§2. The proof of Theorem 1.7

The proof of Theorem 1.7 is given in the next section. Although we need Theorem 1.7 only when $p \equiv 3 \bmod 4$ we give a complete proof since very little additional work is required.

§ 2. The proof of Theorem 1.7

In this section p denotes an odd prime number. We begin by recalling a result about sequences of quadratic residues and nonresidues mod p.

2.1. Lemma. *The number of pairs* $(n, n+1)$ *in the set* $\{1, 2, ..., p-1\}$ *such that* $\left(\frac{n}{p}\right) = 1, \left(\frac{n+1}{p}\right) = -1$ *is equal to* $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$.

Proof. This elementary result is proved completely in [Ha], p. 157-158. (See also [An], Chapter 10.)

The next two lemmas give a way to count the number of lattice points $(x, y) \in \mathbf{Z} \times \mathbf{Z}$, $x, y > 0$, satisfying the conditions of Theorem 1.7.

Let

$$\mathscr{S}(x) = \{(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z} \mid \alpha, \beta > 0, \alpha^2 + \beta^2 < x^2\}$$

and let $\mathscr{P}(x) = \{(\alpha, \beta) \in \mathscr{S}(x) \mid (\alpha, \beta) = 1\}$. Let $S(x) = |\mathscr{S}(x)|$ and $P(x) = |\mathscr{P}(x)|$. (It will be clear from context whether we mean the point (α, β) or the greatest common divisor of α, β.)

2.2. Lemma. *Let* R *be the set of nonzero squares* mod p.

(a) *The function* $\theta : \mathscr{P}(\sqrt{p}) \to R$ *given by* $\theta(x, y) = \dfrac{y^2}{x^2} \bmod p$ *is an injection.*

(b) $P(\sqrt{p}) \leqslant \frac{1}{2}(p-1)$.

Proof. Clearly (a) implies (b) since $|R| = \frac{1}{2}(p-1)$. If (a) is false then there exist two distinct points $(x_1, y_1), (x_2, y_2)$ in $\mathscr{P}(\sqrt{p})$ such that $\dfrac{y_1^2}{x_1^2} \equiv \dfrac{y_2^2}{x_2^2} \bmod p$. Then $y_1^2 x_2^2 - x_1^2 y_2^2 = (y_1 x_2 + x_1 y_2)(y_1 x_2 - x_1 y_2) \equiv 0 \bmod p$. We have $y_1 x_2 + x_1 y_2 \neq 0$ since $x_i, y_i > 0$ and $y_1 x_2 - x_1 y_2 \neq 0$ otherwise $\dfrac{y_1}{x_1} = \dfrac{y_2}{x_2}$ and

then the points $(x_1, y_1), (x_2, y_2)$ would be equal since $(x_i, y_i) = 1$, $i = 1, 2$. We have

$$\begin{aligned}(x_1^2+y_1^2)(x_2^2+y_2^2) &= (x_1x_2+y_1y_2)^2 + (y_1x_2-x_1y_2)^2 \\ &= (x_1x_2-y_1y_2)^2 + (y_1x_2+x_1y_2)^2 .\end{aligned}$$

Either $(y_1x_2-x_1y_2)^2$ or $(y_1x_2+x_1y_2)^2$ is $\geqslant p^2$ since both are nonzero and one of them is divisible by p^2. Therefore $(x_1^2+y_1^2)(x_2^2+y_2^2) \geqslant p^2$ and then either $x_1^2 + y_1^2 \geqslant p$ or $x_2^2 + y_2^2 \geqslant p$. This is a contradiction since both (x_1, y_1) and (x_2, y_2) lie in $\mathscr{P}(\sqrt{p})$.

Remark. Although (b) in the preceeding lemma is not needed in what follows it was included since it gives a fairly good upper bound for $P(\sqrt{p})$ that is valid for all primes. It can be shown using Lemmas 2.4, 2.5 below (see also [HW], p. 268) that $\lim_{p\to\infty} \frac{P(\sqrt{p})}{p} = \frac{3}{2\pi} \approx .477$. It is unusual to obtain, with so little work, such a good estimate that is valid for all prime numbers.

