n進表示平方数

高校３年４組６番　伊藤佑樹

1　はじめに

本日は、数学研究部にお越しくださいまして、ありがとうございます。

この記事ではある数字の列があり、その列をあるn進数で表示された整数だと思えば、平方数となるようなnが存在する数字の列を決定することを考えます。例えば、$2,2,5$という数字の列があったとします。これはもちろん10進法で読めば、15^2になっていて、平方数です。また、61進法で読んでも、87^2になっています。これに対して、$1,3,2$という数字の列はどんな進法で見ても、平方数にはなりえません。このように、どんな数字の列が平方数になることがあり、どんな数字の列が平方数にならないかを考えていこうと思います。

それでは、始めたいと思います。

2　準備

必要となる定義をしておこうと思います。

定義 2.1 (オーダー) a,bが0でない整数のとき、bがaで割り切れることを$a \mid b$で表す。
整数nが素数pに対して、$p^k|n$なるkの最大値を$ord_p n$で表す。

定義 2.2 (合同式) $a,b,n \in \mathbb{Z}$の時、$a-b$がnで割り切れることを

$$a \equiv b \pmod{n}$$

で表す。これをa,bはnを法として合同であるという。

定義 2.3 (Legendre 記号) p：素数

$$x^2 \equiv a \pmod{p}$$

が解を有する時、a を p の平方剰余という。そうでないとき、平方非剰余という。
これをそれぞれ

$$\left(\frac{a}{p}\right) = \pm 1$$

のように表す。

定理 2.4

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

定理 2.5 (平方剰余の相互法則) p, q を相異なる奇素数とする。

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

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

これらをそれぞれ、平方剰余の相互法則、第一補充則、第二補充則と呼ぶ。

定義 2.6 (k 進表示) $a_n.a_{n-1}.\cdots.a_{0(k)}$ で $n+1$ 桁の k 進数を表す。

$$a_n.a_{n-1}.\cdots.a_{0(k)} = \sum_{i=0}^{n} a_i k^i$$

と定義します。(k は 2 以上の自然数、$0 \leq a_i < k$、$a_n \neq 0$,a_i は 10 進法表示)

以下、各 a_i については、10 進法で表します。また、明らかにどの進数について議論しているか分かる場合は書かない場合があります。

命題 2.7 自然数 n を k 進法表示した時、その表示の仕方は一意に定まる。

略証

$$n = a_s.a_{s-1}.\cdots.a_{0(k)} = b_t.b_{t-1}.\cdots.b_{0(k)}$$

と n を 2 通りに表示できたとする。
$a_0 \equiv b_0 \pmod{k}$ で $0 \leq a_0, b_0 \leq k-1$ だから $a_0 = b_0$。こうして、$\dfrac{n-a_0}{k}$ を考えて、同じことをすれば、$a_1 = b_1$。これを繰り返すことで、$s = t, a_i = b_i$ が示される。

証明終

3　1桁の数の場合

この場合は当たり前ですが、次の事実が成り立ちます。

定理 3.1 $n = a_{0(k)}$ が平方数となる $\Leftrightarrow a_0$ が平方数、$a_0 < k$

4　2桁の数の場合

以下、$n = a_1.a_{0(k)}$ が平方数となるものを考える。

定理 4.1 $\exists k$、$n = a_1.a_{0(k)}$ が平方数 $\Leftrightarrow \exists x$、$x^2 \equiv a_0 \pmod{a_1}$

