DOI:10.19789/j.1004-9398.2015.06.001

一个整数表示成两个整数平方和的唯一性

朱一心
(首都师范大学数学科学学院,北京 100048)

摘 要

对于一个可以表示成两个整数平方和的整数,通过其素因数分解式,给出平方和的不同表示方法计算公式,因此给出一个正整数可以唯一表示成两个整数的平方和的充要条件.

关键词: 平方和,素因数分解,唯一分解整环.
中图分类号: O156

所谓一个正整数能唯一表成两个非负整数的平方和是指:若 $n = a^2 + b^2 = u^2 + v^2$ 则有 $a = u, b = v$ 或者 $a = v, b = u$. 我们将数论中相关的基本结论写在一个引理中,可以参见[2,第四章],[3,第四章§8],或者[1,Section18].

引理 (1). 方程 $s^2 \equiv -1 \pmod p$ 对素数 $p = 4m + 1$ 有两个解,对 $p = 2$ 有一个解,对素数 $p = 4m + 3$ 没有解.

(2). 形如 $4m + 3$ 的自然数不能表示成两个整数的平方和.

(3). 形如 $4m + 1$ 的素数可以表示成两个整数的平方和,且表法唯一.

(4). 正整数 n 可以表示成两个整数的和平方和当且仅当 n 的每个形如 $4m + 3$ 的素因子的重数是偶数.

对 $n = a^2 + b^2$,称为 n 的平方和分解,当 $ab \neq 0$ 时称为非平凡分解,即 a, b 都是正整数;当 $ab = 0$ 时称为平凡分解,显然 n 存在平凡平方和分解当且仅当 n 本身是一个平方数;当 $ab \neq 0, (a, b) = 1$ 时称为 n 的互素平方和分解.

记 I 为虚数单位,即 $I^2 = -1$. $\mathrm{Z}(I) = \{x + yI \mid x, y \in \mathrm{Z}\}$,易知这是一个唯一分解整环. 若 $n = a^2 + b^2$,则 n 在 $\mathrm{Z}(I)$ 上对应有四个等价的因数分解:

$$n = (a + bI)(a - bI) = (-a - bI)(-a + bI) = (b - aI)(b + aI) = (-b + aI)(-b - aI)$$

这是因为 $\mathrm{Z}(I)$ 上恰有四个可逆元 $1, -1, I, -I$,而

$$-a - bI = -(a + bI), b - aI = -I(a + bI), -b + aI = I(a + bI)$$

就是说如果 $n = (a + bI)(a - bI) = AB$ 是 $\mathrm{Z}(I)$ 上的因数分解,则 $n = (-A)(-B) = (-IA)(IB) = (IA)(-IB)$ 在 Z 上对应的是同样的平方和分解,在下面的讨论中,我们将不刻意区分说明同一个平方和分解在 $\mathrm{Z}(I)$ 中的不同因数分解表达.

我们可以得到如下定理.

定理 设正整数 $n = 2^{\alpha} p_1^{2\alpha_1+1} \cdots p_r^{2\alpha_r+1} q_1^{2\beta_1} \cdots q_s^{2\beta_s} w_1^{2\gamma_1} \cdots w_t^{2\gamma_t}$,其中 p_i, q_j 是形如 $4m+1$ 的不同素数;w_k 是形如 $4m+3$ 的不同素数;$\alpha, \alpha_i, \beta_j, \gamma_k, r, s, t$ 是非负整数,则:

(1). n 的不同的平方和分解个数为

$$\begin{cases} 1, & r = s = 0; \\ \sum_{k=1}^{s} 2^{k-1}\Delta_k + 1, & r = 0, s \geqslant 1; \\ 2^{r-1}\prod_{i=1}^{r}(\alpha_i + 1), & s = 0, r \geqslant 1; \\ 2^{r-1}\prod_{i=1}^{r}(\alpha_i + 1)\left(\sum_{k=1}^{s} 2^k\Delta_k + 1\right), & r \geqslant 1, s \geqslant 1 \end{cases}$$

其中当 $\alpha \geqslant 2$ 或 $t \geqslant 1$ 时没有互素分解;当 $\alpha = 0$ 或 1,且 $t = 0$ 时有 2^{r+s-1} 个互素分解,它们全是由 $p_i^{2\alpha_i+1}$ 以及 $q_j^{2\beta_j}$ 的互素分解乘积组成的;当 $r \geqslant 1$,或 $r = 0$ 且 α 为奇数时没有平凡分解;当 $r = 0$ 且 α 为偶数时有唯一一个平凡分解.

