$\mathbb{Q}$ における $\mathbb{N}$ の定義可能性に関する J. Robinson の定理について（後編）

近藤 友祐 （神戸大学大学院システム情報学研究科）

最終更新：2020 年 10 月 19 日

このノート[*1]では，「前編」で後回しにしていた 2 つの補題の証明を与える．証明は R. Fraïssé による [2] の Appendix *"Proof of lemmas needed to prove J. Robinson' theorem"* に沿っている（この本はなぜか数学科図書室にしか置いていない）．定理番号は同書に準拠している[*2]．行間を必要以上に埋めた（つもりな）ので，ページ数が膨れ上がってしまった[*3]．

証明では p-進数を用いることで 2 次形式の一般論に乗せやすくし，議論を見通しよくしている[*4]．また p-進数の定義には p-進完備化や射影極限などのムズカシイ概念を持ち出さず，単にある条件を満たす数列（つまり実質的に p-進展開表示のこと）という形でドライに定義している．これは p-進数を全く知らない読者への配慮であると思われるが，そのせいで準備のために全体の 3 分の 1 程度のページを割いている．p-進数に明るい人（あるいはそうでない人も）にとっては命題 1 から命題 6 までは退屈なだけなので，記法やステートメントだけ確認して証明はすべてスキップしてよい．

記法の約束． 混乱のない場合，$\mathbb{Z}$ の部分集合 $\{i \in \mathbb{Z} : a < i < b\}$ を (a, b) と表すことにする．$\{i \in \mathbb{Z} : a \leqslant i < b\}$ は $[a, b)$ と書く．その他の約束は「前編」に準ずる．

さて，次の 2 つの定理が最終目標である：

定理 12 (Lemma 3 in [3])**.** p を $p \equiv 3 \pmod 4$ なる素数，t を有理数とし，$t = u/v$ と既約分数として表示する $(u, v \in \mathbb{Z},\ v \neq 0)$．このとき以下は同値である：

(A) $(\exists x, y, z \in \mathbb{Q})[pt^2 + 2 = x^2 + y^2 - pz^2]$;
(B) $2 \nmid v \quad \& \quad p \nmid v$.

[*1] **TODO** としたところは適宜加筆していく．
[*2] [2] では「定理」「補題」などのラベルを与えていない．主観でラベルを与えた．
[*3] もっとも，[2] でも 7 ページかけて証明しているので，こんなもんかもしれない．
[*4] その代わり，2 次形式に関するいくつかの事実を証明抜きで認めることとなる．一方，D. Flath and S. Wagon による [1] では一般論に乗せることをせず個別的に議論している．また [1] では体 $\mathbb{Q}_l$ でなく環 $\mathbb{Z}/l^n\mathbb{Z}$ を舞台に議論がなされる．

定理 13 (Lemma 4 in [3])**.** p を $p \equiv 1 \pmod 4$ なる素数，$q \neq p$ を奇素数であって $(q/p) = -1$ を満たすものとする．t を有理数とし，$t = u/v$ と既約分数として表示する $(u, v \in \mathbb{Z},\ v \neq 0)$．このとき以下は同値である：

(A) $(\exists x, y, z \in \mathbb{Q})[pqt^2 + 2 = x^2 + qy^2 - pz^2]$;
(B) $p \nmid v \quad \& \quad q \nmid v$.

まずは p-進数の準備に取りかかろう．命題 1 と命題 2 は，p-進数が平方根をもつ必要十分条件を与える命題 5 と命題 6 の証明に用いられる．見てわかる通り，$p = 2$ の場合と p が奇素数の場合で，似通ってはいるものの少し毛色の違う議論を繰り返さなければならない．大抵の場合，$p = 2$ のケースのほうが難しい．

命題 1. $n \in \mathbb{N},\ n \geqslant 3$ とする．このとき，任意の正の奇数 $c \in \mathbb{N}$ に対し次が成り立つ：

$$\left(\frac{c}{2^n}\right) = 1 \quad \Longleftrightarrow \quad c \equiv 1 \pmod 8. \tag{1}$$

証明. $n \geqslant 3$ を勝手な自然数とする．2 つの集合 $A_n, B_n \subseteq \mathbb{N}$ を

$$A_n := \{c \in [0, 2^n) : c \text{ odd } \&\ c \,\%\, 8 = 1\}, \tag{2}$$
$$B_n := \{c \in [0, 2^n) : c \text{ odd } \&\ (c/2^n) = 1\} \tag{3}$$

で定める．$A_n = B_n$ を示せばよい[*5]．

$\boxed{B_n \subseteq A_n}$ $c \in B_n$ とする．ある $x \in \mathbb{Z}$ が存在して $x^2 \equiv c \pmod{2^n}$ となっている．$n \geqslant 3$ なので $x^2 \equiv c \pmod 8$ でもある．c は奇数なので x は奇数である．よって $x = 2a + 1$ $(a \in \mathbb{Z})$ と書ける．すると $x^2 = 4a(a+1) + 1$ である．$a(a+1)$ は連続した 2 つの整数の積なので偶数である．したがって $4a(a+1)$ は 8 の倍数だから $c \equiv x^2 \equiv 1 \pmod 8$ である．よって $c \in A_n$ である．

$\boxed{A_n \subseteq B_n}$ 最初にひとつクレイムを準備する．

> **クレイム 1.** $|A_n| = 2^{n-3}$ である．
>
> $\vdash$ $n \geqslant 3$ に関する帰納法．$n = 3$ のときは $|A_3| = |\{1\}| = 1 = 2^{3-3}$ なので明らか．n で成立すると仮定する．$T := \{a \in [2^n, 2^{n+1}) : a \,\%\, 8 = 1\}$ とおくと $A_{n+1} = A_n \sqcup T$（非交和）であり，$T = \{a \in [2^n, 2^{n+1}) : a \,\%\, 8 = 1\} = \{b + 2^n \in [2^n, 2^{n+1}) : (b + 2^n) \,\%\, 8 = 1\} = \{b \in [0, 2^n) : b \,\%\, 8 = 1\}$ となるから $|T| = |A_n| = 2^{n-3}$ である．したがって $|A_n| = 2^{n-3} + 2^{n-3} = 2^{(n+1)-3}$ である． $\dashv$

[*5] $A_n = B_n$ が示せたとする．$(\Rightarrow)$: $(c/2^n) = 1$ とする．c は明らかに奇数．$d := c \,\%\, 2^n$ とする．d は明らかに奇数．$(d/2^n) = (c \,\%\, 2^n/2^n) = (c/2^n) = 1$. よって $d \in B_n$. よって $d \in A_n$. よって $d \equiv 1 \pmod 8$. $n \geqslant 3$ なので $c \,\%\, 8 = (c \,\%\, 2^n) \,\%\, 8 = d \,\%\, 8 = 1$. $(\Leftarrow)$: $c \equiv 1 \pmod 8$ とする．c は明らかに奇数．$d := c \,\%\, 2^n$ と置く．d は明らかに奇数．$n \geqslant 3$ なので $d \,\%\, 8 = (c \,\%\, 2^n) \,\%\, 8 = c \,\%\, 8 = 1$. よって $d \in A_n$. よって $d \in B_n$. よって $(c/2^n) = (c \,\%\, 2^n/2^n) = (d/2^n) = 1$.

$A_n \subseteq B_n$ を示す．すでに示したように $B_n \subseteq A_n$ であり，またクレイム 1 より $|A_n| = 2^{n-3}$ であるから $|B_n| \leqslant |A_n| = 2^{n-3}$ である．よって，$|B_n| \geqslant 2^{n-3}$ を示せば（$|A_n| \leqslant |B_n| \leqslant |A_n|$ となるから $|A_n| = |B_n|$ となり，したがって $A = B$ となるから）十分である．

> **クレイム 2.** $a, b \in [0, 2^{n-3})$ かつ $a \neq b$ ならば $(2a+1)^2 \not\equiv (2b+1)^2 \pmod{2^n}$ である．よって，写像 $f\colon [0, 2^{n-3}) \ni a \mapsto (2a+1)^2 \mathbin{\%} 2^n \in [0, 2^n)$ は単射である．
>
> $\vdash$ 〔以下，合同記号はすべて $\pmod{2^n}$ とする．〕一般性を失わず $a < b$ としてよい．$(2a+1)^2 \equiv (2b+1)^2$ を仮定して矛盾を導く．$4a^2+4a+1 \equiv 4b^2+4b+1$ より $4(b^2-a^2)+4(b-a) \equiv 0$，したがって $2^2(b+a+1)(b-a) \equiv 0$ である．いま $b+a+1$ と $b-a$ のどちらか一方，そして一方のみが偶数である．場合分け．$\underline{b+a+1 \text{ が偶数の場合}}$ $b+a+1$ は 2^{n-2} で割り切れなければならない．ところが a と b の選び方より $0 < b < 2^{n-3}$ かつ $0 \leqslant a < 2^{n-3}-1$ であるから $0 < b+a+1 < 2^{n-2}$ を得る．よって $b+a+1$ は 2^{n-2} で割り切ることができず矛盾．$\underline{b-a \text{ が偶数の場合}}$ $b-a$ は 2^{n-2} で割り切れなければならない．ところが $b < 2^{n-2}$ と $-a \leqslant 0$ より $b-a < 2^{n-2}$ で，$a < b$ より $0 < b-a$ なので $0 < b-a < 2^{n-2}$ となる．よって $b-a$ は 2^{n-2} で割り切ることができず矛盾．$\dashv$

以上より，

$$
\begin{aligned}
|B_n| &= |\{d^2 \mathbin{\%} 2^n : d \in [0, 2^n) \ \&\ d \text{ odd}\}| && (4)\\
&= |\{(2a+1)^2 \mathbin{\%} 2^n : a \in [0, 2^{n-1})\}| && (5)\\
&\geqslant |\{(2a+1)^2 \mathbin{\%} 2^n : a \in [0, 2^{n-3})\}| && (6)\\
&= |\mathrm{ran}(f)| && (7)\\
&= 2^{n-3}. && (8)
\end{aligned}
$$

となり[*6]，所望の $|B_n| \geqslant 2^{n-3}$ を得る． □

命題 2. p を奇素数とし，n を 1 以上の自然数とする．このとき，$p \nmid a$ であるような任意の $a \in \mathbb{Z}$ に対して次が成り立つ：

$$
\left(\frac{a}{p}\right) = 1 \quad \Longleftrightarrow \quad \left(\frac{a}{p^n}\right) = 1. \tag{9}
$$

証明. $n \geqslant 1$ を勝手な自然数とする．$n = 1$ については自明なので $n \geqslant 2$ とする．集合 $A_n, B_n \subseteq \mathbb{N}$ を

$$
\begin{aligned}
A_n &:= \{a \in [0, p^n) : p \nmid a \ \&\ (a/p) = 1\}, && (10)\\
B_n &:= \{a \in [0, p^n) : p \nmid a \ \&\ (a/p^n) = 1\} && (11)
\end{aligned}
$$

[*6] 最初の等号について．$c \in B_n$ とする．ある $d \in [0, 2^n)$ が存在して $c \equiv d^2 \pmod{2^n}$．d は明らかに奇数．$c \in [0, 2^n)$ なので $c = d^2 \mathbin{\%} 2^n$．逆にある奇数 $d \in [0, 2^n)$ が存在して $c = d^2 \pmod{2^n}$ とする．$(c/2^n) = 1$．また $c \in [0, 2^n)$．よって $c \in B_n$．2 つめの等号について．$[0, 2^n)$ の中の奇数を $2a+1$ $(a \in \mathbb{Z})$ と表すと $0 \leqslant 2a+1 < 2^n$ なので $a \leqslant 0$．$2a < 2^n - 1$ より $2^a \leqslant 2^n - 2$ ゆえ $a \leqslant 2^{n-1} - 1$．ゆえに $a \in [0, 2^{n-1})$ に限られる．逆に $a \in [0, 2^{n-1})$ なら $2a+1 \in [0, 2^n)$．

で定める．$A_n = B_n$ を示せばよい[*7]．

$\boxed{B_n \subseteq A_n}$ $a \in B_n$ とする．$(\exists x \in [0, p^n))[x^2 \equiv a \pmod{p^n}]$ ゆえ，同じ x を証拠に $(\exists x \in [0, p^n))[x^2 \equiv a \pmod{p}]$ なので $(a/p) = 1$ よって $a \in A_n$ である．