証明
$(\Rightarrow)$ $n = a_1 k + a_0$ が平方数 x^2 となるとき、$x^2 = a_1 k + a_0 \equiv a_0 \pmod{a_1}$
$(\Leftarrow)$ $x^2 \equiv a_0 \pmod{a_1}$ なる x が存在するとき、ある m が存在して、

$$a_1 m + a_0 = x^2$$

と表せる。このとき、$\max(a_1, a_0) < m$ であれば、$a_1.a_{0(m)}$ という表示は成り立ち、これは平方数。しかし $\max(a_1, a_0) \geq m$ であれば、$a_1.a_{0(m)}$ という表示は成り立たない。
ここで、$c \in \mathbb{N}$ とすれば、$(x + ca_1)^2 \equiv a_0 \pmod{a_1}$ も成り立ち、

$$a_1(m + 2cx + c^2 a_1) + a_0 = (x + ca_1)^2$$

より、十分大きな c に対しては、$m + 2cx + c^2 a_1 > a_0, a_1$ となるので、$a_1.a_{0(m+2cx+c^2 a_1)}$ という表示は成り立ち、これは平方数。

証明終

定理 4.2 $x^2 \equiv a_0 \pmod{a_1}$ なる x が存在する条件は以下の通り。
$a_1 = p_1^{i_1} p_2^{i_2} \cdots p_f^{i_f}$ (各 p_i : 素数、$i \neq j$ ならば $p_i \neq p_j$) とする。

1. p_i:奇素数、$a_0 = c p_i^l (c \nmid p_i)$ とおけば、l は 0 または偶数で、$\left(\dfrac{c}{p_i}\right) = 1$

2. $ord_2 a_1 = i \geq 1$ のとき、$a_0 = c 2^l (c \nmid 2)$ とおけば、l は 0 または偶数。そして以下のようになる。

   (a) $i \leq l + 1$ のとき、このような x は存在する。

   (b) $i - l = 2$ のとき、$c \equiv 1 \pmod{4}$

(c) $i-l \geq 3$ のとき、$c \equiv 1 \pmod 8$

証明
関君の部誌がこれの一般的な場合について述べています。証明についてはそちらを御覧下さい。こちらでは、2 乗について議論しているので、少し一般的な場合よりは、証明は楽になりますが。

証明終

これらの二つの定理を組み合わせることにより、$a_1.a_{0(k)}$ が平方数となる k を持つかどうかを判定することが出来る。

5　3 桁の数の場合

5.1　準備その 2-二次体-

3 桁の場合を議論するうえで、二次体という概念を導入する。

定義 5.1 (二次体) $m \in \mathbb{Z}$ は平方因数を持たないとする。

$$x + y\sqrt{m} (x, y \in \mathbb{Q})$$

のような形の数の集合を二次体と呼び、$K(\sqrt{m})$ と表す。

定義 5.2 (二次体の整数) 二次の無理数が $\mathbb{Z}$ 係数の二次方程式

$$x^2 + ax + b = 0$$

の解となるとき、これを二次体の整数という。これに対し、$\mathbb{Z}$ の元を有理整数と呼ぶことにする。

この整数の定義から、二次体の整数を記述することができる。

定理 5.3 二次体 $K(\sqrt{m})$ の整数は、$x, y \in \mathbb{Z}$ として、
$m \equiv 2, 3 \pmod 4$ のとき、$x + y\sqrt{m}$
$m \equiv 1 \pmod 4$ のとき、$\dfrac{x + y\sqrt{m}}{2}$、$x \equiv y \pmod 2$

定義 5.4 (ノルム、共役) 二次体 $K(\sqrt{m})$ に属する 2 数、$\alpha = x + y\sqrt{m}, \alpha' = x - y\sqrt{m}$ を互いに共役という。
$N(\alpha) = \alpha\alpha' = x^2 - my^2$ と定め、これを α のノルムという。

定義 5.5 (倍数、約数) $K(\sqrt{m})$ の整数 α, β の商 $\dfrac{\alpha}{\beta} = \gamma$ が整数のとき、α は β で割り切れるといい、α は β の倍数、β は α の約数であるという。

定義 5.6 (単数) $K(\sqrt{m})$ の整数 ϵ が $N(\epsilon) = \pm 1$ となるとき、ϵ を単数という。これは全ての整数の約数になっている。