此处 Δ_k 是 k 个不同的 β_j 乘积的和,即 $\beta_1, \cdots, \beta_s$ 的 k 次基本对称多项式.

(2). 特别地,n 的平方和分解唯一当且仅当 n

收稿日期:2014-09-06

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的所有形如 $4m+1$ 的素因子至多只有一个,即 $n=2^{\alpha}w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$ 或 $n=2^{\alpha}p_1w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$.

证明: 由引理(4),知 $n=2^{\alpha}p_1^{2\alpha_1+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$ 可以平方和分解. 如果结论(1)成立,则 n 有唯一平方和分解当且仅当 $r=s=0$ 或 $s=0$,$r=1$,$\alpha_1=0$,结论(2)显然成立. 我们通过以下 7 个断言证明结论(1)成立.

断言 1: 若素数 $p=4m+3$ 整除 $n=a^2+b^2$,则 $p\mid a$,$p\mid b$.

证明: 否则假设 p 不整除 a,在域 Z_p 中有 $a^{-2}a^2+a^{-2}b^2\equiv 0$,$1+(a^{-1}b)^2\equiv 0(\bmod p)$,与引理(1)矛盾. 由此可见,若 n 有互素平方和分解,则必有 $t=0$.

由断言 1,我们可以假定

$$n=a^2+b^2=2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r},$$

其中 p_i 为形如 $4m+1$ 的素数,α,α_i 为非负整数.

断言 2: 2^{α} 有唯一的平方和分解.

证明: 显然 $1=1^2+0^2$,$2=1^2+1^2$,$4=2^2+0^2$ 都是唯一平方和分解. 当 $\alpha>2$ 时,归纳假设对 $\beta<\alpha$ 都有 2^{β} 的平方和分解唯一.

对于 $2^{\alpha}=a^2+b^2$,显然 a,b 同奇偶. 若 a,b 都是奇数,可设 $a=2a_1+1$,$b=2b_1+1$,于是 $2^{\alpha-1}=(a_1+b_1+1)^2+(a_1-b_1)^2$,但 a_1+b_1+1 与 a_1-b_1 一奇一偶,等式不可能成立.

因此 a,b 都是偶数,可设 $a=2a_1$,$b=2b_1$,于是 $2^{\alpha-2}=a_1^2+b_1^2$ 是唯一平方和分解,因而 $2^{\alpha}=a^2+b^2$ 也是. 由归纳法,$n=2^{\alpha}$ 的平方和分解表达唯一.

事实上,当 $\alpha=2\beta$ 时,有 $2^{\alpha}=(2^{\beta})^2+0^2$ 为平凡分解;当 $\alpha=2\beta+1$ 时,有 $2^{\alpha}=(2^{\beta})^2+(2^{\beta})^2$.

因此 $\alpha\geqslant 2$ 时 2^{α} 没有互素平方和分解,$2=1^2+1^2$ 是 2 仅有的互素平方和分解.

断言 3: 若素数 $p=4m+1$,$\alpha\geqslant 1$,则 p^{α} 有 $\left[\frac{\alpha+2}{2}\right]$(用 $[x]$ 表示对 x 下取整函数)个不同平方和分解,其中互素的平方和分解只有一个,是由 p 的唯一的平方和分解决定的.

证明: 对于 $\alpha=1$,由引理(3),记 $p=x^2+y^2$ 为其唯一平方和分解,而且 $(x,y)=1$,x,y 一奇一偶.

对于 $\alpha\geqslant 2$,设

$$p^{\alpha}=a^2+b^2=(a+bI)(a-bI),$$

则在 $Z(I)$ 上有

$$(x+yI)^{\alpha}(x-yI)^{\alpha}=(a+bI)(a-bI).$$

由于 $Z(I)$ 是唯一因数分解整环,因此 $a+bI$ 是一部分 $(x+yI)$ 的方幂和一部分 $(x-yI)$ 的方幂的乘积,而 $a-bI$ 是余下部分的 $(x+yI)$ 的方幂和 $(x-yI)$ 的方幂的乘积.

