\right| - \left|D^{m_2}(X)\right| + |(E_0^{m_1}(X)\cup E_{b_1}^{m_1}(X))\cap(E_0^{m_2}(X)\cup E_{b_2}^{m_2}(X)|$

$$=(X+1)-2\left|\frac{X}{m_1}\right|-2-2\left|\frac{X}{m_2}\right|-2+4\left|\frac{X}{m_1m_2}\right|+2+\eta$$

$$= X - \frac{2(X-b_1)}{m_1} - \frac{2(X-b_2)}{m_2} + \frac{4(X-e_2)}{m_1m_2} + \eta - 1$$

$$= X(1-\frac{2}{m_1})(1-\frac{2}{m_2}) + \frac{2b_1m_2+2b_2m_1-4e_2}{m_1m_2} + \eta - 1 \qquad (11)$$

由同余方程组解知：

当$\mu(0,b_2)$ +$\mu(b_1,0)$ =e_2时，$\eta = 2$

当$\mu(0,b_2)$ +$\mu(b_1,0)$ =$m_1m_2+e_2$时，$\eta = 0$

3.$m_1, m_2, \cdots\cdots, m_k$两两互质，$X \equiv b_i (\bmod m_i), b_i \neq 0, b_i \in \Gamma_{m_i}, i = 1,\cdots,k$

$X \equiv \mu(b_1, b_2, \cdots, b_k) = e_k, e_k \in \Gamma_{m_1\cdots m_s}$

1)$\forall x \in N(X)$及$x \in N(e_k)$及下列性质：

$H_1 : x \not\equiv 0 (\bmod m_i), i = 1,2,\cdots,k$

$H_2 : x \not\equiv e (\bmod m_i), i = 1,2,\cdots,k$

对于 $N(X)$和 $N(e_k)$中任意元素，要么有性质 H_i $(i=1,2$ 成立，要么性质 H_i $(i=1,2)$ 不成立，则有性质 H_1 成立的所有元素的集合分别为：

$$\bigcap_{i=1}^{k} B_0^{m_i}(X) \text{和} \bigcap_{i=1}^{k} B_0^{m_i}(e_k)$$

$N(X)$和$N(e_k)$ 中有性质 H_2 成立的所有元素的集合分别为：

$$\bigcap_{i=1}^{k} B_{b_i}^{m_i}(X) \text{和} \bigcap_{i=1}^{k} B_{b_i}^{m_i}(e_k)$$

则 $N(X)$ 中有性质 H_1，H_2 都成立的所有元素的集合为：

$$(\bigcap_{i=1}^{k} B_0^{m_i}(X))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(X))$$

$N(e_k)$ 中有性质 H_1，H_2 都成立的所有元素的集合为：

$(\bigcap_{i=1}^{k} B_0^{m_i}(e_k))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(e_k))$

则 $(\bigcap_{i=1}^{k} B_0^{m_i}(X))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(X)) = \bigcup_{\substack{a_i\in\Gamma_{m_i}/\{0,b_i\}\\ i=1,\cdots,k}} E_{\mu(a_1,\cdots,a_k)}^{m_1\cdots m_k}(X)$

共有 t 组，$t=\prod_{i=1}^{k}(m_i-2)$, 每组元素个数之差异由集合 $(i=1,2,\cdots,e_k)$ 是否同时满足 H_1 和 H_2 来确定，同时满足 H_1，H_2 的所有元素的集合为：$(\bigcap_{i=1}^{k} B_0^{m_i}(e_k))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(e_k))$

也就是 $(\bigcap_{i=1}^{k} B_0^{m_i}(X))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(X))$ 中有 $|\bigcap_{i=1}^{k} B_0^{m_i}(e_k)\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(e_k)|$ 组元素个数多 1.

$$\therefore |\bigcap_{i=1}^{k} B_0^{m_i}(X)\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(X)| = t[\frac{X}{m_1\cdots m_k}] + |\bigcap_{i=1}^{k} B_0^{m_i}(e_k)\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(e_k)|$$

$$\because \bigcap_{i=1}^{k} D^{m_i}(X) = (\bigcap_{i=1}^{k} B_0^{m_i}(X))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(X))$$

$$\bigcap_{i=1}^{k} D^{m_i}(e_k) = (\bigcap_{i=1}^{k} B_0^{m_i}(e_k))\cap(\bigcap_{i=1}^{k} B_{b_i}^{m_i}(e_k))$$

$$[\frac{X}{m_1\cdots m_k}] = \frac{X-e_k}{m_1\cdots m_k}$$

$$|\bigcap_{i=1}^{k} D^{m_i}(X)| = t\cdot\frac{X-e_k}{m_1\cdots m_k} + |\bigcap_{i=1}^{k} D^{m_i}(e_k)| = X\cdot\prod_{i=1}^{k}\beta_i - e_k\cdot\prod_{i=1}^{k}\beta_i + |\bigcap_{i=1}^{k} D^{m_i}(e_k)|$$