定理 5.7 (基本単数) $m > 0$ のとき、二次体 $K(\sqrt{m})$ には無数に単数があり、それらは一つの単数 ϵ_0 によって、次の形に表せる。

$$\pm\epsilon_0^n (n \in \mathbb{Z})$$

このような ϵ_0 のうち 1 より大きなものを基本単数と呼ぶ。

定理 5.8 $m \equiv 1 \pmod 4$ のとき、二次体 $K(\sqrt{m})$ の基本単数を ϵ_0 とすれば、

$$\epsilon_0^3 = s + t\sqrt{m} (s, t \in \mathbb{N})$$

定義 5.9 (イデアル) 二次体 $K(\sqrt{m})$ の整数の集合が下記の性質を持つとき、この集合をイデアルという。

1. この集合に属する任意の二つの整数 α, β の和、差がこの集合に属する。

2. この集合に属する整数 α の任意の倍数がこの集合に属する。

定義 5.10 (単項イデアル) 与えられた整数 α の全ての倍数 $\alpha\xi$ の集合はイデアルになっている。これを (α) と表し、α から生じる単項イデアルとよぶ。

定義 5.11 (イデアルの類別) 二次体 K において、イデアル A の各数にある数 ρ を乗じて、その積が全部整数であるならば、それらの積の集合はイデアルとなる。これを ρA で表す。このように、二つのイデアル A, B の間に

$$B = \rho A$$

という関係があるとき、A, B は対等であるという。これを $A \sim B$ で表す。このとき、

$$A \sim A$$

$$A \sim B \Longrightarrow B \sim A$$

$$A \sim B, B \sim C \Longrightarrow A \sim C$$

がなりたつので、これらを類別することが可能になる。つまり、対等とは同類ということである。単項イデアルは互いに対等なので、一つの類をなす。これを主類と呼ぶ。

定義 5.12 (判別式) $m \equiv 2,3 \pmod 4$ のとき、$d = 4m$
$m \equiv 1 \pmod 4$ のとき、$d = m$
この d を二次体 $K(\sqrt{m})$ の判別式という。

定義 5.13 二次体 $K(\sqrt{m})$ に対して、以下のように有理素数を 3 種に分ける。
第一種:$\left(\dfrac{m}{p}\right) = 1$ を満たす p:奇素数、$m \equiv 1 \pmod 8$ の時は $p = 2$ も含む
第二種:$\left(\dfrac{m}{q}\right) = -1$ を満たす q:奇素数、$m \equiv 5 \pmod 8$ の時は $q = 2$ も含む
第三種:d の素因数 l

どういうように、この分け方が導かれたかについては、この記事では扱いませんが、次の定理を見ればその有用性が分かるかと思います。

定理 5.14 二次体 $K(\sqrt{m})$ が主類しかイデアルをもたないとき、$x^2 - my^2 = n$ の解について。ϵ_0:基本単数とする。

1. $N(\epsilon_0) = -1$ のとき
   n が第二種の素数を偶数冪含めば、n が正でも負でも解を有する。

2. $N(\epsilon_0) = 1$ のとき
   n が第二種の素数を偶数冪含めば、$\pm n$ のいずれか一方のときのみ解がある。

この証明はイデアル論によりますが、ここでは省かせていただきます。

5.2 $a_2 = 1$ の場合

この場合については、全て判定することが出来た。結果をまとめると、以下のようになる。

定理 5.15 $\exists k$、$1.b.c_{(k)}$ が平方数となる条件は以下の通り。

1. $b^2 - 4c = 0$ のとき、
   必ず平方数となりうる。
2. $b^2 - 4c > 0$、$ord_2(b^2 - 4c) = 0$ のとき