$\boxed{A_n \subseteq B_n}$

> **クレイム 1.** $|A_n| = p^{n-1}(p-1)/2$ である（この数を P_n と書くことにする）．
>
> $\vdash$ 各 $k \in \mathbb{Z}$ について，$p \nmid a$ かつ $(a/p) = 1$ であるような $a \in [kp + 0, kp + p)$ はちょうど $(p-1)/2$ 個存在する (cf. [6], 命題 1.11.2) ので，そのような区間を p^{n-1} 個つなぎ合わせた区間 $[0, p^n)$ には $p \nmid a$ かつ $(a/p) = 1$ であるような $a \in [0, p)$ は $p^{n-1}(p-1)/2$ 個存在する．したがって $|A_n| = P_n$ である． $\dashv$

$A_n \subseteq B_n$ を示す．すでに示したように $B_n \subseteq A_n$ であり，またクレイム 1 より $|A_n| = P_n$ であるから $|B_n| \leqslant |A_n| = P_n$ である．よって，$|B_n| \geqslant P_n$ を示せば（$|A_n| \leqslant |B_n| \leqslant |A_n|$ となるから $|A_n| = |B_n|$ となり，したがって $A = B$ となるから）十分である．

$C_n \subseteq \mathbb{N}$ を $C_n := \{a \in \mathbb{Z} : 0 < a < p^n/2 \ \&\ p \nmid a\}$ で定める．

> **クレイム 2.** $|C_n| = P_n$ である．
>
> $\vdash$ $n \geqslant 1$ に関する帰納法．$n = 1$ については，$0 < a < p/2$ を満たす整数 a は $1, 2, \ldots, (p-1)/2$ $(= P_1)$ のちょうど P_1 個であり，これらはすべて p の倍数でないのでよい（命題の仮定より p は奇素数であることに注意）．n で成立すると仮定する．p 個の集合 $S_k \subseteq \mathbb{N}$ $(k \in [0, p))$ を
>
> $$S_k := \{a \in \mathbb{N} : kp^n/2 < a < (k+1)p^n/2 \ \&\ p \nmid a\} \tag{12}$$
>
> で定める．このとき $|S_0| = |S_1| = P_n$ である〔“$p^n/2$ を中心に折り返す” 写像 $f\colon S_0 \to S_1$ を $f(a) := p^n - a$ で定める．$a \in S_0$ なら $p \nmid a$ より $p \nmid (p^n - a)$ である．また $-p^n/2 < -a < 0$ より $p^n/2 < p^n - a < p^n$ である．よって f は確かに S_0 から S_1 への写像である．同様に $g\colon S_1 \to S_0$ を $g(b) := p^n - b$ で定める．すると任意の $a \in S$ について $g(f(a)) = p^n - f(a) = p^n - (p^n - a) = a$ であり，同様に任意の $b \in S_1$ について $f(g(b)) = b$ である．よって f は全単射なので $|S_0| = |S_1|$ である〕．帰納法の仮定より $|S_1| = P_n$ である．同様に “$kp^n/2$ を中心に折り返す” 写像で S_k と S_{k+1} を対応させていけば結局 $(\forall k \in [0, p))[|S_k| = P_n]$ がわかる．したがって $|C_n| = \left|\bigcup_{k \in [0,p)} S_k\right| = p \cdot P_n = P_{n+1}$ である（一つ目の等号について，“つなぎ目” の $kp^n/2$ については，k が偶数なら p の倍数，k が奇数なら非整数となるので $\notin C_n$ であることに注意）． $\dashv$

[*7] $A_n = B_n$ が示せたとする．$(\Rightarrow)$: $(a/p) = 1$ とする．$b := a \,\%\, p^n$ とおく．$(b/p) = (a \,\%\, p^n/p) = 1$ である（ここに，2 番目の等号は次のようにしてわかる：いま $x \in \mathbb{Z}$ で $x^2 \equiv a \pmod{p}$ なるものがある．$(a \,\%\, p^n) \,\%\, p = a \,\%\, p = x^2 \,\%\, p$．よって $a \,\%\, p^n \equiv x^2 \pmod{p}$)．よって $b \in A_n$．よって $b \in B_n$．よって $(a/p^n) = (a \,\%\, p^n/p^n) = (b/p^n) = 1$．$(\Leftarrow)$: $(a/p^n) = 1$ とする．$b := a \,\%\, p^n$ とおく．$(b/p^n) = (a \,\%\, p^n/p^n) = (a/p^n) = 1$．よって $b \in B_n$．よって $b \in A_n$．よって $(b/p) = 1$．よって $(a/p) = (a \,\%\, p^n/p) = (b/p) = 1$（先と同様）．

クレイム 3. $a, b \in C_n$ かつ $a \neq b$ ならば $a^2 \not\equiv b^2 \pmod{p^n}$ である．よって，写像 $h\colon C_n \ni a \mapsto a^2 \mathbin{\%} p^n \in [0, p^n)$ は単射である．

$\vdash$ 一般性を失わず $a < b$ としてよい．$a^2 \equiv b^2 \pmod{p^n}$ を仮定して矛盾を導く．$(b+a)(b-a) \pmod{p^n}$ である．$b+a$ と $b-a$ が同時に p の倍数になることはあり得ない〔仮に $b-a = kp$, $b+a = lp$ $(k, l \in \mathbb{Z})$ と書けたら $2b = (k+l)p$ となる．よって $p \mid 2b$ で，p は奇素数だったので $p \mid b$ である．これは $b \in C_n$ に矛盾〕．したがって $p^n \mid (b+a)$ か $p^n \mid (b-a)$ のどちらか一方，そして一方のみが成り立つ．ところが $0 < b < p^n/2$ と $0 < a < p^n/2$ とから $0 < b+a < p^n$ なので前者は起こりえない．同様に $b < p^n/2$ と $-a < 0$ とから $0 < b-a < p^n$ なので後者も起こりえない． $\dashv$

以上より，

$$
\begin{aligned}
|B_n| &= |\{b^2 \mathbin{\%} p^n : b \in [0, p^n) \ \&\ p \nmid b\}| && (13)\\
&\geqslant |\{b^2 \mathbin{\%} p^n : b \in [0, p^n/2) \ \&\ p \nmid b\}| && (14)\\
&= |\mathrm{ran}(h)| && (15)\\
&= |C_n| && (16)\\
&= P_n. && (17)
\end{aligned}
$$

となり，所望の $|B_n| \geqslant P_n$ を得る[*8]．最後の等号はクレイム 3 による． $\square$

[*8] 最初の等号について．$a \in B_n$ とする．ある $b \in [0, p^n)$ で $b^2 \equiv a \not\equiv 0 \pmod{p^n}$ を満たすものがある．$a \in [0, p^n)$ に注意すれば，$b^2 \mathbin{\%} p^n = a \mathbin{\%} p^n = a$．また $p \nmid b^2$ より $p \nmid b$．逆に，ある $b \in [0, p^n)$，$p \nmid b$ が存在して $a = b^2 \mathbin{\%} p^n$ だとする．自明に $a \in [0, p^n)$ かつ $(a/p^n) = 1$．$p \nmid b$ より $p \nmid b^2$．よって $p \nmid a$．よって $a \in B_n$．

定義と事実 3. p を素数とする．

(1) 自然数列 $a=(a_n)_{n\in\mathbb{N},n\geqslant 1}$ が ***p*-進整数**である :$\Longleftrightarrow$

$$(\forall n\geqslant 1)[0\leqslant a_n<p^n \ \&\ a_{n+1}\equiv a_n \pmod{p^n}]. \tag{18}$$

a_n を a の**第 *n* 成分**という．

(2) p-進整数全体の集合を $\mathbb{Z}_p$ と書く．2 つの p-進整数 $a=(a_n)_n$, $b=(b_n)_n$ に対して

$$a+b:=((a_n+b_n)\ \%\ p^n)_n, \tag{19}$$
$$ab:=((a_nb_n)\ \%\ p^n)_n \tag{20}$$

によって加法と乗法を入れることで $\mathbb{Z}_p$ は整域をなす．これを ***p*-進整数環**と呼ぶ．加法単位元 $0_{\mathbb{Z}_p}$ は $(0)_n$，乗法単位元 $1_{\mathbb{Z}_p}$ は $(1)_n$ に等しい．

(3) 任意の $a\in\mathbb{Z}_p$ について，a が単元であること（i.e. $\mathbb{Z}_p$ に乗法逆元をもつこと）と $a_1\neq 0$ であることは同値である．$\mathbb{Z}_p$ の単元がなす乗法群を $\mathbb{Z}_p^\times$ と書く．

(4) $\mathbb{Z}_p$ は整域なので商体が作れる．$\mathbb{Z}_p$ の商体を ***p*-進数体**といい $\mathbb{Q}_p$ と書く．

(5) $(\forall a\in\mathbb{Q}_p\setminus\{0\})(\exists! h\in\mathbb{Z})(\exists! x\in\mathbb{Z}_p^\times)[a=p^hx]$ が成り立つ．これを a の ***p*-進展開**という．

各整数 $k\in\mathbb{Z}$ に対し，k を p-進整数 $\hat{k}:=(k\ \%\ p^n)_n\in\mathbb{Z}_p$ と同一視する．これにより $\mathbb{Z}$ は $\mathbb{Z}_p$ に埋め込める．$\hat{k}$ を k と書いてしまうこともある．各有理数 $s=m/d$ $(m,d\in\mathbb{Z},\ d\neq 0)$ に対し，s を p-進数 $\tilde{s}:=[(\hat{m},\hat{d})]$ と同一視する[*9]．これにより $\mathbb{Q}$ は $\mathbb{Q}_p$ に埋め込める．$\tilde{s}$ を s と書いてしまうこともある．なお，$\hat{k}$ や $\tilde{s}$ は私が勝手に導入した記法であり，標準的なものではない．

TODO: 埋め込みの図式を書く．可換性を調べる．

命題 4. p を素数，$s\in\mathbb{Q}$ とし，$s=u/v$ を既約分数として表示する $(u\in\mathbb{Z},v\in\mathbb{Z}\setminus\{0\})$．このとき次が成り立つ：

$$s\in\mathbb{Z}_p^\times \quad\Longleftrightarrow\quad p\nmid u\ \&\ p\nmid v. \tag{21}$$

示すべき命題の左辺の $s\in\mathbb{Z}_p^\times$ というのは，正確に言えば次のとおりである：自然な埋め込み $j\colon\mathbb{Z}_p^\times\ni a\mapsto[(a,1_{\mathbb{Z}_p})]\in\mathbb{Q}_p$ について，$\tilde{s}\in\mathrm{ran}(j)$ である．

証明. $\boxed{\Longrightarrow}$ $\tilde{s}\in\mathbb{Z}_p^\times$ であると仮定する．まず，$\tilde{s}=[(\hat{u},\hat{v})]$ が p-進整数（と同一視されるような $\mathbb{Q}_p$ の元）であることから，ある $t=(t_n)_n\in\mathbb{Z}_p$ が存在して $[(\hat{u},\hat{v})]\sim[(t,1_{\mathbb{Z}_p})]$，つまり $\hat{u}=\hat{v}t$，つまり

$$(u\ \%\ p^n)_n=(v\ \%\ p^n)_n(t_n)_n=((v\ \%\ p^n)t_n\ \%\ p^n)_n=(vt_n\ \%\ p^n)_n \tag{22}$$

が成り立つ．第 1 成分に注目することで $u\ \%\ p=vt_1\ \%\ p$，すなわち $u\equiv vt_1 \pmod{p}$ を得る．したがっ

[*9] ここに $[(a,b)]\in(\mathbb{Z}_p\times(\mathbb{Z}_p\setminus\{0_{\mathbb{Z}_p}\}))/\sim$ は (a,b) が属する同値類である．同値関係は $(a,b)\sim(c,d):\Longleftrightarrow ad=bc$ (in $\mathbb{Z}_p$) で定義される．

て[*10]$\gcd(v,p) \mid u$ である．仮に $p \mid v$ なら $\gcd(v,p) = p$ なので $p \mid u$ である．すると p は u, v の共通素因数となり u/v の既約性に反する．よって $p \nmid v$ である．さらに，仮定より $s = u/v$ が同一視されるところの $t \in \mathbb{Z}_p$ は単元なので $t_1 \neq 0$ である．p-進整数の定義より $0 \leqslant t_1 < p$ だから $p \nmid t_1$ である．いま $u \equiv vt_1 \pmod{p}$ が成り立っているのであった．$p \nmid v$, $p \nmid t_1$ なので $p \nmid u$ でなければならない．以上で $(\Rightarrow)$ が示せた．