这里 $\beta_i = 1-\frac{2}{m_i}, i=1,2,\cdots,k$

令 $M_k(X) = |\bigcap_{i=1}^{k} D^{m_i}(X)| - X\cdot\prod_{i=1}^{k}\beta_i$

$M_k(e_k) = |\bigcap_{i=1}^{k} D^{m_i}(e_k)| - e_k\cdot\prod_{i=1}^{k}\beta_i$

$\therefore M_k(X) = M_k(e_k)$ (12)

2）集合 $N(X)$ 中任意元素 x 及与集合 $N(X)$ 有关性质

$H_1{}'$: $x\neq 0$ 且 $x\neq b_i \pmod{m_i}, i=1,2,\cdots,k-1$

集合 $N(X)$ 中具有性质 H_1' 的元素集合为 $\bigcap_{i=1}^{k-1} D^{m_i}(X)$

集合 $N([\frac{X}{m_k}])$ 中任意元素 λ 及与集合有关性质

$H_2' : \lambda \neq 0$ 且 $\lambda \not\equiv c_i (\bmod m_i)$, 这里 c_i 满足：$c_i \in \Gamma_{m_i}$ 且 $c_i \cdot m_k \equiv b_i (\bmod m_i), i = 1, 2, \cdots, k-1$

集合 $N([\frac{X}{m_k}])$ 中具有性质 H_2' 的元素集合为 $\bigcap_{i=1}^{k-1} D^{m_i}([\frac{X}{m_k}])$

由于 $E_0^{m_k}(X) = \{0, m_k, \cdots, \lambda m_k, \cdots, [\frac{X}{m_k}]m_k\}$ 中元素是否在 $\bigcap_{i=1}^{k-1} D^{m_i}(X)$ 中就看 $\lambda \in N([\frac{X}{m_k}])$ 是否满足 H_2'，即

$$\lambda \neq 0 \text{且} \lambda \not\equiv c_i (\bmod m_i) \Leftrightarrow \lambda \cdot m_k \neq 0 \text{且} \lambda \cdot m_k - b_i \equiv 0 (\bmod m_i), i = 1, 2, \cdots, k-1$$

同理 $$E_{b_k}^{m_k}(X) = \{b_k, b_k + m_k, \cdots, b_k + [\frac{X}{m_k}]m_k\}$$

$$= \{X, X - m_k, \cdots, X - b' m_k, \cdots, X - [\frac{X}{m_k}]m_k\}$$

$\lambda' \in \{0, 1, \cdots, [\frac{X}{m_k}]\}$ 中元素是否在 $\bigcap_{i=1}^{k-1} D^{m_i}(X)$ 中就看 $\lambda' \in N([\frac{X}{m_k}])$ 是否满足 H_2'

$$\therefore |\bigcap_{i=1}^{k-1} D^{m_i}(X) \cap E_0^{m_k}(X)| = |\bigcap_{i=1}^{k-1} D^{m_i}([\frac{X}{m_k}])|$$

$$\therefore |\bigcap_{i=1}^{k-1} D^{m_i}(X) \cap E_{b_k}^{m_k}(X)| = |\bigcap_{i=1}^{k-1} D^{m_i}([\frac{X}{m_k}])|$$

而 $$|\bigcap_{i=1}^{k} D^{m_i}(X)| = |\bigcap_{i=1}^{k-1} D^{m_i}(X)| - |\bigcap_{i=1}^{k-1} D^{m_i}(X) \cap E_0^{m_k}(X)| - |\bigcap_{i=1}^{k-1} D^{m_i}(X) \cap E_{b_k}^{m_k}(X)|$$

$$= |\bigcap_{i=1}^{k-1} D^{m_i}(X)| - 2|\bigcap_{i=1}^{k-1} D^{m_i}([\frac{X}{m_k}])| \quad (13)$$

$$M_k(X) = |\bigcap_{i=1}^{k} D^{m_i}(X)| - X \cdot \prod_{i=1}^{k} \beta_i$$

$$M_{k-1}(X) = |\bigcap_{i=1}^{k-1} D^{m_i}(X)| - X \cdot \prod_{i=1}^{k-1} \beta_i$$