   (a) $b \geq 10$ のとき、$\dfrac{b^2 - 2b + 1}{8} > c$

(b) $b = 7, 9$ のとき、$\dfrac{b^2 - 6b + 1}{4} > c$

(c) $b = 1, 3, 5$ のとき、平方数とはなりえない。

3. $b^2 - 4c > 0$、$ord_2(b^2 - 4c) = 2$ のとき

(a) $b \geq 16$ のとき、$\dfrac{b^2 - 4b + 4}{12} > c$

(b) $b = 14$ のとき、$8 > c$

(c) $b = 2, 4, 6, 8, 10, 12$ のとき、平方数とはなりえない。

4. $b^2 - 4c > 0$、$ord_2(b^2 - 4c) = 3$ のとき
平方数とはなりえない。

5. $b^2 - 4c > 0$、$ord_2(b^2 - 4c) \geq 4$ のとき

(a) $b \geq 28$ のとき、$\dfrac{b^2 - 8b + 16}{20} > c$

(b) $b = 24, 26$ のとき、$\dfrac{b^2 - 24b + 16}{4} > c$

(c) $b < 24$ のとき、平方数とはなりえない。

6. $b^2 - 4c < 0$ のとき
平方数とはなりえない。

証明

つまりは、ある $k, m(k > b, c)$ が存在して、$k^2 + bk + c = m^2$ となるということである。
これを k について解けば、

$$k = \frac{-b \pm \sqrt{b^2 - 4c + 4m^2}}{2}$$

$\dfrac{\sqrt{b^2 - 4c + 4m^2} - b}{2}$ が整数となり、
$max(b, c)$ より大きくならなければならない。

$$b^2 - 4c + 4m^2 = x^2$$

とおいておく。これは

$$(x + 2m)(x - 2m) = b^2 - 4c$$

と変形できることに注意しておく。

1. $b^2-4c=0$
   このとき、$k=\dfrac{2m-b}{2}$ となり、b は偶数であるから、これは整数。
   また、十分大きな m をとれば、$k>b,c$ とできる。
   よって、平方数となりうる。
2. $b^2-4c>0$、$ord_2(b^2-4c)=0$ のとき

   $k>b,c$ の条件を満たすかどうかには、x として最も大きいものをとった場合を考えてみればよい。これは

   $$x+2m=b^2-4c, x-2m=1$$

   の場合である。このとき、

   $$x=\frac{b^2-4c+1}{2}, m=\frac{b^2-4c-1}{4}, k=\frac{b^2-2b+1-4c}{4}$$

   はそれぞれ $b^2-4c\equiv 1 \pmod 4$ より、整数。このとき、$k>b,c$ となる条件を考える。

   $$\frac{b^2-2b+1-4c}{4}>b, \frac{b^2-2b+1-4c}{4}>c$$

   より、

   $$\frac{b^2-6b+1}{4}>c, \frac{b^2-2b+1}{8}>c$$

   あとは、この 2 つの左辺の大小、正負を考慮すれば定理の通りとなる。
3. $b^2-4c>0$、$ord_2(b^2-4c)=2$ のとき

   $k>b,c$ の条件を満たすかどうかには、x として最も大きいものをとった場合を考えてみればよい。$x+2m, x-2m$ の和は偶数、差は 4 の倍数でなければならないので、x が最も大きくとれるのは

   $$x+2m=\frac{b^2-4c}{2}, x-2m=2$$

   の場合である。このとき、

   $$x=\frac{b^2-4c+4}{4}, m=\frac{b^2-4c-4}{8}, k=\frac{b^2-4b+4-4c}{8}$$

   となる。$ord_2(b^2-4c)=2$、b:偶数より、x,m,k は整数となる。このとき、$k>b,c$ となる条件を考える。

   $$\frac{b^2-4b+4-4c}{8}>b, \frac{b^2-4b+4-4c}{8}>c$$

より、

$$\frac{b^2-12b+4}{4}>c, \frac{b^2-4b+4}{12}>c$$

この２つの左辺の大小、正負を考慮すれば定理の通りとなる。

4. $b^2-4c>0$、$ord_2(b^2-4c)=3$ のとき

$x+2m, x-2m$ の和は偶数だから、「$ord_2(x+2m)=2$ かつ $ord_2(x-2m)=1$」または「$ord_2(x+2m)=1$ かつ $ord_2(x-2m)=2$」となるが、このとき $x+2m, x-2m$ の差は 4 の倍数とならず、x, m, k を全て整数としてはとれない。よって、平方数とはなりえない。