$\boxed{\Longleftarrow}$ $p \nmid u$ かつ $p \nmid v$ であることを仮定する．$\tilde{s} = [(\hat{u}, \hat{v})] \in \mathbb{Q}_p$ が p-進整数（と同一視される元）であること，すなわちある $t = (t_n)_n \in \mathbb{Z}_p$ が存在して $\hat{u} = \hat{v}t$ であることをいえばよい．そのためには $(u \,\%\, p^n)_n = (v \,\%\, p^n)_n (t_n)_n = ((v \,\%\, p^n)t_n \,\%\, p^n)_n = (vt_n \,\%\, p^n)_n$，つまり $(\forall n \geqslant 1)[u \equiv vt_n \pmod{p^n}]$ を満たす $t_n \in \mathbb{Z}, 0 \leqslant t_n < p^n$ $(n \geqslant 1)$ が存在することをいえばよい．$n \geqslant 1$ とする．先の脚注により，$u \equiv vx \pmod{p^n}$ が解をもつための条件は $\gcd(v, p^n) \mid u$ である．いま $p \nmid v$ かつ $v \neq 0$ なので $\gcd(v, p^n) = 1$ である．よって $\gcd(v, p^n) \mid u$ が自明に成り立ち，$u \equiv vx \pmod{p^n}$ は解 $x \in \mathbb{Z}$ をもつ．$t_n := x \,\%\, p^n$ とすればよい．次に $\tilde{s}$ の可逆性をいう．そのためには $s = u/v$ が同一視されるところの $t \in \mathbb{Z}_p$ について $t_1 \neq 0$ であることをいえばよい．いま $u \equiv vt_1 \pmod{p}$ であった．仮定より $p \nmid u$ だったから $vt_1 \equiv 0 \pmod{p}$ とはなりえない．したがって $t_1 \neq 0$ である． □

なんとなく想像されるように，Robinson の定理の証明では平方数がカギを握る．$\mathbb{Q}_p$ の元が平方数である（i.e. $\mathbb{Q}_p$ の中に平方根をもつ）ための必要十分条件を，命題 5（$p = 2$ の場合）と命題 6（$p \neq 2$ の場合）で与える．おそらく多くの教科書に載っている有名な命題である[*11]．

命題 5. $t \in \mathbb{Q}_2 \setminus \{0\}$ とする．以下は同値である：

(1) $(\exists u \in \mathbb{Q}_2)[t = u^2]$ （これを “t is a square in $\mathbb{Q}_2$” などという）；
(2) $(\exists! h \in \mathbb{Z})(\exists! c \in \mathbb{Z}_2^\times)[t = 2^h c \ \&\ h \text{ even} \ \&\ (\forall n \geqslant 1)[c_n \equiv 1 \pmod{8}]]$.

証明. $t \in \mathbb{Q}_2 \setminus \{0\}$ を固定する．

$\boxed{(1) \implies (2)}$ $t = u^2$ なる $u \in \mathbb{Q}_2$ が存在したと仮定する．$u \neq 0$ であるから，$u = 2^k d$ となる $k \in \mathbb{Z}$ および $d \in \mathbb{Z}_2^\times$ が一意に存在する．$t = u^2 = 2^{2k} d^2$ である．$h := 2k$, $c := d^2$ が (2) の条件を満たすことをいえばよい．$k \in \mathbb{Z}$ が偶数であることは定め方からよい．また $c \in \mathbb{Z}_2$ が単元であることもよい（d の乗法逆元の 2 乗が証拠）．$(\forall n \geqslant 1)[c_n \equiv 1 \pmod{8}]$ を示していく．

> **クレイム 1.** (d_1, d_2, d_3) は $(1,1,1), (1,1,5), (1,3,3), (1,3,7)$ のいずれかに等しい．
>
> $\vdash$ d_1 が 1 に限られることは d が可逆ゆえ $d_1 \neq 0$ であり $0 \leqslant d_1 < 2^1$ であることから明らか．2-進整数の定義より，
>
> $$(*) \qquad d_2 \overset{2}{\equiv} d_1 \ \&\ 0 \leqslant d_2 < 4 \tag{23}$$
>
> $$(\dagger) \qquad d_3 \overset{4}{\equiv} d_2 \ \&\ 0 \leqslant d_3 < 8 \tag{24}$$

[*10] 一般に，$a, b, c \in \mathbb{Z}, a, b \neq 0$ に対し，$x \in \mathbb{Z}$ に関する方程式 $c \equiv ax \pmod{b}$ が解をもつことと $\gcd(a,b) \mid c$ であることは同値である (cf. [6], 定理 1.8.5 (1))．これを $(a,b,c) = (v,p,u)$ として用いよ．

[*11] 一般論である Hensel の補題から系として示されることが多いようだ．

が成立する．$(*)$ より $d_2 = 1$ または $d_2 = 3$ である．$d_2 = 1$ の場合，$(\dagger)$ より $d_3 \overset{4}{\equiv} 1 \ \&\ 0 \leqslant d_3 < 8$ であるから d_3 は 1 か 5 に限られる．$d_2 = 3$ の場合，$(\dagger)$ より $d_3 \overset{4}{\equiv} 3 \ \&\ 0 \leqslant d_3 < 8$ であるから d_3 は 3 か 7 に限られる．よってクレイムが成り立つ． ⊣

$c = d \cdot d = (d_n)_n \cdot (d_n)_n = (d_n \cdot d_n \ \%\ 2^n)_n = (d_n^2 \ \%\ 2^n)_n$ について，$(\forall n \geqslant 1)[c_n \equiv 1 \pmod 8]$ を示す．$n = 1, 2, 3$ についてはクレイム 1 よりよい．$n \geqslant 4$ の場合，c が 2-進数であることから $\cdots \overset{64}{\equiv} c_5 \overset{32}{\equiv} c_4 \overset{16}{\equiv} c_3 \overset{8}{\equiv} 1$ となっているから $\cdots \overset{8}{\equiv} c_5 \overset{8}{\equiv} c_4 \overset{8}{\equiv} c_3 \overset{8}{\equiv} 1$ となりよい．

$\boxed{(2) \implies (1)}$ t が (2) のような表現をもっているとし，そのような一意的な $h \in \mathbb{Z}$, $c \in \mathbb{Z}_2^\times$ をとる．c は可逆なので，先の議論と同様に (c_1, c_2, c_3) の候補は $(1,1,1)$, $(1,1,5)$, $(1,3,3)$, $(1,3,7)$ となるが，仮定より $c_n \overset{8}{\equiv} 1$ $(n = 1, 2, 3)$ なので $(c_1, c_2, c_3) = (1, 1, 1)$ でしかありえないことに留意せよ．

クレイム 2. $(\forall n \geqslant 1)(\exists x \in \mathbb{Z})[x^2 \equiv c_n \pmod{2^n}]$.

$\vdash$ $n = 1, 2, 3$ については $x = 1$ とすればよい．$n \geqslant 4$ とする．$c_n \equiv 1 \pmod 8$ であるから，命題 1 より $(c_n / 2^n) = 1$ である．よって $(\exists x \in \mathbb{Z})[x^2 \equiv c_n \pmod{2^n}]$ である． ⊣

クレイム 2 により，

$$(\forall n \geqslant 1)[x_n^2 \equiv c_n \pmod{2^n}] \tag{25}$$

を満たす $x_n \in \mathbb{Z}$ $(n \geqslant 1)$ たちがとれる．それらを固定する．c_n たちは奇数なので x_n たちも奇数であることに注意する．この x_n たちをもとに，自然数 $n \geqslant 1$ に関する命題

$$\Psi(n)\colon\ (\exists a \in [0, 2^{n+1}))(\exists b \in [0, 2^{n+2}))\left[d_n \overset{2^n}{\equiv} a \overset{2^{n+1}}{\equiv} b \ \ \&\ \ a^2 \overset{2^{n+1}}{\equiv} c_{n+1} \ \ \&\ \ b^2 \overset{2^{n+1}}{\equiv} c_{n+2}\right] \tag{26}$$

がすべての n にわたって満たされるような列 $d_n \in \mathbb{Z}$ $(n \geqslant 1)$ を帰納的に構成する．

$d_1 := 1$ とせよ．$a = 1$, $b = 5$ を証拠に $\Psi(1)$ が成立する[*12]．

$n \geqslant 1$ とする．d_n が構成され，$\Psi(n)$ が確かめられたと仮定する．その上で，$\Psi(n+1)$ を満たすように d_{n+1} を構成する．いま，$\Psi(n)$ が成り立っているので，その証拠となる $a \in [0, 2^{n+1})$, $b \in [0, 2^{n+2})$ を固定する．$d_{n+1} := a$ とせよ．$\Psi(n+1)$ を確かめる．そのためには，ある $v \in [0, 2^{n+2})$ と $w \in [0, 2^{n+3})$ であって

$$d_{n+1} \overset{2^{n+1}}{\equiv} v \overset{2^{n+2}}{\equiv} w \quad \& \quad v^2 \overset{2^{n+2}}{\equiv} c_{n+2} \quad \& \quad w^2 \overset{2^{n+2}}{\equiv} = c_{n+3} \ \cdots (\spadesuit) \tag{27}$$

を満たすものを見出せばよい．

クレイム 3. 次の 4 つのうちいずれかが成り立つ：

(1) $x_{n+3} \equiv b \pmod{2^{n+2}}$;

(2) $x_{n+3} \equiv -b \pmod{2^{n+2}}$;

[*12] 証拠として $a = 3$, $b = 3$ を取ることもできる．これは平方根が 2 つ存在することにちなむ現象であろう．

(3) $x_{n+3} \equiv b + 2^{n+1} \pmod{2^{n+2}}$;
(4) $x_{n+3} \equiv -b - 2^{n+1} \pmod{2^{n+2}}$.

$\vdash x_{n+3}^2 \overset{2^{n+3}}{\equiv} c_{n+3} \overset{2^{n+2}}{\equiv} c_{n+2} \overset{2^{n+2}}{\equiv} b^2$ なので，$(x_{n+3}-b)(x_{n+3}+b) \equiv 0 \pmod{2^{n+2}}$ が成り立つ．x_{n+3} と b は奇数なので，ある $r, s \in \mathbb{Z}$ によって $x_{n+3} = 2r+1$, $b = 2s+1$ と書ける．すると $(x_{n+3}-b)(x_{n+3}+b) = 4(r-s)(r+s+1)$ が成り立つ．したがって $2^{n+2} \mid 4(r-s)(r+s+1)$ である．ゆえに $2^n \mid (r-s)(r+s+1)$ である．いま，$r-s$ と $r+s+1$ の偶奇は不一致である．場合分け．$r-s$ が偶数のとき $2^n \mid (r-s)$ でなければならない．よって $r-s = 2^n l$ なる $l \in \mathbb{Z}$ が存在する．l が偶数の場合，$r-s = 2^{n+1}l'$ $(l' \in \mathbb{Z})$ と書ける．よって $2(r-s) = 2^{n+2}l'$ となる．$2(r-s) = x_{n+3}-b$ であるから，結局 $x_{n+3} - b \equiv 0 \pmod{2^{n+2}}$ である．この場合 (1) が成立するのでよい．l が奇数の場合，$r-s = 2^n(2l'+1)$ $(l' \in \mathbb{Z})$ と書ける．よって $2(r-s) = 2^{n+2}l' + 2^{n+1}$ となる．すると $x_{n+3} - b \equiv 2^{n+1} \pmod{2^{n+2}}$ となり，この場合 (3) が成立するのでよい．$r+s+1$ が偶数のとき $2^n \mid (r+s+1)$ でなければならない．よって $r+s+1 = 2^n l$ なる $l \in \mathbb{Z}$ が存在する．l が偶数の場合，$r+s+1 = 2^{n+1}l'$ $(l' \in \mathbb{Z})$ と書ける．よって $2(r+s+1) = 2^{n+2}l'$ となる．$2(r+s+1) = x_{n+3}+b$ であるから，結局 $x_{n+3} + b \equiv 0 \pmod{2^{n+2}}$ である．この場合 (2) が成立するのでよい．l が奇数の場合，$r+s+1 = 2^n(2l'-1)$ $(l' \in \mathbb{Z})$ と書ける．よって $2(r+s+1) = 2^{n+2}l' - 2^{n+1}$ となる．すると $x_{n+3} + b \equiv -2^{n+1} \pmod{2^n}$ となり，この場合 (4) が成立するのでよい． ⊣

$b' := (b + 2^{n+1}) \mathbin{\%} 2^{n+2} \in [0, 2^{n+2})$ とおく．

クレイム 4.