考虑到共轭性,设

$$a+bI=(x+yI)^k(x-yI)^l,$$
$$a-bI=(x-yI)^k(x+yI)^l,k+l=\alpha.$$

不妨设 $k\leqslant l$,则

$$a+bI=[(x+yI)(x-yI)]^k(x-yI)^{l-k}=p^k(x-yI)^{\alpha-2k},$$
$$a-bI=p^k(x+yI)^{\alpha-2k}$$

因此

$$p^{\alpha}=(a+bI)(a-bI)=[p^k(x-yI)^{\alpha-2k}][p^k(x+yI)^{\alpha-2k}].$$

记

$$X_k+Y_kI=(x+yI)^{\alpha-2k}=\sum_{i=0}^{\alpha-2k}C_{\alpha-2k}^{i}x^{\alpha-2k-i}(yI)^i,$$

其中

$$X_k=\sum_{i=0}^{\left[\frac{\alpha-2k}{2}\right]}C_{\alpha-2k}^{2i}x^{\alpha-2k-2i}(-1)^iy^{2i},$$
$$Y_k=\sum_{i=0}^{\left[\frac{\alpha-2k-1}{2}\right]}C_{\alpha-2k}^{2i+1}x^{\alpha-2k-2i-1}(-1)^iy^{2i+1}.$$

则 $X_k^2+Y_k^2=p^{\alpha-2k}$,而 p^{α} 恰好有如下 $\left[\frac{\alpha}{2}\right]+1=\left[\frac{\alpha+2}{2}\right]$ 个平方和分解:

$$\rho^{\alpha}=(p^kX_k)^2+(p^kY_k)^2,0\leqslant k\leqslant\left[\frac{\alpha}{2}\right].$$

若 d 是 X_k,Y_k 的最大公因数,则 $d\mid X_k^2+Y_k^2=p^{\alpha-2k}$. 因此 d 是 p 方幂,$X_k+Y_kI=(x+yI)^{\alpha-2k}$ 在 $Z(I)$ 的因数分解式中有因数 $p=(x+yI)(x-yI)$,与因数唯一分解性不合. 于是 $d=1$,即 X_k,Y_k 互素. 此即证明了只有当 $k=0$ 时 $p^{\alpha}=X_0^2+Y_0^2$ 才是互素分解. 其中

$$X_0=\sum_{i=0}^{\left[\frac{\alpha}{2}\right]}C_{\alpha}^{2i}x^{\alpha-2i}(-1)^iy^{2i},$$
$$Y_0=\sum_{i=0}^{\left[\frac{\alpha-1}{2}\right]}C_{\alpha}^{2i+1}x^{\alpha-2i-1}(-1)^iy^{2i+1}.$$

事实上,对于 $p^{\alpha}=a^2+b^2$,若 a,b 有公因数,必为 p 方幂. 设 $a=p^kX_k$,$b=p^kY_k$,则 p 不整除 X_k 与 Y_k,而 $p^{\alpha-2k}=X_k^2+Y_k^2$ 是互素分解,而且有 $X_k+Y_kI=(x+yI)^{\alpha-2k}$.

断言 4: 若 p,q 是两个不同的形如 $4k+1$ 的素

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

数,$n = p^\alpha = a^2 + b^2$,$m = q^\beta = x^2 + y^2$ 是两个互素的平方和分解,则 $nm = (ax - by)^2 + (ay + bx)^2 = (ax + by)^2 + (ay - bx)^2$ 是仅有两个不同的互素平方和分解.

证明: 显然

$$\begin{aligned} nm &= [(a + bI)(x + yI)][(a - bI)(x - yI)] \\ &= [(a + bI)(x - yI)][(a - bI)(x + yI)] \\ &= [(ax - by) + (ay + bx)I][(ax - by) - (ay + bx)I] \\ &= [(ax + by) + (bx - ay)I][(ax + by) - (bx - ay)I] \end{aligned}$$

又由 $(a,b) = (x,y) = 1$,则 $(a + bI)(x + yI)$ 不等于以下 8 个中任一个

$$\pm(a + bI)(x - yI),\ \pm(a - bI)(x + yI),$$
$$\pm I(a + bI)(x - yI),\ \pm I(a - bI)(x + yI),$$

因此上述两个因数分解在 $Z(I)$ 中是不同的,从而对应于 Z 中不同的平方和分解.