2.3. LEMMA. *Assume* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. *Let* $\tau: R \to \{0, 1, -1\}$ *where* $\tau(z^2) = \left(\frac{a+bz^2}{p}\right)$. *Then* $\left|\tau^{-1}(-1)\right| = \dfrac{p - \left(\frac{-1}{p}\right)}{4}$.

Proof. Since $\left(\frac{a}{p}\right) = 1$, we have $\tau(z^2) = -1 \Leftrightarrow \left(\frac{1+\frac{b}{a}z^2}{p}\right) = -1$. Since $\left(\frac{b/a}{p}\right) = 1$, by Lemma 2.1 this happens if and only if $\frac{b}{a}z^2$ is one of the $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$ elements β in R such that $\left(\frac{\beta}{p}\right) = 1, \left(\frac{\beta+1}{p}\right) = -1$. Therefore, there are exactly $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$ elements z^2 in R such that $\tau(z^2) = -1$.

Since $\left(\frac{a + b\frac{y^2}{x^2}}{p}\right) = -1 \Leftrightarrow \left(\frac{ax^2+by^2}{p}\right) = -1$ when $p \nmid x$, it follows from Lemmas 2.2, 2.3 that proving Theorem 1.7 is equivalent to finding (x, y)

$\in \mathscr{P}(\sqrt{p})$ such that $\tau \circ \theta(x, y) = -1$. This is equivalent to showing $\theta(\mathscr{P}(\sqrt{p}))$ $\cap \tau^{-1}(-1)$ is nonempty. Since θ is injective, $|\tau^{-1}(-1)| = \dfrac{p - \left(\dfrac{-1}{p}\right)}{4}$, and $|R| = \dfrac{p-1}{2}$, it is sufficient to show $P(\sqrt{p}) + \dfrac{p - \left(\dfrac{-1}{p}\right)}{4} > \dfrac{p-1}{2}$. Thus to prove Theorem 1.7, we are reduced to showing

$$P(\sqrt{p}) > \frac{p-1}{2} - \frac{p - \left(\frac{-1}{p}\right)}{4} = \begin{cases} \dfrac{p-3}{4} & \text{if } p \equiv 3 \bmod 4 \\ \dfrac{p-1}{4} & \text{if } p \equiv 1 \bmod 4 . \end{cases}$$

As pointed out earlier, $\lim\limits_{p \to \infty} \dfrac{P(\sqrt{p})}{p} \approx .477$. Thus it is clear that for all but finitely many primes p we have $\dfrac{P(\sqrt{p})}{p} > \dfrac{1}{4}$, i.e., $P(\sqrt{p}) > \dfrac{p-1}{4}$. Since we need to check this result for all primes p, $p \neq 5$, it is necessary to give rather careful estimates. We now compute $P(x)$ and compare it to $\dfrac{x^2-1}{4}$.

Let μ be the Möbius function: If $n \in \mathbf{Z}$, $n = \prod\limits_{i=1}^{t} p_i^{e_i}$, then

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^t & \text{if each } e_i = 1 \\ 0 & \text{if some } e_i > 1 . \end{cases}$$

Let [ ] denote the greatest integer function.

2.4. LEMMA. $P(x) = \sum\limits_{i=1}^{\infty} \mu(i)\, S\left(\dfrac{x}{i}\right) = \sum\limits_{i=1}^{\left[\frac{x}{\sqrt{2}}\right]} \mu(i)\, S\left(\dfrac{x}{i}\right)$.