$(\exists e \in [0, 2^{n+3}))\left[b \overset{2^{n+2}}{\equiv} e \ \&\ e^2 \overset{2^{n+3}}{\equiv} c_{n+3}\right]$ または $(\exists e' \in [0, 2^{n+3}))\left[b' \overset{2^{n+2}}{\equiv} e' \ \&\ e'^2 \overset{2^{n+3}}{\equiv} c_{n+3}\right]$.

$\vdash$ いま $x_{n+3}^2 \overset{2^{n+3}}{\equiv} c_{n+3} \overset{2^{n+2}}{\equiv} c_{n+2} \overset{2^{n+2}}{\equiv} b^2$ なので $(x_{n+3}-b)(x_{n+3}+b) \equiv 0 \pmod{2^{n+2}}$ である．

クレイム 3 より，2^{n+2} を法として，x_{n+3} は，b, $b+2^{n+1}$, $-b$, $-b-2^{n+1}$ のいずれかに合同である．2 つめと 4 つめは 2^{n+2} を法として b' と合同なので，結局 $x_{n+3} \equiv \pm b \pmod{2^{n+2}}$ または $x_{n+3} \equiv \pm b' \pmod{2^{n+2}}$ が成り立つ．$x_{n+3} \equiv \pm b \pmod{2^{n+2}}$ のとき，$e = (\pm x_{n+3}) \mathbin{\%} 2^{n+3}$ を証拠に前半が成立する．$x_{n+3} \equiv \pm b' \pmod{2^{n+2}}$ のとき，$e' = (\pm x_{n+3}) \mathbin{\%} 2^{n+3}$ を証拠に後半が成立する． ⊣

クレイム 4 の前半が成り立つ場合 $(v, w) := (b, e)$ を証拠に (♠) が成立する．クレイム 4 の後半が成り立つ場合 $(v, w) := (b', e')$ を証拠に (♠) が成立する．

以上で列 d_n $(n \geqslant 1)$ の構成を終わる．構成の仕方により，$d := (d_n)_n$ は $d^2 = c$ を満たす 2-進整数である．また $d_1 \neq 0$ なので，d は可逆である．$u := 2^{h/2}d \in \mathbb{Q}_2$ と定めることで，$u^2 = 2^h d^2 = 2^h c = t$ となり，所望のものが導けた． □

命題 6. p を奇素数，$t \in \mathbb{Q}_p \setminus \{0\}$ とする．以下は同値である：

(1) $(\exists u \in \mathbb{Q}_p)[t = u^2]$　(これを "t is a square in $\mathbb{Q}_p$" などという)；
(2) $(\exists! h \in \mathbb{Z})(\exists! c \in \mathbb{Z}_p^\times)[t = p^h c \ \&\ h \text{ even} \ \&\ p \nmid c_1 \ \&\ (c_1/p) = 1]$.

また，(2) の c について $(\forall n \geqslant 1)[p \nmid c_n \ \&\ (c_n/p) = 1]$ である．

証明. p を奇素数とし，$t \in \mathbb{Q}_p \setminus \{0\}$ を固定する．

(1) $\Longrightarrow$ (2) $t = u^2$ なる $u \in \mathbb{Q}_p$ が存在したと仮定する．$u \neq 0$ であるから，$u = p^k d$ となる $k \in \mathbb{Z}$ および $d \in \mathbb{Z}_p^\times$ が一意に存在する．$t = u^2 = p^{2k} d^2$ である．$h := 2k$, $c := d^2$ が (2) の条件を満たすことをいえばよい．$k \in \mathbb{Z}$ が偶数であることは定め方からよい．また $c \in \mathbb{Z}_p$ が単元であることもよい（d の乗法逆元の 2 乗が証拠）．d は可逆なので $0 < d_1 < p$. ゆえに $p \nmid d_1$ である．いま $c_1 = (d^2)_1 = d_1^2 \ \%\ p$ である[*13]．よって $p \nmid c_1$ である．また $(c_1/p) = (d_1^2 \ \%\ p/p) = (d_1^2/p) = (d_1/p)(d_1/p) = (\pm 1)^2 = 1$ となる．h, c の一意性については，$h \in \mathbb{Z}$ と $c \in \mathbb{Z}_p^\times$ と $t \neq 0$ に気を付ければ定義 3 に書いた事実よりよい．"また" については，ある $x \in \mathbb{Z}$ について $\cdots \overset{p^3}{\equiv} c_3 \overset{p^2}{\equiv} c_2 \overset{p}{\equiv} c_1 \overset{p}{\equiv} x^2 \overset{p}{\not\equiv} 0$ となっているから $\cdots \overset{p}{\equiv} c_3 \overset{p}{\equiv} c_2 \overset{p}{\equiv} c_1 \overset{p}{\equiv} x^2 \overset{p}{\not\equiv} 0$ であり，確かに $(\forall n \geqslant 1)[p \nmid c_n \ \&\ (c_n/p) = 1]$ である．

(2) $\Longrightarrow$ (1) t が (2) のような表現をもっているとし，そのような一意的な $h \in \mathbb{Z}$, $c \in \mathbb{Z}_p^\times$ をとる．上と同じくして $(\forall n \geqslant 1)[p \nmid c_n \ \&\ (c_n/p) = 1]$ である．命題 2 により $(\forall n \geqslant 1)[p \nmid c_n \ \&\ (c_n/p^n) = 1]$ である．したがって，$x_1, x_2, x_3, \ldots \in \mathbb{Z}$ で

$$(\forall n \geqslant 1)[x_n^2 \equiv c_n \pmod{p^n}] \tag{28}$$

であるものがとれる．この x_n たちをもとに

$$(\forall n \geqslant 1)[0 \leqslant d_n < p^n \ \&\ p \nmid d_n \ \&\ c_n = d_n^2 \ \%\ p^n \ \&\ (n \geqslant 2 \Rightarrow d_n \overset{p^{n-1}}{\equiv} d_{n-1})] \cdots (*) \tag{29}$$

を満たす整数列 d_n $(n \geqslant 1)$ を帰納的に構成する[*14]．

$n = 1$ については $d_1 := x_1 \ \%\ p$ とせよ．$d_1^2 \ \%\ p = (x_1 \ \%\ p)^2 \ \%\ p = x_1^2 \ \%\ p = c_1$ であり，また $x_1^2 \equiv c_1 \not\equiv 0 \pmod{p}$ なので $p \nmid d_1$ である．よって $n = 1$ の場合の $(*)$ はよい．

d_n まで構成されたと仮定する．d_{n+1} を定めたい．いま $c \in \mathbb{Z}_p$ なので $c_{n+1} \equiv c_n \pmod{p^n}$ である．したがって $x_{n+1}^2 \equiv c_{n+1} \equiv c_n \equiv d_n^2 \pmod{p^n}$ なので $(x_{n+1} + d_n)(x_{n+1} - d_n) \equiv 0 \pmod{p^n} \cdots (\dagger)$ である．

> **クレイム 1.** $p^n \mid (x_{n+1} + d_n)$ または $p^n \mid (x_{n+1} - d_n)$ である．
>
> $\vdash$ $p \nmid (x_{n+1} + d_n)$ または $p \nmid (x_{n+1} - d_n)$ であることをいえば（$(\dagger)$ よりどちらか片方の因子が p を n 個独占することになるので）十分である．$x_{n+1} + d_n = pa$, $x_{n+1} - d_n = pb$ なる $a, b \in \mathbb{Z}$ の存在を仮定して矛盾を導く．両式の差を取って $2d_n = p(a - b)$ を得る．p は奇素数だったので

[*13] $(d^2)_1 = (d \cdot d)_1 = ((d_n)_n (d_n)_n)_1 = ((d_n \cdot d_n \ \%\ p^n)_n)_1 = (((d_n)^2 \ \%\ p^n)_n)_1 = (d_1)^2 \ \%\ p^1$.

[*14] 要するに $c = d^2$ なる $d \in \mathbb{Z}_p^\times$ を作りたい．一見 $d := (x_n)_n$ とすれば良さそうにもに思えるが，それでは $\in \mathbb{Z}_p^\times$ かどうかが全く不明なので，以下の議論で適切に作り変えてやる必要がある．

$2 \mid (a-b)$ でなければならない．すると $(a-b)/2$ は整数で $d_n = p(a-b)/2$ なので $p \mid d_n$ である．これは d_n の取り方に反する． ⊣

クレイム 2． $x_{n+1} \equiv d_n \pmod{p^n}$ と $-x_{n+1} \equiv d_n \pmod{p^n}$ のどちらか一方，そして一方のみが成り立つ．

⊢ 少なくとも一方が成り立つことはクレイム 1 そのものである．排他性を示す．仮に両者ともに成り立ったとすると，辺々加えて $2d_n \equiv 0 \pmod{p^n}$ を得る．p は奇素数なので $p \mid d_n$ である．しかしこれは d_n の取り方に反する． ⊣

クレイム 2 により，d_{n+1} を矛盾なく

$$d_{n+1} := \begin{cases} x_{n+1} \mathbin{\%} p^{n+1} & \text{if } d_n \equiv x_{n+1} \pmod{p^n} \\ (-x_{n+1}) \mathbin{\%} p^{n+1} & \text{if } d_n \equiv -x_{n+1} \pmod{p^n} \end{cases} \tag{30}$$

で定めることができる．$n+1$ についての $(*)$ を確認する．どの場合も $p \nmid x_{n+1}$ なので $p \nmid d_{n+1}$ は明らか．また定め方より $0 \leqslant d_{n+1} < p^{n+1}$ も明らか．また，どの場合も % の左オペランドを y と書けば $d_{n+1} \mathbin{\%} p^n = (y \mathbin{\%} p^{n+1}) \mathbin{\%} p^n = y \mathbin{\%} p^n = d_n$ なので $d_{n+1} \equiv d_n \pmod{p^n}$ もよい．$c_{n+1} = d_{n+1}^2 \mathbin{\%} p^n$ を示す．

- $d_n \equiv x_{n+1} \pmod{p^n}$ の場合，$d_{n+1}^2 \mathbin{\%} p^{n+1} = (x_{n+1} \mathbin{\%} p^{n+1})^2 \mathbin{\%} p^{n+1} = x_{n+1}^2 \mathbin{\%} p^{n+1} = c_{n+1}$ である．
- $d_n \equiv -x_{n+1} \pmod{p^n}$ の場合，$d_{n+1}^2 \mathbin{\%} p^{n+1} = ((-x_{n+1}) \mathbin{\%} p^{n+1})^2 \mathbin{\%} p^{n+1} = (-x_{n+1})^2 \mathbin{\%} p^{n+1} = (-x_{n+1})^2 \mathbin{\%} p^{n+1} = c_{n+1}$ である．

以上で列 d_n $(n \geqslant 1)$ の構成を終わる．$(*)$ が満たされていることより $d := (d_n)_n$ は p-進整数である．また $d_1 \neq 0$ なので，d は可逆である．$(*)$ より $d^2 = c$ (in $\mathbb{Z}_p$) である．$u := p^{h/2} d \in \mathbb{Q}_p$ と定めることで，$u^2 = p^h d^2 = p^h c = t$ となり，所望のものが導けた．$(*)$ が満たされていることより，$d := (d_n)_n$ は $d^2 = c$ を満たす p-進整数である．また $d_1 \neq 0$ なので，d は可逆である．$u := 2^{h/2} d \in \mathbb{Q}_p$ と定めることで，$u^2 = 2^h d^2 = 2^h c = t$ となり，所望のものが導けた． □

次に掲げる Hasse-Minkowski による美しい定理は，補題および補題 11 の証明に用いる．

事実 7 (**Hasse–Minkowski の定理，$\mathbb{Q}$ 係数 2 次形式に関する局所大域原理**)**.** 有理数係数の 2 次形式

$$f(\vec{x}) = \sum_{i=1}^{n} a_i x_i^2 \qquad n \geqslant 1,\ a_i \in \mathbb{Q} \tag{31}$$

および有理数 $t \neq 0$ について，以下は同値である：

(1) $(\exists \vec{x} \in \mathbb{Q}^n)[f(\vec{x}) = t]$;
(2) $(\exists \vec{x} \in \mathbb{R}^n)[f(\vec{x}) = t]$ & $(\forall r\colon \text{prime})(\exists \vec{x} \in \mathbb{Q}_r^n)[f(\vec{x}) = t]$.