5. $b^2-4c>0$、$ord_2(b^2-4c)\geq 4$ のとき

$k>b, c$ の条件を満たすかどうかには、x として最も大きいものをとった場合を考えてみればよい。$x+2m, x-2m$ の和は偶数、差は 4 の倍数でなければならないので、x が最も大きくとれるのは

$$x+2m=\frac{b^2-4c}{4}, x-2m=4$$

の場合である。このとき、

$$x=\frac{b^2-4c+16}{8}, m=\frac{b^2-4c-16}{16}, k=\frac{b^2-8b+16-4c}{16}$$

$ord_2(b^2-4c)\geq 4$、b:偶数より、x, m, k は整数となる。
このとき、$k>b, c$ となる条件を考える。

$$\frac{b^2-8b+16-4c}{16}>b, \frac{b^2-8b+16-4c}{16}>c$$

より、

$$\frac{b^2-24b+16}{4}>c, \frac{b^2-8b+16}{20}>c$$

この２つの左辺の大小、正負を考慮すれば定理の通りとなる。

6. $b^2-4c<0$ のとき

(a) $ord_2(b^2-4c)=0$ のとき
上と同様に、

$$x+2m=4c-b^2, x-2m=-1$$

のときを考えればよい。このとき、

$$x=\frac{-b^2+4c-1}{2}, m=\frac{-b^2+4c+1}{4}, k=\frac{-b^2-2b-1+4c}{4}$$

となる。しかし、

$$k = \frac{-b^2 - 2b - 1 + 4c}{4} = \frac{-(b+1)^2 + 4c}{4} < c$$

となるので、不適。よって、この場合平方数とはなりえない。

(b) $ord_2(b^2 - 4c) = 2$ のとき

上と同様に、

$$x + 2m = \frac{4c - b^2}{2}, x - 2m = -2$$

のときを考えればよい。このとき、

$$x = \frac{-b^2 + 4c - 4}{4}, m = \frac{-b^2 + 4c + 4}{4}, k = \frac{-b^2 - 4b - 4 + 4c}{8}$$

となる。しかし、

$$k = \frac{-b^2 - 4b - 4 + 4c}{8} = \frac{-(b+2)^2 + 4c}{8} < c$$

となるので、不適。よって、この場合平方数とはなりえない。

(c) $ord_2(b^2 - 4c) = 3$ のとき

$b^2 - 4c > 0$ のときと同じ理由で平方数とはなりえない。。

(d) $ord_2(b^2 - 4c) \geq 4$ のとき

上と同様に、

$$x + 2m = \frac{4c - b^2}{4}, x - 2m = -4$$

のときを考えればよい。このとき、

$$x = \frac{-b^2 + 4c - 16}{8}, m = \frac{-b^2 + 4c + 16}{16}, k = \frac{-b^2 - 8b - 16 + 4c}{16}$$

となる。しかし、

$$k = \frac{-b^2 - 8b - 16 + 4c}{16} = \frac{-(b+4)^2 + 4c}{16} < c$$

となるので、不適。よって、この場合平方数とはなりえない。

証明終

5.3 a_0 が平方数の場合

$a.b.c^2{}_{(k)}$ について考える。この場合は a が平方因数を有さない場合については解決した。

定理 5.16 $a.b.c^2{}_{(k)}$ は a が平方因数を持たないとき、ある k が存在して平方数となる。

証明

$ak^2+bk+c^2=y^2$ とすれば、

$$k=\frac{-b+\sqrt{b^2-4ac^2+4ay^2}}{2a}$$

$\sqrt{b^2-4ac^2+4ay^2}$ が整数でなければならないので、$b^2-4ac^2+4ay^2=x^2$ とおく。$y'=2y$ として、これを変形すれば、