$$M_{k-1}([\frac{X}{m_k}])=\left|\bigcap_{i=1}^{k-1}D^{m_i}([\frac{X}{m_k}])\right|-[\frac{X}{m_k}]\cdot\prod_{i=1}^{k-1}\beta_i$$

$$\therefore M_k(X)=M_{k-1}(X)-2M_{k-1}([\frac{X}{m_k}])+X\cdot\prod_{i=1}^{k-1}\beta_i-X\cdot\prod_{i=1}^{k}\beta_i-2[\frac{X}{m_k}]\prod_{i=1}^{k-1}\beta_i$$

$$=M_{k-1}(X)-2M_{k-1}([\frac{X}{m_k}])+2\Delta'_{k-1}(X) \qquad (14)$$

$$\Delta'_{k-1}(X)=(\frac{X}{m_k}-[\frac{X}{m_k}])\cdot\prod_{i=1}^{k-1}\beta_i=\frac{b_k}{m_k}\cdot\prod_{i=1}^{k-1}\beta_i$$

由此$M_{k-1}(X)=M_{k-2}(X)-2M_{k-2}([\frac{X}{m_k}])+2\Delta'_{k-2}(X)$

$$\vdots$$

$$M_2(X)=M_1(X)-2M_1([\frac{X}{m_k}])+2\Delta'_1(X)$$

而$M_1(X)=|D^{m_1}(X)|-X\cdot\beta_1=\frac{2b_1}{m_1}-1$

$$\Delta'_s(X)=\frac{b_{s+1}}{m_{s+1}}\cdot\prod_{i=1}^{s}\beta_i, s=1,2,\cdots,k-1$$

$$\therefore M_k(X)=-2(M_1([\frac{X}{m_2}])+M_2([\frac{X}{m_3}])+\cdots+M_{k-1}([\frac{X}{m_k}]))+2\sum_{s=1}^{k-1}(\frac{b_{s+1}}{m_{s+1}}\cdot\prod_{i=1}^{s}\beta_i)+\frac{2b_1}{m_1}-1 \qquad (15)$$

$(\beta_i=1-\frac{2}{m_i}$ $i=$ 1, 2; k ,

又$\because X\equiv e_{s+1}(\bmod m_1\cdots m_{s+1}), e_{s+1}\in\Gamma_{m_1\cdots m_{s+1}}$

$$\therefore [\frac{X}{m_{s+1}}]-[\frac{e_{s+1}}{m_{s+1}}]\equiv 0(\bmod m_1\cdots m_s)$$

$$M_s([\frac{X}{m_{s+1}}])=M_s([\frac{e_{s+1}}{m_{s+1}}]), s=1,2,\cdots,k-1$$

由公式(12)有

$$\therefore M_k(X)=-2(M_1([\frac{e_2}{m_2}])+M_2([\frac{e_3}{m_3}])+\cdots+M_{k-1}([\frac{e_k}{m_k}]))+2\sum_{s=1}^{k-1}(\frac{b_{s+1}}{m_{s+1}}\cdot\prod_{i=1}^{s}\chi_i)+\frac{2b_1}{m_1}-1 \qquad (16)$$

五．哥氏猜想证明

定理 3：当 X 为较大的正偶数时，$\exists p \in P(X)$ 满足 $X-p \in P(X)$。

证明：设 $Q_1(X)=\{r\in P(X) \mid X\equiv 0(\bmod r)\}, Q_2(X)=\{r\in P(X) \mid r\notin Q_1(X)$ 且 $r\le\sqrt{X}\}$

1)显然 $2\in Q_1(X)$，$\forall r\in Q_1(X)$ 和 $x\in N(X)$

$(X-x)\equiv o(\bmod r)\Leftrightarrow x\in E_0^r(X)$

$x\equiv o(\bmod r)\Leftrightarrow x\in E_0^r(X)$

2) $\forall r\in Q_2(X), X\equiv t_0(\bmod r), t_0\in\Gamma_r$ 且 $t_0\ne 0$

$x\equiv 0(\bmod r)\Leftrightarrow x\in E_0^r(X)$

$(X-x)\equiv o(\bmod r)\Leftrightarrow x\in E_{t_0}^p(X).$

这时记 $B_0^r(X)=\ell_{N(X)}(E_0^r(X)), B_{t_0}^r(X)=\ell_{N(X)}(E_{t_0}^r(X)),$

$D^r(X)=\ell_{N(X)}(E_0^r(X)\cup(E_{t_0}^r(X))=B_0^r(X)\cap B_{t_0}^r(X)$

综上：

①当 $r\in Q_1(X)$ 时，如果 $x\ne 0(\bmod r)$ 且 $(X-x)\not\equiv 0(\bmod r)\Leftrightarrow x\in B_0^r(X).$