奇数 $u \in \mathbb{Z}$ に対し，$\varepsilon(u), \omega(u) \in \{0, 1\}$ を

$$\varepsilon(u) = \begin{cases} 0 & \text{if } r \equiv 1 \pmod 4 \\ 1 & \text{if } r \equiv 3 \pmod 4 \end{cases} \tag{32}$$

$$\omega(u) = \begin{cases} 0 & \text{if } u \equiv \pm 1 \pmod 8 \\ 1 & \text{if } u \equiv \pm 3 \pmod 8 \end{cases} \tag{33}$$

で定める[*15][*16].

定義と事実 8. (1) 素数 r および $a, b \in \mathbb{Z} \setminus \{0\}$ に対し，**Hilbert 記号** $(a, b)_r$ を

$$(a, b)_r := \begin{cases} +1 & \text{if } ax^2 + bx^2 - z^2 = 0 \text{ が } \mathbb{Q}_r \text{ に } (0,0,0) \text{ でない解をもつ} \\ -1 & \text{o.w.} \end{cases} \tag{34}$$

で定める.

(2) $a, b \in \mathbb{Z} \setminus \{0\}$ を，自然数 $\alpha, \beta \in \mathbb{N}$ と奇数 $u, v \in \mathbb{Z}$ を用いて $a = 2^\alpha u$, $b = 2^\beta v$ と表示する．このとき次が成立する：

$$(a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}. \tag{35}$$

(3) r を奇素数とする．$a, b \in \mathbb{Z} \setminus \{0\}$ を，自然数 $\alpha, \beta \in \mathbb{N}$ と $u, v \in \mathbb{Z}$（ただし $p \nmid u$ かつ $p \nmid v$）を用いて $a = r^\alpha u$, $b = r^\beta v$ と表示する．このとき次が成立する：

$$(a, b)_r = \left(\frac{u}{r}\right)^\beta \left(\frac{v}{r}\right)^\alpha (-1)^{\alpha\beta\varepsilon(r)}. \tag{36}$$

TODO: 証明.

Hilbert 記号について次の性質が成り立つ：任意の素数 r および整数 $a, b, c \in \mathbb{Z} \setminus \{0\}$ について，

$$(a, b)_r = (b, a)_r, \qquad (1, a)_r = 1, \qquad (a, bc)_r = (a, b)_r (a, c)_r. \tag{37}$$

1 つめは定義の対称性から自明である．2 つめも $x^2 + ay^2 - z^2 = 0$ は非自明解 $(1, 0, 1)$ をもつことからよい．
TODO: 3 つめ

[*15] これは標準的に用いられている記号である.
[*16] 同じことだが，$\varepsilon(u) = \frac{u-1}{2}$ % 2, $\omega(u) = \frac{u^2-1}{8}$ % 2 とも書ける.

補題 9. (1) p, r を素数，$p \equiv 3 \pmod 4$ とする．このとき，任意の $t \in \mathbb{Q} \setminus \{0\}$ について (A) と (B) は同値である：

(A) $(\exists x, y, z \in \mathbb{Q}_r)[x^2 + y^2 - pz^2 = t]$;

(B) $(r \neq 2 \ \& \ r \neq p)$ または $\neg(\exists s \in \mathbb{Q}_r)[t = ps^2]$.

(2) p, r を素数，$p \equiv 1 \pmod 4$ とし，$q \neq p$ を $(q/p) = -1$ をみたす奇素数とする．このとき，任意の $t \in \mathbb{Q} \setminus \{0\}$ について (A) と (B) は同値である：

(A) $(\exists x, y, z \in \mathbb{Q}_r)[x^2 + qy^2 - pz^2 = t]$;

(B) $(r \neq p \ \& \ r \neq q)$ または $\neg(\exists s \in \mathbb{Q}_r)[t = pqs^2]$.

証明. 3 元 2 次形式に関する次の事実[*17]を認めることとする．

事実． $a, b, c \in \mathbb{Z} \setminus \{0\}$，$w \in \mathbb{Q}$ とする．このとき，(a) と (b) は同値である：

(a) $(\exists x, y, z \in \mathbb{Q}_r)[ax^2 + by^2 + cz^2 = w]$;

(b) $(-1, -abc)_r = (a, b)_r (b, c)_r (a, c)_r$ または $\neg(\exists s \in \mathbb{Q}_r)[w = -abcs^2]$

(1) p, r を素数，$p \equiv 3 \pmod 4$ とし，$t \in \mathbb{Q} \setminus \{0\}$ を固定する．

クレイム 1． 次が成り立つ：

(a) $r = 2 \implies (-1, p)_r = -1$;

(b) $r = p \implies (-1, p)_r = -1$;

(c) $(r \neq 2 \ \& \ r \neq p) \implies (-1, p)_r = 1$;

したがって，$(-1, p)_r = 1 \iff r \neq 2 \ \& \ r \neq p$ である．

$\vdash$ -1 と p を適切に分解し，定義 8 に掲げた事実を用いて計算するだけである．

(a): $r = 2$ とする．$-1 = r^0(-1)$, $p = r^0 p$, $r \nmid (-1)$, $r \nmid p$ と表示できる．そこで $(\alpha, \beta, u, v) := (0, 0, -1, p)$ と置く．$\varepsilon(u) = 1$, $\varepsilon(v) = 1$ である．よって $(-1, p)_r = (-1)^{1 \cdot 1 + 0 \cdot \omega(v) + 0 \cdot \omega(u)} = (-1)^1 = -1$ である．

(b): $r = p$ とする．$-1 = r^0(-1)$, $p = r^1(-1)$, $r \nmid (-1)$, $r \nmid (-1)$ と表示できる．そこで $(\alpha, \beta, u, v) := (0, 1, -1, -1)$ と置く．$\varepsilon(u) = 1$, $\varepsilon(v) = 1$ である．よって $(-1, p)_r = (-1/r)^1 (-1/r)^0 (-1)^{0 \cdot 1 \cdot \varepsilon(r)} = (-1/r) = (-1)^{\varepsilon(r)} = (-1)^1 = -1$ である (cf. [4] Chap. 1 §3 Thm. 5 (ii), also [6] 定理 1.11.10 (1))．

(c): $r \neq 2$ かつ $r \neq p$ とする．$-1 = r^0(-1)$, $p = r^0 p$, $r \nmid (-1)$, $r \nmid p$ と表示できる．そこで $(\alpha, \beta, u, v) := (0, 0, -1, p)$ と置く．すると $(-1, p)_r = (-1/r)^0 (p/r)^0 (-1)^{0 \cdot 0 \cdot \varepsilon(r)} = 1$ である．

“したがって” は (a)–(c) の言い換えにすぎない． $\dashv$

[*17] **TODO:** これが書いてある文献を探す

(A) $\Longrightarrow$ (B) (A) を仮定する．つまり $(a,b,c,w)=(1,1,-p,t)$ として事実の (a) の条件が満たされていると仮定する．事実の (a)⇒(b) より $(-1,p)_r=(1,1)_r(1,-p)_r(1,-p)_r$ または $\neg(\exists s\in\mathbb{Q}_r)[t=ps^2]$ である．後者の場合は自明に (B) が満たされる．前者の場合，右辺の因子はすべて 1 に等しいので $(-1,p)_r=1$ である．クレイム 1 より $r\neq 2$ かつ $r\neq p$ である．よってこの場合も (B) が満たされる．

(B) $\Longrightarrow$ (A) (B) を仮定する．$r\neq 2$ & $r\neq p$ の場合はクレイム 1 より $(-1,p)_r=1$ である．したがって $(-1,p)_r=(1,1)_r(1,-p)_r(1,-p)_r$ である．$(a,b,c,w)=(1,1,-p,t)$ として事実の (b) の条件が満たされるので，事実の (b)⇒(a) より所望の $(\exists x,y,z\in\mathbb{Q}_r)[x^2+y^2-pz^2=t]$ を得る．

(2) p,r を素数，$p\equiv 1 \pmod 4$ とし，$q\neq p$ を $(q/p)=-1$ なる奇素数とする．$t\in\mathbb{Q}\setminus\{0\}$ を固定する．

クレイム 2. 次が成り立つ：

(a) $r=2 \implies (p,-q)_r=1$;

(b) $r=p \implies (p,-q)_r=-1$;

(c) $r=q \implies (p,-q)_r=-1$;

(d) $r\neq 2$ & $r\neq p$ & $r\neq q \implies (p,-q)_r=1$.

したがって $(p,-q)_r=1 \iff r\neq p$ & $r\neq q$ である．

$\vdash$ p と $-q$ を適切に分解し，定義 8 に掲げた事実を用いて計算するだけである．

(a): $r=2$ とする．$p=r^0p$, $-q=r^0(-q)$, $r\nmid p$, $r\nmid(-q)$ と表示できる．そこで $(\alpha,\beta,u,v):=(0,0,p,-q)$ と置く．$\varepsilon(u)=0$ なので $(p,-q)_r=(-1)^{0\cdot\varepsilon(v)+0\cdot\omega(v)+0\cdot\omega(u)}=(-1)^0=1$ である．

(b): $r=p$ とする．$p=r^1\cdot 1$, $-q=r^0(-q)$, $r\nmid 1$, $r\nmid(-q)$ と表示できる．そこで $(\alpha,\beta,u,v):=(1,0,1,-q)$ と置く．すると $(p,-q)_r=(1/r)^0(-q/r)^1(-1)^{1\cdot 0\cdot\varepsilon(r)}=(-q/r)=(q/r)(-1/r)=-(-1/r)=-(-1)^{\varepsilon(r)}=-(-1)^0=-1$ である．

(c): $r=q$ とする．$p=r^0p$, $-q=r^1(-1)$, $r\nmid p$, $r\nmid(-1)$ と表示できる．そこで $(\alpha,\beta,u,v):=(0,1,p,-1)$ と置く．$(p,-q)_r=(p/q)^1(-1/q)^0(-1)^{0\cdot 1\cdot\varepsilon(r)}=(p/r)=(p/q)=(q/p)\cdot(-1)^{\varepsilon(p)\varepsilon(q)}=-(-1)^{0\cdot\varepsilon(q)}=-1$ (cf. [4] Chap. 1 §3 Thm. 6, also [6] 定理 1.11.10 (3) 平方剰余の相互法則).