$$x^2-ay'^2=b^2-4ac^2$$

この方程式に $x\equiv b \pmod{2a}$、y':偶数を満たし、x が $k>a,b,c^2$ を満たすほど十分大きな解があることを示す。
$(x,y')=(b,2c)$ とすれば、明らかにこれは解になっている。

$$x+y'\sqrt{a}=(b+2c\sqrt{a})(d+e\sqrt{a})^l$$

(c,d は $d^2-ae^2=1$ を満たす自然数、l は非負整数) を満たす x,y' は方程式 $x^2-ay'^2=b^2-4ac^2$ の解となる。
$s+t\sqrt{a}=(d+e\sqrt{a})^l(s,t\in\mathbb{N})$ とすれば、$s\equiv d^l \pmod{a}$。
$d^2-ae^2=1$ より、d,a は互いに素。これより、$d^{\varphi(a)}\equiv 1 \pmod{a}$。[1]

1. a:奇数のとき
   「d : 偶数、e : 奇数」または「d : 奇数、e : 偶数」となっている。
   前者の場合、$s+t\sqrt{a}=(d+e\sqrt{a})^{2i}(i\in\mathbb{N})$ とすれば、s:奇数、t:偶数。
   後者の場合、これは何乗しても s:奇数、t:偶数となる。

   よって、$s+t\sqrt{a}=(d+e\sqrt{a})^{2\varphi(a)}$ とすれば、$s\equiv 1 \pmod{2a}$、t:偶数。
   このとき、

   $$x+y'\sqrt{a}=(b+2c\sqrt{a})(d+e\sqrt{a})^{2\varphi(a)i}(i\in\mathbb{N})$$

   とすれば、$x\equiv b \pmod{2a}$、y':偶数を満たし、i を十分大きくとることで、x が $k>a,b,c^2$ を満たすほど十分大きな解となり、示された。
2. a:偶数のとき

   $$a=2a'$$

[1] $\varphi(a)$ で a 以下で a と互いに素な整数の個数を表し、これは Euler 関数と呼ばれるものである。n,x が互いに素のとき、$x^{\varphi(n)}\equiv 1 \pmod{n}$ が成り立つ。

とする。「d:奇数、e:偶数」または「d:奇数、e:奇数」となっている。
前者の場合、$s+t\sqrt{a}=(d+e\sqrt{a})^{2i}(i\in\mathbb{N})$ とすれば、$s\equiv 1 \pmod 4$、t:偶数。
後者の場合、$s+t\sqrt{a}=(d+e\sqrt{a})^{4i}(i\in\mathbb{N})$ とすれば、$s\equiv 1 \pmod 4$、t:4 の倍数。
これは $d\equiv 1,3 \pmod 4$、$e\equiv 1,3 \pmod 4$ の 4 通りについて確かめれば容易に確認できる。

よって、$s+t\sqrt{a}=(d+e\sqrt{a})^{4\varphi(a)}$ とすれば、$s\equiv 1 \pmod{4a'}$、t:偶数。
このとき、

$$x+y'\sqrt{a}=(b+2c\sqrt{a})(d+e\sqrt{a})^{4\varphi(a)i}(i\in\mathbb{N})$$

とすれば、$x\equiv b \pmod{2a}$、y':偶数を満たし、i を十分大きくとることで、x が $k>a,b,c^2$ を満たすほど十分大きな解となり、示された。

証明終

5.4 いくつかの特殊な場合

定理 5.17 $p\equiv 3 \pmod 8$:有理素数、$K(\sqrt{p})$ の類数は 1、b:偶数、b^2-4pc は第二種の素数を偶数冪含むとき、$\exists k$、$p.b.c_{(k)}$ は平方数。

まずは、次の補題を示す。

補題 5.18 p:有理素数とする。$K(\sqrt{p})$(:類数 1 の二次体) の基本単数 $\epsilon_0=d+e\sqrt{p}$ を考える。このとき、

$$d\equiv\begin{cases}-1 & (p\equiv 3 \pmod 8)\\ 1 & (p\equiv 7 \pmod 8)\end{cases} \pmod p$$