②当 $r\in Q_2(X)$ 时，如果 $x\ne 0(\bmod r)$ 且 $(X-x)\not\equiv 0(\bmod r)\Leftrightarrow x\in D^r(X).$

3) 设 $T(X)=\left(\bigcap_{r\in Q_1(X)}B_0^r(X)\right)\cap\left(\bigcap_{r\in Q_2(X)}D^r(X)\right)\Big/\{1,X-1\}$

$Q_1(X)\cup Q_2(X)=\{p_1,\cdots,p_s\}$

这里 $s=\Phi([\sqrt{X}]), s_1=|Q_1(X)|, s_2=|Q_2(X)|, s_1+s_2=s$

如果集合 $T(X)\ne\phi$，则 $\forall x\in T(X)$ 同时满足下列条件

①$x\ne 1$ 且 $p_i\nmid x \qquad i=1,2,\cdots,s \qquad \therefore x\in P(X)$

②$X-x\ne 1$ 且 $p_i\nmid(X-x) \qquad i=1,2,\cdots,s \qquad \therefore X-x\in P(X)$

4）为便于计算，把 $Q_2(X)$ 中元素按从小到大的顺序排列为：$r_1,r_2,\cdots r_{s_2}$

且 $X\equiv b_i(\bmod r_i), b_i\ne 0, b_i\in\Gamma_{r_i}, i=1,\cdots,s_2$

记 $B(X)=\bigcap_{r\in Q_1(X)}B_0^r(X)$，则 $|B(X)|=\alpha\cdot X$，这里 $\alpha=\prod_{r\in Q_1(X)}(1-\frac{1}{r})$

①$|B(X)\cap D^{r_1}(X)|=|B(X)|-2|B([\frac{X}{r_1}])|$

$$=\alpha\cdot X(1-\frac{2}{r_1})+2(\frac{\alpha X}{r_1}-|B([\frac{X}{r_1}])|)$$

$$|B(X)\cap D^{r_1}(X)|-X\cdot\alpha\cdot\beta_1=2(\alpha\cdot[\frac{X}{r_1}]-|B([\frac{X}{r_1}])|)+\delta_0$$

这里$\beta_1=1-\frac{2}{r_1}$，$\delta_0=\frac{2b_1}{r_1}\cdot\alpha$

②$|B(X)\cap(\bigcap_{i=1}^{2}D^{r_i}(X))|=|B(X)\cap D^{r_1}(X)|-2|B([\frac{X}{r_2}])\cap D_{c_1}^{r_1}([\frac{X}{r_2}])|$

这里$D_{c_1}^{r_1}([\frac{X}{r_2}])=N([\frac{X}{r_2}])\Big/(E_0^{r_1}([\frac{X}{r_2}])\cup E_{c_1}^{r_1}([\frac{X}{r_2}]))$

c_1满足$c_1\cdot r_2\equiv b_1(\bmod r_1),c_1\neq 0$且$c_1\in\Gamma_{r_1}$

$$|B(X)\cap(\bigcap_{i=1}^{2}D^{r_i}(X))|-X\cdot\alpha\cdot\prod_{i=1}^{2}\beta_i$$
$$=|B(X)\cap D^{r_1}(X)|-X\cdot\alpha\cdot\beta_1+2([\frac{X}{r_2}]\cdot\alpha\cdot\beta_1-|B([\frac{X}{r_2}])\cap D_{c_1}^{r_1}([\frac{X}{r_2}])|)+\delta_1$$

这里$\beta_i=1-\frac{2}{r_i}$，$i=1,2$　　$\delta_1=\frac{2b_2}{r_2}\cdot\alpha\cdot\beta_1$

③$|B(X)\cap(\bigcap_{i=1}^{k}D^{r_i}(X))|=|B(X)\cap(\bigcap_{i=1}^{k-1}D^{r_i}(X))|-2|B([\frac{X}{r_k}])\cap(\bigcap_{i=1}^{k-1}D_{d_i}^{r_i}([\frac{X}{r_k}]))|$