(d): $r\neq 2$ & $r\neq p$ & $r\neq q$ とする．$p=r^0p$, $-q=r^0(-q)$, $r\nmid p$, $r\nmid(-q)$ と表示できる．そこで $(\alpha,\beta,u,v):=(0,0,p,-q)$ と置く．$\varepsilon(u)=1$, $\varepsilon(v)=1$ である．よって $(p,-q)_r=(p/r)^0(-q/r)^0(-1)^{0\cdot 0\cdot\varepsilon(r)}=1$ である．

“したがって”：($\Rightarrow$) $(p,-q)_r=1$ とする．(b) の対偶より $r\neq p$ がわかり，(c) の対偶より $r\neq q$ がわかる．($\Leftarrow$) $r\neq p$ & $r\neq q$ とする．$r=2$ なら (a) より $(p,-q)_r=1$ であり，$r\neq 2$ なら (d) より $(p,-q)_r=1$ であるので，いずれにせよ $(p,-q)_r=1$ である． $\dashv$

(A) $\Longrightarrow$ (B) (A) を仮定する．

クレイム 3. $(p,-q)_r=1$ または $\neg(\exists s\in\mathbb{Q}_r)[t=pqs^2]$ が成り立つ．

⊢ いま．(A)，つまり $(a,b,c,w)=(1,q,-p,t)$ として事実の (a) の条件が満たされている．事実の (a)⇒(b) より $(-1,pq)_r=(1,q)_r(q,-p)_r(1,-p)_r\cdots(*)$ または $\neg(\exists s\in\mathbb{Q}_r)[t=pqs^2]$ である．後者の場合は自明にクレイムが満たされる．前者の場合を考える．$(1,q)_r=(1,-p)_r=1$ なので，$(*)$ は $(-1,pq)_r=(q,-p)_r\cdots(\dagger)$ と変形できる．Hilbert 記号の性質により，

(1) $(-1,pq)_r=(-1,p)_r(-1,q)_r$;

(2) $(q,-p)_r=(q,-1)_r(q,p)_r=(-1,q)_r(q,p)_r=(-1,q)_r(-1,p)_r(-q,p)_r$;

が成り立つ．すると $(p,-q)_r=(-q,p)_r\overset{(2)}{=}(q,-p)_r/(-1,q)_r(-1,p)_r\overset{(1)}{=}(q,-p)_r/(-1,pq)_r\overset{(\dagger)}{=}(q,-p)_r/(q,-p)_r=1$ がわかる．以上でクレイム 3 が示された． ⊣

クレイム 3 の後半が成り立っている場合 (B) は満たされるのでよい．クレイム 3 の前半が成り立っている場合も，クレイム 2 より $r\neq p$ かつ $r\neq q$ となるので (B) が満たされる．以上で (A)⇒(B) が示せた．

(B)⟹(A) (B) を仮定する．$r\neq p$ & $r\neq q$ の場合．クレイム 2 より $(p,-q)_r=1$ である．このことと Hilbert 記号の諸性質から $(-1,pq)_r=(1,q)_r(1,-p)_r(q,-p)_r$ がわかる[*18]．したがって $(a,b,c,w)=(1,q,-p,t)$ として事実の (b) の条件が満たされるので，事実の (b)⇒(a) より所望の $(\exists x,y,z\in\mathbb{Q}_r)[x^2+qy^2-pz^2=t]$ を得る． □

続く補題と補題 11 で Hasse–Minkowski の定理を用いる．[3] では補題と補題 11 の証明を与えていない．

補題 10 (Lemma 1 in [3])**.** p を，$p\equiv 3\pmod 4$ を満たす素数とする．このとき，任意の $t\in\mathbb{Q}\setminus\{0\}$ について以下は同値である：

(1) $(\exists x,y,z\in\mathbb{Q})[x^2+y^2-pz^2=t]$;

(2) $\neg(\exists k\in\mathbb{Z})(\exists s\in\mathbb{Q})[t=ks^2\ \&\ k\equiv p\pmod 8]$ &
$\neg(\exists k\in\mathbb{Z})(\exists s\in\mathbb{Q})[t=pks^2\ \&\ p\nmid k\ \&\ (k/p)=1]$

証明. p を $p\equiv 3$ なる素数とし，$t\in\mathbb{Q}\setminus\{0\}$ を任意に取り固定する．

クレイム 1. (1) は次に掲げる (1)' と同値である：

$$(1)'\qquad (\forall r\colon \text{prime})(\exists x,y,z\in\mathbb{Q}_r)[x^2+y^2-pz^2=t]. \tag{38}$$

⊢ まず，Hasse–Minkowski の定理（定理 7）より，(1) は (1)' & $(\exists x,y,z\in\mathbb{R})[x^2+y^2-pz^2=t]$ であることと同値である．ところが後半は $t>0$ なら $(x,y,z)=(\sqrt{t},0,0)$ として，$t<0$ なら $(x,y,z)=(0,0,\sqrt{-t/p})$ として常に真なので，結局 (1) と (1)' は同値である． ⊣

クレイム 1 により，補題を示すには (1)' ⟺ (2) を示せば十分である．

[*18] $\because (-1,pq)_r=(-1,p)_r(-1,q)_r=(-1,p)_r\cdot 1\cdot(-1,q)_r=(-1,p)_r(p,-q)_r(-1,q)_r=(-1,p)_r(-q,p)_r(q,-1)_r=(q,p)_r(q,-1)_r=(q,-p)_r=(1,q)_r(1,-p)_r(q,-p)_r$. **TODO:** もっと楽に

$\boxed{(2) \Longrightarrow (1)'}$ (2) を仮定する．(1)' を示すため，勝手な素数 r を取る．$r \neq 2$ & $r \neq p$ の場合は補題 9(1) の (B) $\Longrightarrow$ (A) よりよい．$r = 2$ の場合と $r = p$ の場合を考える．

• $r = 2$ の場合．$\neg(\exists a \in \mathbb{Q}_2)[t = pa^2]$ をいえば，同じく補題 9(1) の (B) $\Longrightarrow$ (A) より (1)' が従うのでこれを示す．$t = pa^2$ なる $a \in \mathbb{Q}_2$ がとれたとして矛盾を導く．$t \neq 0$ より $a^2 \neq 0$ である．命題 5 より，$a^2 = 2^h c$ & $(\forall n \geqslant 1)[c_n \equiv 1 \pmod 8]$ を満たすような偶数 $h \in \mathbb{Z}$ および $c \in \mathbb{Z}_2^\times$ が一意に存在する．$c = a^2/2^h = t/(2^h p) \in \mathbb{Q}$ である．そこで c を $c = u/v$ $(u \in \mathbb{Z},\ v \in \mathbb{Z} \setminus \{0\})$ として既約分数表示する．命題 4 の $(\Rightarrow)$ より，$2 \nmid u$ & $2 \nmid v$ である．$k := puv \in \mathbb{Z}$, $s := 2^{h/2}/v \in \mathbb{Q}$ と定めよ．すると $ks^2 = puv \cdot 2^h/v^2 = p \cdot 2^h \cdot u/v = p \cdot 2^h c = pa^2 = t$ である．また $c = u/v$ より $u = cv$，正確には $\hat{u} = c\hat{v}$ が $\mathbb{Z}_2$ で成り立っている．したがって $\hat{u}\hat{v} = c\hat{v}\hat{v}$，つまり $(uv \mathbin{\%} 2^n)_n = (c_n v^2 \mathbin{\%} 2^n)_n$ が $\mathbb{Z}_2$ で成り立つ．特に $n = 3$ に注目することで $uv \equiv c_3 v^2 \pmod 8$ が $\mathbb{Z}$ で成り立つ．いま v は奇数なので $v^2 \equiv 1 \pmod 8$ であり，$(\forall n \geqslant 1)[c_n \equiv 1 \pmod 8]$ だったから $c_3 \equiv 1 \pmod 8$ である．よって $uv \equiv 1 \pmod 8$ となり，$k = puv \equiv p \pmod 8$ である．結局 $t = ks^2$, $k \equiv p \pmod 8$ なる $k \in \mathbb{Z}$, $s \in \mathbb{Q}$ が見出せたことになるが，これは (2) に反する．

• $r = p$ の場合．同じく $(\exists a \in \mathbb{Q}_p)[t = pa^2]$ から矛盾を導けばよい．$t = pa^2$ なる $a \in \mathbb{Q}_p$ がとれたとする．$a^2 = t/p \in \mathbb{Q}$ である．命題 6 より，$a^2 = p^h c$ & $p \nmid c_1$ & $(c_1/p) = 1$ を満たすような偶数 $h \in \mathbb{Z}$ および $c \in \mathbb{Z}_p^\times$ が一意に存在する．$c = a^2/p^h = t/p^{h+1} \in \mathbb{Q}$ である．そこで $c = u/v$ $(u \in \mathbb{Z},\ v \in \mathbb{Z} \setminus \{0\})$ として既約分数表示する．命題 4 の $(\Rightarrow)$ より，$p \nmid u$ & $p \nmid v$ である．$k := uv \in \mathbb{Z}$, $s := p^{h/2}/v \in \mathbb{Q}$ と定めよ．すると $pks^2 = puv \cdot p^h/v^2 = p \cdot p^h \cdot u/v = p \cdot p^h c = pa^2 = t$ である．$p \nmid u$ & $p \nmid v$ より $p \nmid k$ である．また $c = u/v$ より $u = cv$，正確には $\hat{u} = c\hat{v}$ が $\mathbb{Z}_p$ で成り立っている．したがって $\hat{u}\hat{v} = c\hat{v}\hat{v}$，つまり $(uv \mathbin{\%} p^n)_n = (c_n v^2 \mathbin{\%} p^n)_n$ が $\mathbb{Z}_p$ で成り立つ．特に $n = 1$ に注目することで $uv \equiv c_1 v^2 \pmod p$ が $\mathbb{Z}$ で成り立つ．したがって $(k/p) = (uv/p) = (c_1 v^2/p) = (c_1/p)(v/p)(v/p) = 1 \cdot (\pm 1)^2 = 1$ である．結局 $t = pks^2$, $(k/p) = 1$ なる $k \in \mathbb{Z}$, $s \in \mathbb{Q}$ が見出せたことになるが，これは (2) に反する．

$\boxed{(1)' \Longrightarrow (2)}$ (1)' を仮定する．$\neg(2)$ が成り立つとして矛盾を導く．まず，(1)' と補題 9 の (1) より $(\forall r\colon \text{prime})[(r \neq 2$ & $r \neq p)$ or $\neg(\exists w \in \mathbb{Q}_r)[t = pqw^2]]$，つまり $(\forall r\colon \text{prime})[(r = 2 \text{ or } r = p) \Longrightarrow \neg(\exists w \in \mathbb{Q}_r)[t = pqw^2]]$ を得る．特に $r = 2, p$ とすることで

$$\neg(\exists w \in \mathbb{Q}_2)[t = pw^2] \ \&\ \neg(\exists w \in \mathbb{Q}_p)[t = pw^2] \qquad \cdots(*) \tag{39}$$

を得る．いま (2) が成り立つと仮定しているのであった．場合分け．

• $(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[t = ks^2$ & $k \equiv p \pmod 8]$ の場合．そのような k, s を取る．いま，$p \in \mathbb{Z}$ の $\mathbb{Z}_2$ への埋め込み $\hat{p} = (p \mathbin{\%} 2^n)_n$ について，$2 \nmid p$ だったので，その第 1 成分は 1 である．したがって $\hat{p}$ は可逆なので $a \in \mathbb{Z}_2^\times$ で $\hat{p}a = 1$ (in $\mathbb{Z}_2$) なるものがとれる．$(\forall n \geqslant 1)[pa_n \equiv 1 \pmod{2^n}]$ が成り立つから，$(\forall n \geqslant 3)[pa_n \equiv 1 \pmod 8]$ が成り立つ．$\hat{k}a \in \mathbb{Z}_2$ の各成分を考える．$n \geqslant 3$ のとき，$p \equiv k \pmod 8$ に注意して $(\hat{k}a)_n \mathbin{\%} 8 = (ka_n \mathbin{\%} 2^n) \mathbin{\%} 8 = ka_n \mathbin{\%} 8 = pa_n \mathbin{\%} 8 = 1$ である．$n = 1$ のとき，$(\hat{k}a)_1 = ka_1 \mathbin{\%} 2 = 1$, である．$n = 2$ のとき，まず $pa_2 \equiv 1 \pmod 4$ であり $p \equiv 3 \pmod 4$ だったので $a_2 = 3$ でしかありえない．また $k \equiv p \equiv 3 \pmod 4$ なので $(\hat{k}a)_2 = ka_2 \mathbin{\%} 4 = 3^2 \mathbin{\%} 4 = 1$ である．結局 $(\forall n \geqslant 1)[(\hat{k}a)_n \equiv 1 \pmod 8]$ である．$\hat{k}a = 2^0 \cdot \hat{k}a$ と 2-進展開表示する．命題 6 を $h = 0$, $c = \hat{k}a$ として用いて，$u^2 = \hat{k}a$ なる $u \in \mathbb{Q}_2$ を

得る．すると $\mathbb{Q}_2$ で $t = ks^2 = k \cdot 1 \cdot s^2 = kpas^2 = pkas^2 = p(us)^2$, $us \in \mathbb{Q}_2$ を得る[*19]．これは $(*)$ の前半部分と矛盾する．