Proof. Since $S(\sqrt{2}) = 0$, we have $S\left(\dfrac{x}{i}\right) = 0$ if $i \geqslant \left[\dfrac{x}{\sqrt{2}}\right] + 1$. In order to count how many times each lattice point is counted in the sum $\sum\limits_{i=1}^{\infty} \mu(i)\, S\left(\dfrac{x}{i}\right)$ we partition the lattice points in $\mathscr{S}(x)$ into the rays passing through the origin. Let $(\alpha, \beta) \in \mathscr{P}(x)$ and consider all multiples $(m\alpha, m\beta)$

that lie in $\mathscr{S}(x)$. Let n be the unique positive integer such that $(n\alpha, n\beta) \in \mathscr{S}(x)$ but $((n+1)\alpha, (n+1)\beta) \notin \mathscr{S}(x)$. Then for a given positive integer i, we have $(j\alpha, j\beta) \in \mathscr{S}\left(\frac{x}{i}\right)$ precisely for $\left[\frac{n}{i}\right]$ values of j since if $\left(\left[\frac{n}{i}\right]+1\right)(\alpha, \beta) \in \mathscr{S}\left(\frac{x}{i}\right)$ then $i\left(\left[\frac{n}{i}\right]+1\right)(\alpha, \beta) \in \mathscr{S}(x)$. But $i\left(\left[\frac{n}{i}\right]+1\right) \geqslant n+1$. Therefore exactly $\left[\frac{n}{i}\right]$ points on the ray through (α, β) lie in $\mathscr{S}\left(\frac{x}{i}\right)$. It follows that in the sum to be evaluated, the points on the ray through (α, β) contribute $\sum_{i=1}^{\infty} \mu(i)\left[\frac{n}{i}\right] = 1$. To prove this last equality we start with the well known fact $\sum_{i|m} \mu(i) = \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if } m > 1. \end{cases}$ Then $1 = \sum_{m=1}^{n} \sum_{i|m} \mu(i) = \sum_{i=1}^{n} \mu(i)\left[\frac{n}{i}\right]$ since $\left[\frac{n}{i}\right]$ is the number of multiples of i that are $\leqslant n$. Therefore the sum to be evaluated counts the number of points in $\mathscr{P}(x)$ and this completes the proof.

2.5. LEMMA. *For all* $x \geqslant 1, \frac{\pi}{4}x^2 - 2x + 1 < S(x) < \frac{\pi}{4}x^2$.

Proof. To each point $(\alpha, \beta) \in \mathscr{S}(x)$ associate the lattice square for which (α, β) is the lower left corner. Let M_1 denote the region covered by these squares. Then $S(x) =$ area of M_1. Let M_2, M_3 be the two strips of length x, width 1, parallel to the axes where $M_2 = \{(x_1, y_1) \mid 0 \leqslant x_1 \leqslant x, 0 \leqslant y_1 \leqslant 1\}$, and $M_3 = \{(x_1, y_1) \mid 0 \leqslant x_1 \leqslant 1, 0 \leqslant y_1 \leqslant x\}$. When $x \geqslant 1$, these strips cover a combined area of $2x - 1$. Since the quarter circle of radius x is contained in $M_1 \cup M_2 \cup M_3$, it follows $\frac{\pi}{4}x^2 < S(x) + 2x - 1$.

Now to each point (α, β) in $\mathscr{S}(x)$ associate the lattice square for which (α, β) is the upper right corner. These lattice squares lie entirely in the first quadrant and inside the circle of radius x. Therefore $S(x) < \frac{\pi}{4}x^2$.

2.6. LEMMA. *Let* $m > n \geqslant 1, m, n \in \mathbf{Z}$. *Then*

$$\frac{1}{(n+1)^2} + \frac{1}{(n+2)^2} + \ldots + \frac{1}{m^2} < \frac{1}{n} - \frac{1}{m}.$$

Proof. Apply the integral test to $\int_n^m \frac{1}{t^2}\,dt$ or observe

$$\sum_{i=n}^{m-1} \frac{1}{(i+1)^2} < \sum_{i=n}^{m-1} \left(\frac{1}{i} - \frac{1}{i+1}\right) = \frac{1}{n} - \frac{1}{m}.$$

We now use Lemmas 2.4, 2.5 to estimate $P(x)$. We need to determine values of x for which $P(x) > \dfrac{x^2-1}{4}$. First assume $x > 10$. Then $\dfrac{x}{\sqrt{2}} > 7$ so $\left[\dfrac{x}{\sqrt{2}}\right] \geqslant 7$.