注意到 $(ax - by)$,$(ay + bx)$ 若有公因数必是 p 或 q 方幂,设若 p 是 $(ax - by)$,$(ay + bx)$ 的公因数,即 $p \mid (ax - by) + (ay + bx)I$,$p \mid (a + bI)(x + yI)$,必有 $p \mid (a + bI)$,此与 a,b 互素不合. 因此上述两个分解是互素的.

最后,由断言 3,$n = p^\alpha = a^2 + b^2$ 由 p 的唯一的互素平方和分解决定,$m = q^\beta = x^2 + y^2$ 由 q 的唯一的平方和分解决定. 若 $nm = X^2 + Y^2$ 是互素的平方和分解,考虑 $nm = (X + YI)(X - YI)$ 在 $Z(I)$ 中的分解,知道 $a + bI$ 和 $x + yI$ 是 $X + YI$ 或者 $X - YI$ 的因数,由因数分解唯一性,知 $X + YI$ 等价于

$$(a + bI)(x + yI),(a + bI)(x - yI),$$
$$(a - bI)(x + yI),(a - bI)(x - yI)$$

之一,因此对应的平方和分解为 $(ax - by)^2 + (ay + bx)^2$,$(ax + by)^2 + (ay - bx)^2$ 之一.

上面证明还可以看到,只要 $n = p^\alpha = a^2 + b^2$,$m = q^\beta = x^2 + y^2$ 都不是平凡的平方和分解,则 $nm = (ax - by)^2 + (ay + bx)^2 = (ax + by)^2 + (ay - bx)^2$ 就是两个不同的平方和分解. 当 $m = q^\beta = (q^{\beta/2})^2 + 0^2$ 是平凡分解时,$nm = (ax - by)^2 + (ay + bx)^2 = (ax + by)^2 + (ay - bx)^2 = (aq^{\beta/2})^2 + (bq^{\beta/2})^2$ 只是一个平方和分解.

断言 5: 若 p,q 是两个不同的形如 $4k + 1$ 的素数,$n = p^\alpha, m = q^\beta$,则 nm 的不同平方和分解个数为:

$$\begin{cases} 2(k + 1)(l + 1), & \alpha = 2k + 1, \beta = 2l + 1; \\ (k + 1)(2l + 1), & \alpha = 2k + 1, \beta = 2l; \\ (2k + 1)(l + 1), & \alpha = 2k, \beta = 2l + 1; \\ 2kl + k + l + 1, & \alpha = 2k, \beta = 2l. \end{cases}$$

证明: 由断言 4,$p^\alpha q^\beta$ 的平方和分解是由 p^α 的平方分解和与 q^β 的平方和分解组成的,其中的互素分解只有 2 个. p^α 的一个非平凡平方分解和与 q^β 的一个非平凡平方和分解可以组成 $p^\alpha q^\beta$ 的 2 个不同的平方和分解. p^α 的一个是平凡平方和分解与 q^β 的平方和分解只能组成 $p^\alpha q^\beta$ 的一个平方和分解. 而由断言 3,当 α 是偶数时,p^α 才有平凡的平方和分解.

当 $\alpha = 2k + 1, \beta = 2l + 1$ 时,$p^\alpha q^\beta$ 的不同平方和分解数为 $2(k + 1)(l + 1)$.

当 $\alpha = 2k + 1, \beta = 2l$ 时,$p^\alpha q^\beta$ 的不同平方和分解数为 $2(k + 1)l + k + 1$.

当 $\alpha = 2k, \beta = 2l + 1$ 时,$p^\alpha q^\beta$ 的不同平方和分解数为 $2k(l + 1) + l + 1$.

当 $\alpha = 2k, \beta = 2l$ 时,$p^\alpha q^\beta$ 的不同平方和分解数为 $2kl + k + l + 1$,其中有一个是平凡分解.

断言 6: 若 n 是形如 $4m + 1$ 的素数的乘积,有 N 个不同的平方和分解,N_1 个互素分解. 则 $2^\alpha \cdot n\ (\alpha \geqslant 1)$ 有 N 个不同平方和分解,当 $\alpha \geqslant 2$ 时其中没有互素分解,当 $\alpha = 1$ 时其中有 N_1 个互素分解.