• $(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[t = pks^2 \ \&\ p \nmid k \ \&\ (k/p) = 1]$ の場合．そのような k, s を取る．$p \nmid k$ に注意すると，k の $\mathbb{Q}_p$ への埋め込み $\hat{k} = (k \ \%\ p^n)_n$ の第 1 成分は $k \ \%\ p \neq 0$ である．よって $\hat{k} \in \mathbb{Z}^\times$ である．$\hat{k} = p^0 \cdot \hat{k}$ と p-進展開表示する．$(\hat{k})_1 = k \ \%\ p$ について $p \nmid (k \ \%\ p)$ かつ $(k \ \%\ p/p) = (k/p) = 1$ に注意すると，命題 6 を $h = 0$, $c = \hat{k}$ として用いて $u \in \mathbb{Q}_p$ で $\hat{k} = u^2$ なるものがとれる．したがって $t = pks^2 = pu^2s^2 = p(us)^2$, $us \in \mathbb{Q}_p$ を得る[*20]．これは $(*)$ の後半部分と矛盾する． □

補題 11 (Lemma 2 in [3])**.** p, q を，$p \neq q$, $(q/p) = -1$ および $p \equiv 1 \pmod 4$ を満たす奇素数とする．このとき，任意の $t \in \mathbb{Q} \setminus \{0\}$ について以下は同値である：

(1) $(\exists x, y, z \in \mathbb{Q})[x^2 + qy^2 - pz^2 = t]$;
(2) $\neg(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[t = pks^2 \ \&\ p \nmid k \ \&\ (k/p) = -1] \ \&$
$\neg(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[t = qks^2 \ \&\ p \nmid k \ \&\ (k/q) = -1]$

証明. p, q を定理の仮定を満たす勝手な奇素数とする．平方剰余の相互法則 (cf. [4] Chap. 1 §3 Thm. 6, also [6] 定理 1.11.10 (3)) より $(p/q) = (q/p) \cdot (-1)^{\varepsilon(p)\varepsilon(q)} = -(-1)^{0 \cdot \varepsilon(q)} = -1$ であることを指摘しておく．$t \in \mathbb{Q} \setminus \{0\}$ を任意に取り固定する．

> **クレイム 1.** (1) は次に掲げる (1)' と同値である：
>
> $$(1)' \qquad (\forall r\colon \text{prime})(\exists x, y, z \in \mathbb{Q}_r)[x^2 + qy^2 - pz^2 = t]. \tag{40}$$
>
> ⊢ まず，Hasse–Minkowski の定理（定理 7）より，(1) は (1)' & $(\exists x, y, z \in \mathbb{R})[x^2 + qy^2 - pz^2 = t]$ であることと同値である．ところが後半は $t > 0$ なら $(x, y, z) = (\sqrt{t}, 0, 0)$ として，$t < 0$ なら $(x, y, z) = (0, 0, \sqrt{-t/p})$ として常に真なので，結局 (1) と (1)' は同値である． ⊣

クレイム 1 により，補題を示すには (1)' $\iff$ (2) を示せば十分である．

(2) $\Longrightarrow$ (1)' (2) を仮定する．(1)' を示すため，勝手な素数 r を取る．$r \neq p$ & $r \neq q$ の場合は補題 9(1) の (B) $\Longrightarrow$ (A) よりよい．$r = p$ の場合と $r = q$ の場合を考える．

• $r = p$ の場合．$\neg(\exists a \in \mathbb{Q}_p)[t = pqa^2]$ をいえば，同じく補題 9(2) の (B) $\Longrightarrow$ (A) より (1)' が従うのでこれを示す．$t = pqa^2$ なる $a \in \mathbb{Q}_p$ がとれたとして矛盾を導く．$a^2 = t/pq \in \mathbb{Q}$ である．$t \neq 0$ より $a^2 \neq 0$ である．命題 6 より，$a^2 = p^h c$ & $p \nmid c_1$ & $(c_1/p) = 1$ を満たすような偶数 $h \in \mathbb{Z}$ および $c \in \mathbb{Z}_p^\times$ が一意に存在する．$c = a^2/p^h \in \mathbb{Q}$ である．そこで $c = u/v$ $(u \in \mathbb{Z},\ v \in \mathbb{Z} \setminus \{0\})$ として既約分数表示する．命題 4 の $(\Rightarrow)$ より，$p \nmid u$ & $p \nmid v$ である．$k := quv \in \mathbb{Z}$, $s := p^{h/2}/v \in \mathbb{Q}$ と定めよ．$p \nmid k$ で

[*19] **TODO:** この計算で $\mathbb{Q}$, $\mathbb{Q}_2$, $\mathbb{Z}_2$ の元を大雑把に同一視をしているので，もうちょい丁寧に書きなおすかも．キリがないけど……．
[*20] **TODO:** この計算で $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Z}_p$ の元を大雑把に同一視をしているので，もうちょい丁寧に書きなおすかも．キリがないけど……．

ある．$pks^2 = pquv \cdot p^h/v^2 = pq \cdot p^h \cdot u/v = pq \cdot p^h c = pqa^2 = t$ である．また $c = u/v$ より $u = cv$, 正確には $\hat{u} = c\hat{v}$ が $\mathbb{Z}_p$ で成り立っている．したがって $\hat{u}\hat{v} = c\hat{v}\hat{v}$，つまり $(uv \ \%\ p^n)_n = (c_n v^2 \ \%\ p^n)_n$ が $\mathbb{Z}_p$ で成り立つ．特に $n = 1$ に注目することで $uv \equiv c_1 v^2 \pmod{p}$ が $\mathbb{Z}$ で成り立つ．したがって $(k/p) = (quv/p) = (qc_1v^2/p) = (q/p)(c_1/p)(v/p)(v/p) = (-1) \cdot 1 \cdot (\pm 1)^2 = -1$ である．結局 $t = pks^2$, $p \nmid k$, $(k/p) = -1$ なる $k \in \mathbb{Z}$, $s \in \mathbb{Q}$ が見出せたことになるが，これは (2) に反する．

• $r = q$ の場合．$(p/q) = -1$ に注意すれば，上の議論の p と q を機械的に入れ替えて全く同様に (1)' が導かれる．

$\boxed{\text{(1)'} \Longrightarrow \text{(2)}}$ (1)' を仮定する．¬(2) が成り立つとして矛盾を導く．まず，(1)' と補題 9 の (2) より $(\forall r\colon \text{prime})[(r \neq p \ \&\ r \neq q) \text{ or } \neg(\exists w \in \mathbb{Q}_r)[t = pqw^2]]$，つまり $(\forall r\colon \text{prime})[(r = p \text{ or } r = q) \implies \neg(\exists w \in \mathbb{Q}_r)[t = pqw^2]]$ を得る．特に $r = p, q$ とすることで

$$\neg(\exists w \in \mathbb{Q}_p)[t = pqw^2] \ \&\ \neg(\exists w \in \mathbb{Q}_q)[t = pqw^2] \qquad (*) \tag{41}$$

を得る．いま ¬(2) が成り立つと仮定しているのであった．場合分け．

• $(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[t = pks^2 \ \&\ p \nmid k \ \&\ (k/p) = -1]$ の場合．そのような k, s を取る．いま，$q \in \mathbb{Z}$ の $\mathbb{Z}_p$ への埋め込み $\hat{q} = (q \ \%\ p^n)_n$ について，$p \neq q$ だったので，その第 1 成分は $q \ \%\ p \neq 0$ である．したがって $a \in \mathbb{Z}_p^\times$ で $\hat{q}a = 1$ (in $\mathbb{Z}_p$) なるものがとれる．$\hat{q}a$ の第 1 成分について $qa_1 \ \%\ p = 1$ であるから $qa_1 \equiv 1 \pmod{p}$ である．したがって $(q/p)(a_1/p) = (qa_1/p) = (1/p) = 1$ となり，仮定より $(q/p) = -1$ だったので $(a_1/p) = -1$ である．いま，$\hat{k} \in \mathbb{Z}_p$ の第 1 成分は $k \ \%\ p \neq 0$ である．したがって $\hat{k} \in \mathbb{Z}_p^\times$ である．したがって $a\hat{k} \in \mathbb{Z}_p^\times$ である．$a\hat{k}$ の第 1 成分 $a_1 k \ \%\ p$ について $(a_1 k \ \%\ p/p) = (a_1 k/p) = (a_1/p)(k/p) = (-1)^2 = 1$ である．$a\hat{k} = p^0 \cdot a\hat{k}$ と p-進展開表示する．命題 6 を $r = p$, $h = 0$, $c = a\hat{k}$ として用いて，$u^2 = \hat{a}k$ なる $u \in \mathbb{Q}_p$ を得る．すると $\mathbb{Q}_p$ で $t = pks^2 = p \cdot 1 \cdot ks^2 = pqaks^2 = pqu^2s^2 = pq(us)^2$, $us \in \mathbb{Q}_p$ を得る[*21]．これは $(*)$ の前半部分と矛盾する．

• $(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[t = qks^2 \ \&\ q \nmid k \ \&\ (k/q) = -1]$ の場合．$(p/q) = -1$ に注意すれば，上の議論の p と q を機械的に入れ替えて全く同様に矛盾が導かれる． □

ようやく 1 つめの主定理にたどり着いた．

定理 12 (Lemma 3 in [3]，再掲)**.** p を $p \equiv 3 \pmod{4}$ なる素数，t を有理数とし，$t = u/v$ と既約分数として表示する $(u, v \in \mathbb{Z},\ v \neq 0)$．このとき以下は同値である：

(A) $(\exists x, y, z \in \mathbb{Q})[pt^2 + 2 = x^2 + y^2 - pz^2]$;

(B) $2 \nmid v \ \ \&\ \ p \nmid v$.

証明. 定理の仮定のように p, t, u, v をとって固定する．まず，斉次性が効いて次が成り立つ：

[*21] **TODO:** この計算で $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Z}_p$ の元を大雑把に同一視をしているので，もうちょい丁寧に書きなおすかも．キリがないので書き直さないかも．

クレイム 1. (A) は次に掲げる (A)' と同値である：

$$\text{(A)':}\quad (\exists x,y,z\in\mathbb{Q})[pu^2+2v^2=x^2+y^2-pz^2]. \tag{42}$$

$\vdash$ $\underline{\text{(A)}\Rightarrow\text{(A)'}}$ $pt^2+2=x_0^2+y_0^2-pz_0^2$，すなわち $pu^2/v^2+2=x_0^2+y_0^2-pz_0^2$ なる $x_0,y_0,z_0\in\mathbb{Q}$ がとれたとする．両辺に v^2 を乗じて $pu^2+2v^2=(vx_0)^2+(vy_0)^2-p(vz_0)^2$ を得る．よって $(x,y,z)=(vx_0,vy_0,vz_0)\in\mathbb{Q}^3$ を証拠に (A)' が成立する． $\underline{\text{(A)'}\Rightarrow\text{(A)}}$ $pu^2+2v^2=x_1^2+y_1^2-pz_1^2$ なる $x_1,y_1,z_1\in\mathbb{Q}$ がとれたとする．$v\neq 0$ に注意して両辺を v^2 で除し，$p(u/v)^2+2=(x_1/v)^2+(y_1/v)^2-p(z_1/v)^2$ を得る（念のため：平方剰余記号でなくただの分数）．$u/v=t$ だったから，結局 $(x,y,z)=(x_1/v,y_1/v,z_1/v)\in\mathbb{Q}^3$ を証拠に (A)' が成立する． $\dashv$

したがって，定理を示すには次の 3 つの含意を示せばよい[*22]：

イ $2\mid v \implies \neg$(A)';
ロ $2\nmid v$ & $p\mid v \implies \neg$(A)';
ハ $2\nmid v$ & $p\nmid v \implies$ (A)'.