補題の証明
まずは、$N(\epsilon_0)=1$ であることを示す。
これは $p\equiv 3 \pmod 4$ より、$d^2-pe^2\not\equiv 3 \pmod 4$ なので、明らか。
$p\equiv 3 \pmod 8$ のときのみ、$(Ap-1)^2-pe^2=1$ なる A,d,e が存在することを示せばよい。
この式を変形して、

$$A^2p-2A-e^2=0$$

$$(Ap-2)A=e^2$$

1. A が奇数の時

   奇数 s,t を用いて、$A, Ap-2$ は互いに素だから、$A=s^2, Ap-2=t^2$ と表すことができる。これより、

$$t^2 - ps^2 = -2$$

   定理 5.14 より、$t^2 - ps^2 = \pm 2$ のいずれかのみを解に持つが、 $(\mathrm{mod}\ 8)$ でみれば、$p \equiv 3\ (\mathrm{mod}\ 8)$ では、-2 のときに解を有し、$p \equiv 7\ (\mathrm{mod}\ 8)$ では、2 のときに解を有することが分かる。よって、この場合は示された。
2. A が偶数の時

   $A, Ap-2$ の最大公約数は 2 となる。

   (a) $ord_2 A = 1$ のとき

   奇数 s,t を用いて、$A = 2s^2, Ap-2 = 2^{2f+1}t^2$ と表せる。

$$2ps^2 - 2 = 2^{2f+1}t^2$$

$$4^f t^2 - ps^2 = -1$$

   となるが、両辺を $(\mathrm{mod}\ 4)$ でみれば、これは有り得ない。

   (b) $ord_2(Ap-2) = 1$ のとき

   奇数 s,t を用いて、$Ap-2 = 2s^2, A = 2^{2f+1}t^2$ と表せる。

$$2^{2f+1}t^2 p - 2 = 2s^2$$

$$4^f t^2 - s^2 = 1$$

   となるが、両辺を $(\mathrm{mod}\ 4)$ でみれば、これはありえない。

証明終

ちなみに、これは類数 1 という条件を除いても、成り立つ。

定理の証明

$$pk^2 + bk + c = y^2$$

となるとき、

$$k = \frac{-b + \sqrt{b^2 - 4pc + 4py^2}}{2p}$$

$b^2 - 4pc + 4py^2 = x^2$ とおく。$x \equiv b \pmod{2p}$ でなければならない。
$y' = 2y$ とおく。y' は偶数でなければならないことに注意しておく。

$$x^2 - py'^2 = b^2 - 4pc$$

定理 5.14 より、$x^2 - py'^2 = \pm(b^2 - 4pc)$ のいずれかのみが解を持つが、平方剰余の第一補充則より、

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

となるので、$x^2 - py'^2 = b^2 - 4pc$ は解を持つ。
さて、このとき、b:偶数であることも考慮に入れれば、$x \equiv \pm b \pmod{2p}$ である。

$$x + y'\sqrt{p} = (f + g\sqrt{p})\epsilon_0^l$$

(f, g は $f^2 - pg^2 = b^2 - 4pc$ を満たす自然数、ϵ_0は基本単数) とすれば、この x, y' は解となっている。
$\epsilon_0 = d + e\sqrt{p}$ とすれば、$d \equiv -1 \pmod{p}$ なので、$f \equiv -b \pmod{p}$ であれば、基本単数の奇数乗を乗じればよく、$f \equiv b \pmod{p}$ であれば、基本単数の偶数乗を乗じればよい。また、両辺を $\pmod 4$ で見れば、x は常に偶数であるので、こうすれば、$x \equiv b \pmod{2p}$ とできる。また基本単数を十分回乗じれば、x は $k > p, b, c$ を満たせるほど大きくできる。よって、示された。

証明終

定理 5.19 $p \equiv 1 \pmod 4$:有理素数、$K(\sqrt{p})$ の類数は 1、b:奇数、$b^2 - 4pc$ は第二種の素数を偶数冪含むとき、$\exists k$、$p.b.c_{(k)}$ は平方数。