证明: 由断言 2,记 2^α 的唯一平方和分解式为

$$2^\alpha = u_\alpha^2 + v_\alpha^2 = (u_\alpha + v_\alpha I)(u_\alpha - v_\alpha I),$$

其中 $u_{2\beta+1} = v_{2\beta+1} = 2^\beta$,而 $u_{2\beta} = 2^\beta, v_{2\beta} = 0$. 设

$$2^\alpha \cdot n = a^2 + b^2 = (a + bI)(a - bI),$$

则在 $Z(I)$ 的因数分解式中,$u_\alpha + v_\alpha I$ 或者 $u_\alpha - v_\alpha I$ 其中之一是 $a + bI$ 的因数. 若记 $a + bI$ 的其它因数的乘积为 $X + YI$,则

$$\begin{aligned} &(a + bI)(a - bI) \\ &= (u_\alpha + v_\alpha I)(u_\alpha - v_\alpha I)(X + YI)(X - YI) = 2^\alpha \cdot n \end{aligned}$$

于是 $(X + YI)(X - YI) = n$,即 $X + YI$ 有 N 种可能.

当 $\alpha = 2\beta + 1$ 时,$a + bI$ 等价于以下四种情况之一:

$$\begin{aligned} &(2^\beta + 2^\beta I)(X + YI) = 2^\beta((X - Y) + (X + Y)I), \\ &(2^\beta + 2^\beta I)(X - YI) = 2^\beta((X + Y) + (X - Y)I), \\ &(2^\beta - 2^\beta I)(X + YI) = 2^\beta((X + Y) - (X - Y)I), \\ &(2^\beta - 2^\beta I)(X - YI) = 2^\beta((X - Y) - (X + Y)I), \end{aligned}$$

对应 $2^\alpha \cdot n$ 的分解都是 $(2^\beta(X + Y))^2 + (2^\beta(X - Y))^2$. 其中 $\beta = 0$ 时,$2n = (X + Y)^2 + (X - Y)^2$ 是互素分解,因为 $(X + Y, X - Y) = (X,Y) = 1$.

当 $\alpha = 2\beta$ 时,$a + bI$ 等价于 $2^\beta(X + YI)$ 或者

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$2^{\beta}(X-YI)$ 之一,对应 $2^{\alpha}\cdot n$ 的分解是 $(2^{\beta}X)^2+(2^{\beta}Y)^2$.

于是 $2^{\alpha}\cdot n$ 有 N 个不同的平方和分解,当 $\alpha\geqslant 1$ 时其中没有互素的分解. 当 $\alpha=1$ 时有 N_1 个互素分解.

断言 7: 设 $n=2^{\alpha}p_1^{2\alpha_1+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}$,其中 p_i, q_j 为形如 $4m+1$ 的素数,r 为正整数,$\alpha,\alpha_i,\beta_j,s$ 为非负整数. 则 n 有 $2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)\left(\sum_{k=1}^{s}2^k\Delta_k+1\right)$ 个不同的平方和分解; 其中当 $\alpha\geqslant 2$ 时没有互素分解,当 $\alpha=0,1$ 时有 2^{r+s-1} 个互素分解; $r\geqslant 1$ 时没有平凡分解.

证明: $Z(I)$ 上的因数分解唯一性,若 $n=a^2+b^2$,则 $a+bI$ 在 $Z(I)$ 上的不可约因数是分别由 2^{α}, $p_i^{2\alpha_i+1}$, $q_j^{2\beta_j}$ 的不可约因数组成的,即 n 的平方和分解是由 2^{α}, $p_i^{2\alpha_i+1}$, $q_j^{2\beta_j}$ 的平方和分解按照断言 4 和断言 5 的方法乘积组成的,而且互素的分解由互素的分解乘积组成.

下面按照断言 5,计算 $p_1^{2\alpha_1+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}$ 的平方和分解个数.

$p_1^{2\alpha_1+1}\cdots p_r^{2\alpha_r+1}$ 的平和方分解个数为 $2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)$,其中有 2^{r-1} 个互素.

$q_1^{2\beta_1}q_2^{2\beta_2}$ 的平方和分解个数为 $2\beta_1\beta_2+\beta_1+\beta_2+1$,其中有 1 个互素 1 个平凡.