これらを順に示していく．

イ $2\mid v$ とする．$v=2a$ $(a\in\mathbb{Z})$ と書く．$t=u/v$ の既約性より $2\nmid u$ である．$u=2b+1$ $(b\in\mathbb{Z})$ と書く．

クレイム 2. $pu^2+2v^2\equiv p \pmod 8$ である．

$\vdash$ $b(b+1)$ は連続する整数の積なので偶数である．$b(b+1)=2c$ $(c\in\mathbb{Z})$ と書く．すると $pu^2+2v^2-p=p(2b+1)^2+2(2a)^2-p=p(2b+1)^2-p+8a^2=4pb(b+1)+8a^2=8(pc+a^2)\equiv 0 \pmod 8$ なので結局 $pu^2+2v^2\equiv p \pmod 8$ である． $\dashv$

よって

$$0\neq pu^2+2v^2=(pu^2+2v^2)\cdot 1^2,\qquad pu^2+2v^2\equiv p \pmod 8 \tag{43}$$

の形に書けた．補題より，所望の $\neg(\exists x,y,z\in\mathbb{Q})[pu^2+2v^2=x^2+y^2-pz^2]$，つまり $\neg$(A)' を得る．

ロ v を奇数，$p\mid v$ とする．$v=pa$ $(a\in\mathbb{Z})$ と書く．$pu^2+2v^2=pu^2+2p^2a^2=p(u^2+2pa^2)$ である．いま，$t=u/v$ の既約性より $p\nmid u$ である．したがって $p\nmid(u^2+2pa^2)$ である．また $(u^2+2pa^2/p)=(u^2/p)=(u/p)(u/p)=(\pm 1)^2=1$ である．結局

$$0\neq pu^2+2v^2=p(u^2+2pa^2)\cdot 1^2,\qquad p\nmid(u^2+2pa^2),\qquad \left(\frac{u^2+2pa^2}{p}\right)=1 \tag{44}$$

の形に書けた．補題より，所望の $\neg(\exists x,y,z\in\mathbb{Q})[pu^2+2v^2=x^2+y^2-pz^2]$，つまり $\neg$(A)' を得る．

ハ $2\nmid v$ & $p\nmid v$ とする．

[*22] イ，ロより $2\mid v$ or $(2\nmid v$ & $p\mid v) \implies \neg$(A)'，すなわち $\top$ & $(2\mid v$ or $p\mid v) \implies \neg$(A)'，すなわち $(2\mid v$ or $p\mid v) \implies \neg$(A)'，すなわち $\neg$(B) $\implies \neg$(A)'，すなわち (A)' $\implies$ (B) がわかる．ハは (B) $\implies$ (A)' そのもの．

クレイム 3. 次の否定が成り立つ：

$$(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[pu^2 + 2v^2 = pks^2 \ \&\ p \nmid k \ \&\ (k/p) = -1] \text{ or}$$
$$(\exists k \in \mathbb{Z})(\exists s \in \mathbb{Q})[pu^2 + 2v^2 = ks^2 \ \&\ k \equiv p \pmod 8].$$

$\vdash$ 上式か下式のいずれかが成り立つとして矛盾を導く．上式が成立したとする．そのような k, s をとり，$s = n/d$ $(n, d \in \mathbb{Z}, d \neq 0)$ と既約分数として表示する．すると $d^2(pu^2 + 2v^2) = pkn^2$ となり，$p \mid d^2(pu^2 + 2v^2)$，したがって $p \mid 2d^2v^2$ である．いま $p \nmid v$ を仮定していたので $p \mid d$ である．したがって $d = pe$ $(e \in \mathbb{Z})$ と書ける．すると $p^2e^2(pu^2 + 2v^2) = pkn^2$ ゆえ $pe^2(pu^2 + 2v^2) = kn^2$ となり，$p \mid kn^2$ である．いま $p \nmid k$ であったから $p \mid n^2$ となり，$p \mid n$ である．よって d と n は p を共通素因数として持つことになるが，これは $s = n/d$ の既約性に反する．
下式が成立したとする．そのような k, s をとり，$s = n/d$ $(n, d \in \mathbb{Z}, d \neq 0)$ と既約分数として表示する．すると $d^2(pu^2 + 2v^2) = kn^2$ となる．したがって $d^2(pu^2 + 2v^2) \ \%\ 4 = kn^2 \ \%\ 4 \cdots (*)$ である．しかしこれは矛盾である〔まず仮定より $k \equiv p \equiv 3 \pmod 4$ であることに気を付ける．n が偶数の場合 $(*)$ の右辺は 0 である．$s = n/d$ の既約性より d は奇数である．すると，奇数の 2 乗は常に $\equiv 1 \pmod 4$ であることに注意すれば，4 を法として $d^2(pu^2 + 2v^2) \equiv 1 \cdot (p \cdot 1 + 2 \cdot 1) \equiv 3 + 2 \equiv 1$ となり $(*)$ の左辺は 1 である．これは矛盾．n が奇数の場合 $(*)$ の右辺は 3 である．d が偶数なら $(*)$ の左辺は 0 で矛盾．d が奇数の場合も先と同じくして $(*)$ の左辺は 1 となり矛盾〕． $\dashv$

いま，$pu^2 + 2v^2 > 0$ ゆえ $pu^2 + 2v^2 \in \mathbb{Q} \setminus \{0\}$ である．クレイム 3 と補題 11 により，所望の $(\exists x, y, z \in \mathbb{Q})[pu^2 + 2v^2 = x^2 + y^2 - pz^2]$ を得る． $\square$

ようやく最後の主定理にたどり着いた．

定理 13 (Lemma 4 in [3]，再掲)**.** p を $p \equiv 1 \pmod 4$ なる素数，$q \neq p$ を奇素数であって $(q/p) = -1$ を満たすものとする．t を有理数とし，$t = u/v$ と既約分数として表示する $(u, v \in \mathbb{Z},\ v \neq 0)$．このとき以下は同値である：

(A) $(\exists x, y, z \in \mathbb{Q})[pqt^2 + 2 = x^2 + qy^2 - pz^2]$;
(B) $p \nmid v \ \ \&\ \ q \nmid v$.

証明. 定理の仮定のように p, q, t, u, v をとって固定する．まず，斉次性が効いて次が成り立つ：

クレイム 1. (A) は次に掲げる (A)' と同値である：

$$\text{(A)':}\quad (\exists x, y, z \in \mathbb{Q})[pqu^2 + 2v^2 = x^2 + qy^2 - pz^2]. \tag{45}$$

$\vdash$ (A)$\Rightarrow$(A)' $pqt^2 + 2 = x_0^2 + qy_0^2 - pz_0^2$，すなわち $pqu^2/v^2 + 2 = x_0^2 + qy_0^2 - pz_0^2$ なる $x_0, y_0, z_0 \in \mathbb{Q}$ がとれたとする．両辺に v^2 を乗じて $pqu^2 + 2v^2 = (vx_0)^2 + q(vy_0)^2 - p(vz_0)^2$ を得る．よって

$(x,y,z)=(vx_0,vy_0,vz_0)\in\mathbb{Q}^3$ を証拠に (A)' が成立する． (A)'⇒(A) $pqu^2+2v^2=x_1^2+qy_1^2-pz_1^2$ なる $x_1,y_1,z_1\in\mathbb{Q}$ がとれたとする．$v\neq 0$ に注意して両辺を v^2 で除し，$pq(u/v)^2+2=(x_1/v)^2+q(y_1/v)^2-p(z_1/v)^2$ を得る（念のため：平方剰余記号でなくただの分数）．$u/v=t$ だったから，結局 $(x,y,z)=(x_1/v,y_1/v,z_1/v)\in\mathbb{Q}^3$ を証拠に (A)' が成立する． ⊣

したがって，定理を示すには (A)' $\Longleftrightarrow$ (B) を示せばよい．

(B) $\Longrightarrow$ (A)' $p\nmid v$ かつ $q\nmid v$ であることを仮定する．仮に $p\mid(pqu^2+2v^2)$ ならば $p\mid 2v^2$ となり，$p\neq 2$ だったから $p\mid v$ となる．これは $p\nmid v$ に反する．したがって $p\nmid(pqu^2+2v^2)$ である．また仮に $q\mid(pqu^2+2v^2)$ ならば $q\mid 2v^2$ となり，q は奇数だったから $q\mid v$ となる．これは $q\nmid v$ に反する．したがって $q\nmid(pqu^2+2v^2)$ である．

クレイム 2. 次の否定が成り立つ：

$$(\exists k\in\mathbb{Z})(\exists s\in\mathbb{Q})[pqu^2+2v^2=pks^2\ \&\ p\nmid k\ \&\ (k/p)=-1]\ \text{or}$$
$$(\exists k\in\mathbb{Z})(\exists s\in\mathbb{Q})[pqu^2+2v^2=qks^2\ \&\ q\nmid k\ \&\ (k/q)=-1].$$

⊢ 上式か下式のいずれかが成り立つとして矛盾を導く．上式が成立したとする．そのような $k\in\mathbb{Z}$ および $s\in\mathbb{Q}$ をとり，$s=n/d$ $(n,d\in\mathbb{Z},\ d\neq 0)$ と既約分数として表示する．すると $d^2(pqu^2+2v^2)=pkn^2$ となり，$p\mid d^2(pqu^2+2v^2)$ である．いま $p\nmid(pqu^2+2v^2)$ であったから $p\mid d^2$ である．よって $p\mid d$ である．よって $d=pe$ $(e\in\mathbb{Z})$ と書ける．すると $p^2e^2(pqu^2+2v^2)=pkn^2$ ゆえ $pe^2(pqu^2+2v^2)=kn^2$ となり，$p\mid kn^2$ である．いま $p\nmid k$ であったから $p\mid n^2$ となり，$p\mid n$ である．結局 d と n は p を共通素因数として持つが，これは $s=n/d$ の既約性に反する．
下式が成立したとする．この場合も $q\nmid(pqu^2+2v^2)$ を用いて全く同様に矛盾が導かれる． ⊣

いま，$pqu^2+2v^2>0$ ゆえ $pqu^2+2v^2\in\mathbb{Q}\setminus\{0\}$ である．これに注意してクレイム 2 に対して補題 11 を用いることで，所望の $(\exists x,y,z\in\mathbb{Q})[pqu^2+2v^2=x^2+qy^2-pz^2]$ を得る．

(A)' $\Longrightarrow$ (B) 対偶を示す．$p\mid v$ または $q\mid v$ であることを仮定する．

$p\mid v$ の場合．$v=pa$ $(a\in\mathbb{Z})$ と書ける．よって $pqu^2+2v^2=p(qu^2+2pa^2)$ である．$t=u/v$ の既約性より $p\nmid u$ である．また $p\neq q$ なので $p\nmid qu^2$ である．よって $p\nmid(qu^2+2pa^2)$ である．また $(qu^2+2pa^2/p)=(qu^2/p)=(q/p)(u/p)(u/p)=-1\cdot(\pm1)^2=-1$ である．以上より

$$0\neq pqu^2+2v^2=p(qu+2pa^2)\cdot 1^2,\qquad \left(\frac{qu+2pa^2}{p}\right)=-1 \tag{46}$$

が成り立つ．補題 11 より所望の ¬(A)' を得る．

$q\mid v$ の場合．$v=qb$ $(b\in\mathbb{Z})$ と書ける．よって $pqu^2+2v^2=q(pu^2+2qb^2)$ である．$t=u/v$ の既約性より $q\nmid u$ である．また $p\neq q$ で q は奇素数なので $q\nmid 2pu^2$ である．よって $q\nmid(pu^2+2qb^2)$ である．また $(pu^2+2qb^2/q)=(pu^2/q)=(p/q)(u/q)(u/q)=(p/q)\cdot(\pm1)^2=(p/q)=(q/p)\cdot(-1)^{\varepsilon(p)\varepsilon(q)}=-(-1)^{0\cdot\varepsilon(q)}=-1$ である (cf. [4] Chap. 1 §3 Thm. 6, also [6] 定理 1.11.10 (3) 平方剰余の相互法則).

$(pu^2/q) = (p/q)(u/q)(u/q) = (p/q)\cdot(\pm 1)^2 = (p/q)$ である．以上より

$$0 \neq pqu^2 + 2v^2 = q(pu + 2qb^2)\cdot 1^2, \qquad \left(\frac{pu + 2qb^2}{q}\right) = -1 \tag{47}$$

が成り立つ．補題 11 より所望の ¬(A)’ を得る． □

参考文献

[1] Flath, D. and Wagon, S., *How to pick out the integers in the rationals: An application of number theory to logic*, American Mathematical Monthly, **98** (9), 812–823, 1991.

[2] Fraïssé, R., Course of Mathematical Logic, vol. 2, Model Theory, Springer, 1974.

[3] Robinson, J., *Definability and decision problems in arithmetic*, Journal of Symbolic Logic, **14** (2), 98–114, 1949.

[4] Serre, J.-P., A Course in Arithmetic, Springer, 1973.

[5] ボレビッチ・シャハレビッチ（佐々木義雄訳），整数論（上），吉岡書店，1971.

[6] 雪江明彦，整数論１：初等整数論から p 進数へ，日本評論社，2013.

[7] **TODO:** 文献追加