補題 5.20 $p \equiv 1 \pmod 4$:有理素数、$x^2 - py^2 = 1$ の最小正数解は $x \equiv -1 \pmod p$ を満たす。

この補題は、$p \equiv 1 \pmod 4$ のとき、$K(\sqrt{p})$ における基本単数のノルムが -1 であることがイデアルを使った議論により示され、これを使えば示される。
また、この定理はこの補題を使えば先の定理と同様にして示すことが出来る。

5.5 $a_2 = 2$ の場合

定理 5.21 $b^2 - 8c$ が第二種の素数つまり $q \equiv 3, 5 \pmod 8$ なる素数を偶数冪含めば、$\exists k$、$2.b.c_{(k)}$ は平方数。

証明

これまでと同様に

$$x^2 - 2y^2 = b^2 - 8c$$

が $x \equiv b \pmod 4$、y:偶数なる解を持つことに帰着できる。
両辺を $\pmod 4$ で見れば、明らかに y:偶数。

基本単数のノルムが -1 であることより、このとき解はある。それを s, t とおく。$x^2 - 2y^2 = 1$ の最小正数解は $(x, y) = (3, 2)$ であることより、

$$x + y\sqrt{2} = (s + t\sqrt{2})(3 + 2\sqrt{2})^l$$

により、方程式の解が表される。
$b \equiv 0, 2 \pmod 4$ の場合は、もとの方程式の両辺を $\pmod 8$ で比較することにより、示される。
$b \equiv 1, 3 \pmod 4$ の場合は、$(3 + 2\sqrt{2})$ を s が $1, 3$ のどちらと合同であるかによって、奇数回か偶数回かは変わるが、必要な回数かければよい。
十分回 $(3 + 2\sqrt{2})$ を乗じれば、$k > 2, b, c$ とできる。
よって、示された。

証明終

6 例

ここまでいくつか判定する方法を述べてきたので、それを実際に使って判定してみようと思います。

例 6.1 14.12 は平方数とはなりえない。
これは定理 4.2 による。

例 6.2 1.7.4 は平方数とはなりえない。
これは定理 5.15 による。

例 6.3 1.7.1 は平方数となりうる。
これは定理 5.15 による。実際、8 進数だとして読めば、$121 = 11^2$ である。

例 6.4 3.8.3 は平方数となりえない。
これは定理 5.17 による。

例 6.5 2.7.14 は平方数となりうる。
これは定理 5.21 による。実際、67 進数だとして読めば、$4761 = 69^2$ である。

7　あとがき

結局、かなり特殊ないくつかの場合だけ述べるにとどまってしまい、少し残念です。しかも、4 桁以上となると意味不明ですし。自分としては最後の部誌だったので、少々消化不良って感じです。

3 桁の場合の話になりますが、

$$x^2 - ay^2 = n$$

が解を有するかどうかの判定自体がかなり各個撃破的な判定しかできず、しかもその最小正数解の剰余まで求めるというのはなかなか厳しい問題であったかのようには思います。a が合成数だと、基本単数自体の剰余（みたいなの）が分からないとかいう問題にも直面しました。なんか他にいいアイデアを思いつかれたら、是非是非教えていただきたいです。

この記事では、平方剰余や二次体に関していくつか証明抜きで事実だけを羅列するにとどまってしまいましたが、どちらも整数論において非常に大きな意味を持ち、かつ綺麗な理論が展開されてると思う（あくまで主観ですが。）ので興味を持った方はそれに関しても詳しく見ていただければいいかなと思います。下にあげる「初等整数論講義」は名著だと思います。

最後になりましたが、この場を借りて編集の平野君に感謝の意を表しておきたいと思います。
また、最後まで読んでくださった皆様、ありがとうございました。
質問・感想があれば、youky_snow@hotmail.com までお願いします。

8　参考文献

「初等整数論講義」高木貞治著　共立出版