$q_1^{2\beta_1}q_2^{2\beta_2}q_3^{2\beta_3}$ 的平方和分解个数为

$$2(2\beta_1\beta_2+\beta_1+\beta_2)\beta_3+(2\beta_1\beta_2+\beta_1+\beta_2)+\beta_3+1=4\Delta_3+2\Delta_2+\Delta_1+1$$

其中有 2 个互素 1 个平凡.

用归纳法可证 $q_1^{2\beta_1}\cdots q_s^{2\beta_s}$ 的平方和分解个数为 $\sum_{k=1}^{s}2^{k-1}\Delta_k+1$ 个平方和分解,其中有 2^{s-1} 个互素分解 1 个平凡.

因此,$p_1^{2\alpha+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}$ 的平方和分解个数为

$$2\cdot 2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)\sum_{k=1}^{s}2^{k-1}\Delta_k+2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)=2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)\left(\sum_{k=1}^{s}2^k\Delta_k+1\right)$$

其中有 $2\cdot 2^{r-1}2^{s-1}=2^{r+s-1}$ 个互素.

于是,按照断言 4,$2^{\alpha}p_r^{2\alpha_r+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}$ 的平方和分解个数为

$$2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)\left(\sum_{k=1}^{s}2^k\Delta_k+1\right)$$

由上述 7 个断言,定理结论成立. □

在进行下一步讨论之前,让我们来考察定理证明中不同情形的一些例子,以便加深对证明的体会.

断言 3 中关于 p^{α} 的分解: 对于 $5=2^2+1^2$,有

$$\begin{aligned}5^2&=5^2+0^2\\&=(2+I)^2(2-I)^2=(3+4I)(3-4I)\\&=3^2+4^2\\5^3&=(5\cdot 1)^2+(5\cdot 2)^2\\&=(2+I)^3(2-I)^3=(2+11I)(2-11I)\\&=2^2+11^2\\5^4&=(5^2)^2+0^2\\&=[5(2+I)^2][5(2-I)^2]\\&=[5(3+4I)][5(3-4I)]\\&=(5\cdot 3)^2+(5\cdot 4)^2\\&=(2+I)^4(2-I)^4\\&=(-7+24I)(-7-24I)=7^2+24^2\end{aligned}$$

类似地对 $13=3^2+2^2$,注意到

$$\begin{aligned}(3+2I)^2&=5+12I,\\(3+2I)^3&=-9+46I,\\(3+2I)^4&=-119+120I,\\(3+2I)^5&=-597+122I,\end{aligned}$$

有

$$\begin{aligned}13^2&=13^2+0^2=5^2+12^2\\13^3&=(13\cdot 3)^2+(13\cdot 2)^2=9^2+46^2\\13^4&=(13^2)^2+0^2=(13\cdot 5)^2+(13\cdot 12)^2\\&=119^2+120^2\\13^5&=(13^2\cdot 3)^2+(13^2\cdot 2)^2\\&=(13\cdot 9)^2+(13\cdot 46)^2=597^2+122^2\end{aligned}$$

5^4 有 $3=\left[\frac{4+2}{2}\right]$ 个分解,13^5 有 $3=\left[\frac{5+2}{2}\right]$ 个分解.

断言 5 中关于 $p^{2\alpha+1}q^{2\beta}$ 的分解:

$$\begin{aligned}5^4\cdot 13^5&=(5^2\cdot 13^2\cdot 3)^2+(5^2\cdot 13^2\cdot 2)^2\\&=(5^2\cdot 13\cdot 9)^2+(5^2\cdot 13\cdot 46)^2\\&=(5^2\cdot 597)^2+(5^2\cdot 122)^2\end{aligned}$$

注意到

$$\begin{aligned}&[5\cdot 3+5\cdot 4I)(13^2\cdot 3+13^2\cdot 2I)]\cdot\\&[5\cdot 3-5\cdot 4I)(13^2\cdot 3-13^2\cdot 2I)]\\=\ &[5\cdot 3+5\cdot 4I)(13^2\cdot 3-13^2\cdot 2I)]\cdot\\&[5\cdot 3-5\cdot 4I)(13^2\cdot 3+13^2\cdot 2I)],\end{aligned}$$

而

$$\begin{aligned}&(5\cdot 3+5\cdot 4I)(13^2\cdot 3+13^2\cdot 2I)\\=\ &5\cdot 13^2(1+18I),\\&(5\cdot 3+5\cdot 4I)(13^2\cdot 3-13^2\cdot 2I)\\=\ &5\cdot 13^2(17+6I),\end{aligned}$$