这里$D_{d_i}^{r_i}([\frac{X}{r_k}])=N([\frac{X}{r_k}])\Big/(E_0^{r_i}([\frac{X}{r_k}])\cup E_{d_i}^{r_i}([\frac{X}{r_k}]))$

d_i满足$d_i\cdot r_k\equiv b_i(\bmod r_i),d_i\neq 0$且$d_i\in\Gamma_{r_i},i=1,2,\cdots,k-1$

$$|B(X)\cap(\bigcap_{i=1}^{k}D^{r_i}(X))|-X\cdot\alpha\cdot\prod_{i=1}^{k}\beta_i$$
$$=|B(X)\cap(\bigcap_{i=1}^{k-1}D^{r_i}(X))|-X\cdot\alpha\cdot\prod_{i=1}^{k-1}\beta_i+2([\frac{X}{r_k}]\cdot\alpha\cdot\prod_{i=1}^{k-1}\beta_i-|B([\frac{X}{r_k}])\cap(\bigcap_{i=1}^{k-1}D_{d_i}^{r_i}([\frac{X}{r_k}]))|)+\delta_{k-1}$$

这里$\beta_i=1-\frac{2}{r_i}$，$i=1,2,\cdots,k$　　$\delta_{k-1}=\frac{2b_k}{r_k}\cdot\alpha\cdot\prod_{i=1}^{k-1}\beta_i,k=2,\cdots,s_2$

令$T_k(X)=|B(X)\cap(\bigcap_{i=1}^{k}D^{r_i}(X))|-X\cdot\alpha\cdot\prod_{i=1}^{k}\beta_i$

$$T'_{k-1}([\frac{X}{r_k}])=[\frac{X}{r_k}]\cdot\alpha\cdot\prod_{i=1}^{k-1}\beta_i-|B([\frac{X}{r_k}])\cap(\bigcap_{i=1}^{k-1}D_{d_i}^{r_i}([\frac{X}{r_k}]))|$$

$$T'_0([\frac{X}{r_1}])=\alpha\cdot[\frac{X}{r_1}]-|B([\frac{X}{r_1}])|$$

则$T_{s_2}(X)=2(T'_0([\frac{X}{r_1}])+T'_1([\frac{X}{r_2}])+\cdots+T'_{s_2-1}([\frac{X}{r_{s_2}}]))+\sum_{k=1}^{s_2}\delta_{k-1}$ (17)

5）设$m_k=r_1\cdots r_k(k=1,2,\cdots,s_2),m=\prod_{r\in Q_1(X)}r$

$$X\equiv e_k(\bmod mm_k),e_k\in\Gamma_{mm_k}$$

由于$\frac{X-e_k}{r_k}\equiv 0(\bmod mm_{k-1})$

$$\therefore[\frac{X}{r_k}]-[\frac{e_k}{r_k}]\equiv 0(\bmod mm_{k-1})$$

$$\therefore T'_{k-1}([\frac{X}{r_k}])=T'_{k-1}([\frac{e_k}{r_k}]),k=1,2,\cdots,s_2$$

$\therefore T_{s_2}(X)=2(T'_0([\frac{e_1}{r_1}])+T'_1([\frac{e_2}{r_2}])+\cdots+T'_{s_2-1}([\frac{e_{s_2}}{r_{s_2}}]))+\sum_{k=1}^{s_2}\delta_{k-1}$ (18)

$$\because T'_{k-1}([\frac{X}{r_k}])>-\log_2{}^X,k=1,2,\cdots,s_2$$

$$\therefore T_{s_2}(X)>-2s_2\cdot\log_2{}^X$$

$$\because 2\in Q_1(X)$$

$$|T(X)|>\frac{X}{2}\cdot\prod_{i=2}^{s}(1-\frac{2}{p_i})-2s\cdot\log_2 X-2,s=\Phi([\sqrt{X}])$$

当X较大时，比如$X\geq 2^{30}$时，$\frac{X}{2}\cdot\prod_{i=2}^{s}(1-\frac{2}{p_i})>10\sqrt{X}$

而$s=\Phi([\sqrt{X}])<\frac{2\sqrt{X}}{\log_2{}^{\sqrt{X}}}$ $\therefore s\log_2{}^X<4\sqrt{X}$

$|T(X)| > 2\sqrt{X}$

$\therefore$ 当$X \geq 2^{30}$时，$T(X)$为非空集合

任取$x_0 \in T(X)$, 则$p_i = x_0, p_j = X - x_0$皆为质数

$\therefore X = p_i + p_j$　　结论成立。