因此

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$$5^4\cdot13^5=[(5\cdot3)^2+(5\cdot4)^2][(13^2\cdot3)^2+(13^2\cdot2)^2]$$
$$=(5\cdot13^2)^2+(5\cdot13^2\cdot18)^2$$
$$=(5\cdot13^2\cdot17)^2+(5\cdot13^2\cdot6)^2$$

类似地还有下面的分解

$$5^4\cdot13^5=[(5\cdot3)^2+(5\cdot4)^2][(13\cdot9)^2+(13\cdot46)^2]$$
$$=(5\cdot13\cdot157)^2+(5\cdot13\cdot174)^2$$
$$=(5\cdot13\cdot211)^2+(5\cdot13\cdot102)^2$$
$$=[(5\cdot3)^2+(5\cdot4)^2][97^2+122^2]$$
$$=(5\cdot2754)^2+(5\cdot1303)^2$$
$$=(5\cdot2022)^2+(5\cdot2279)^2$$
$$=[7^2+24^2][(13^2\cdot3)^2+(13^2\cdot2)^2]$$
$$=(13^2\cdot27)^2+(13^2\cdot86)^2$$
$$=(13^2\cdot69)^2+(13^2\cdot58)^2$$
$$=[7^2+24^2][(13\cdot9)^2+(13\cdot46)^2]$$
$$=(13\cdot1167)^2+(13\cdot106)^2$$
$$=(13\cdot1041)^2+(13\cdot538)^2$$
$$=[7^2+24^2][97^2+122^2]$$
$$=15182^2+1251^2$$
$$=13474^2+7107^2$$

$5^4\cdot13^5$ 有 $15=(2k+1)(l+1)$ 个平方和分解式，其中最后 $2=2^{1+1-1}$ 个是互素的分解.

依照定理的结论，我们可以寻找具有平方和分解个数较少的自然数，比如得到一个正整数恰有两个非平凡的平方和分解的充要条件.

推论 1　正整数 n 恰有两个非平凡的平方和分解，当且仅当 n 有个平方和分解且以下之一成立:

(1). $n=2^{2\alpha+1}p^2w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$;

(2). $n=2^{2\alpha}p^4w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$;

(3). $n=2^{\alpha}p^3w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$;

(4). $n=2^{\alpha}pqw_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$.

其中 p,q 是形如 $4m+1$ 的素数，w_k 是形如 $4m+3$ 的素数，α,γ_k 是非负整数.

证明: 设 $n=2^{\alpha}p_1^{2\alpha_1+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}w_1^{2\gamma_1}\cdots w_t^{2\gamma_t}$. 其中 p_i,q_j 是形如 $4m+1$ 的素数; w_k 是形如 $4m+3$ 的素数; $\alpha,\alpha_i,\beta_j,\gamma_k,r,s,t$ 为非负整数. 由定理 1 的断言 1，只要对 $n=2^{\alpha}p_1^{2\alpha_1+1}\cdots p_r^{2\alpha_r+1}q_1^{2\beta_1}\cdots q_s^{2\beta_s}$ 讨论.

当 $r=0$ 时，且若 α 是奇数，则 n 不是平方数，因此 n 有 2 个平方和分解. 于是 $2=\sum_{k=1}^{s}2^{k-1}\Delta_k+1$，可得 $s=1,\beta_1=1,n=2^{2\alpha+1}q_1^2$.

当 $r=0$ 时，且若 α 是偶数，则 n 是平方数，因此 n 有 3 个平方和分解. 于是 $3=\sum_{k=1}^{s}2^{k-1}\Delta_k+1$，可得 $s=1,\beta_1=2,n=2^{2\alpha}q_1^4$.

当 $r\geqslant1$ 时，n 不是平方数，因此 n 有 2 个平方和分解. 于是 $2=2^{r-1}\prod_{i=1}^{r}(\alpha_i+1)(\sum_{k=1}^{s}2^k\Delta_k+1)$，可得 $r=1,\alpha_1=1,s=0$，或者 $r=2,\alpha_1=\alpha_2=0,s=0$，即 $n=2^{\alpha}p_1^3$ 或者 $n=2^{\alpha}p_1p_2$. □

对于平方和中出现 1 的情况，我们有如下特别的结论.

推论 2　设 $p=4m+1$ 是素数，α 是正整数，$p^{\alpha}-1$ 是平方数，则 α 是奇数，$p-1$ 和 m 都是平方数.

证明: 设若 $p^{\alpha}-1$ 是平方数，即有互素平方和分解 $p^{\alpha}=1+y^2$. 由定理证明的断言 3，每一个 p 的方幂都有唯一的互素平方和分解，且由 p 的唯一的平方和分解决定.

当 $\alpha=2\beta$ 是偶数时，记 p^{β} 的唯一的互素平方和分解为 X^2+Y^2，则 $p^{2\beta}=(X^2-Y^2)^2+(2XY)^2$ 是 $p^{2\beta}$ 唯一的互素平方和分解. 必有 $X^2-Y^2=1$，因而 $X=1,Y=0$，不可能.

当 $\alpha=2\beta+1$ 是奇数时，设 $p=x^2+y^2$ 是互素平方和分解，记 p^{α} 的唯一的互素平方和分解为 $X_0^2+Y_0^2$. 由定理 1 的断言 3，可设

$$X_0=\sum_{i=0}^{\beta}C_{2\beta+1}^{2i}x^{2\beta+1-2i}(-1)^iy^{2i},$$
$$Y_0=\sum_{i=0}^{\beta}C_{2\beta+1}^{2i+1}x^{2\beta-2i}(-1)^iy^{2i+1}$$

由 $x\mid X_0,y\mid Y_0$，由于 $X_0=1$ 或者 $Y_0=1$，因此 $x=1$ 或者 $y=1$，即 $p-1$ 是平方数，于是 m 是平方数. □

推论 2 的结论不是充分的，如 $p=5=1+2^2$，但 $5^3-1=124,5^5-1=3124,5^7-1=78124$ 都不是平方数，事实上由于最后三位数是 124，可以证明除了 $5-1$ 外，$5^{2\alpha+1}-1$ 都不是平方数.

对于 $m\leqslant33$，p 是素数的情况列表如下，经过计算对 $1\leqslant\alpha\leqslant7$ 没有找到 α 使得 $p^{2\alpha+1}-1$ 是平方数:

m	1	2	3	5	7	8	10	12	13	18	20	27	28	33
p	5	17	37	101	197	257	401	577	677	1297	1601	2917	3137	4357

(下转第 10 页)

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

A),1996,39: 246 – 263.

[17] S L. Yang, J N. Chen Hopf actions on factor rings and induced Hopf actions [J]. Comm. in Algebra,1997, 25: 1103 – 1110.

[18] F. Panaite A Maschke-type Theorem for Quasi-Hopf Algebras in "In Rings Hopf algebeas and Brauer groups" [M]. Dekker,New York,1998: 201 – 207.

[19] D. Bulacu ,S. Caenepeel. Intergrals for (dual) quasi-Hopf algebras. Applications, QA/0110063v2 18 Oct 2002.

Maschke Type Theorem for Quasi-Hopf Algebra

Yang Cunjie

(School of Mathematical Sciences, Capital Normal University,Beijing 100048)

Abstract

We prove that Maschke type theorem for quasi-Hopf algebra.

Key words: quasi-Hopf algebra, gauge transformation, quasi two-cocycle, Maschke type theorem.

(上接第 5 页)

参 考 文 献

[1] Underwood Dudley. Elementary Number Theory (Second Edition). W. H. Freeman and Company, San Francisco,1978.

[2] Martin Aigner, Günter M. Ziegler. Proofs from THE BOOK(中译本) 数学天书中的证明(冯荣权,宋春伟,宗传明译). 北京: 高等教育出版社,2009.

[3] 柯召,孙琦. 数论讲义. 北京: 高等教育出版社,1986.

On the Uniqueness for an Integer to be a Sum of Two Squares

Zhu Yixin

(School of Mathematical Sciences, Captial Normal University, Beijing 100048)

Abstract

For an integer n which is a sum of two integer squares, such that $n = a^2 + b^2$, we give the formula to counting the number of pairs (a, b), by prime factors of n. And then we get a necessary and sufficient condition for an integer to be a sum of two integer squares in uniquness way.

Key words: sum of two integer squares, prime factor, unique factorization domain.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net