$$P(x) = \sum_{i=1}^{\infty} \mu(i)\, S\left(\frac{x}{i}\right) = \sum_{i=1}^{\left[\frac{x}{\sqrt{2}}\right]} \mu(i)\, S\left(\frac{x}{i}\right)$$

$$\geqslant S(x) - S\left(\frac{x}{2}\right) - S\left(\frac{x}{3}\right) - S\left(\frac{x}{5}\right) + S\left(\frac{x}{6}\right) - \sum_{i=7}^{\left[\frac{x}{\sqrt{2}}\right]} S\left(\frac{x}{i}\right)$$

$$> \left(\frac{\pi}{4}x^2 - 2x + 1\right) - \frac{\pi}{4}\left(\frac{x}{2}\right)^2 - \frac{\pi}{4}\left(\frac{x}{3}\right)^2 - \frac{\pi}{4}\left(\frac{x}{5}\right)^2$$

$$+ \left(\frac{\pi}{4}\left(\frac{x}{6}\right)^2 - 2\left(\frac{x}{6}\right) + 1\right) - \frac{\pi}{4}x^2\left(\frac{1}{7^2} + \ldots + \frac{1}{\left[\frac{x}{\sqrt{2}}\right]^2}\right)$$

$$> \frac{\pi}{4}x^2\left(1 - \frac{1}{4} - \frac{1}{9} - \frac{1}{25} + \frac{1}{36} - \frac{1}{6} + \frac{1}{\left[\frac{x}{\sqrt{2}}\right]}\right) - 2x\left(1 + \frac{1}{6}\right) + 2 \text{ (by Lemma 2.6)}$$

$$= \frac{\pi}{4}x^2\left(\frac{46}{100}\right) + \frac{\pi}{4}x^2\left(\frac{1}{\left[\frac{x}{\sqrt{2}}\right]}\right) - \frac{7}{3}x + 2$$

$$\geqslant \frac{23\pi}{200}x^2 + \left(\frac{\sqrt{2}\pi}{4} - \frac{7}{3}\right)x + 2, \text{ since } \frac{x^2}{\left[\frac{x}{\sqrt{2}}\right]} \geqslant \sqrt{2}x\,.$$

Let $f(x) = \dfrac{23\pi}{200}x^2 + \left(\dfrac{\sqrt{2}\pi}{4} - \dfrac{7}{3}\right)x + 2$, $g(x) = \dfrac{x^2-1}{4}$. One can check that $f(10) > g(10)$, $f'(10) > g'(10)$, $f''(10) > g''(10)$. Therefore $P(x) > f(x) > g(x)$ for all $x > 10$. This implies $P(\sqrt{p}) > \dfrac{p-1}{4}$ if $\sqrt{p} > 10$, i.e., $p > 100$. It remains to show $P(\sqrt{p}) > \dfrac{p-1}{4}$ if $p < 100$, $p \neq 5$.

At this point we simply count lattice points directly and construct the table below. The table shows $P(\sqrt{p}) > \frac{p-1}{4}$ for all primes $p < 100$ except $p = 5$. This completes the proof of Theorem 1.7 and hence the Main Theorem has been proved completely.

p	$P(\sqrt{p})$	Range of primes where $P(\sqrt{p}) > \frac{p-1}{4}$
59	27	$59 \leqslant p \leqslant 97$
31	15	$31 \leqslant p \leqslant 53$
19	9	$19 \leqslant p \leqslant 29$
11	5	$11 \leqslant p \leqslant 17$
7	3	$p = 7$
3	1	$p = 3$
5	1	$1 \not> \frac{5-1}{4}$

§ 3. Consequences of the Main Theorem

In this section we derive some consequences of the Main Theorem that have applications to the algebraic theory of quadratic forms. The results in this section are well known ([La], Chapter 6). The point is that we have new and more elementary proofs.

Let $\langle\langle a, b, c\rangle\rangle$ denote the 3-fold Pfister form

$$\langle 1, a\rangle \otimes \langle 1, b\rangle \otimes \langle 1, c\rangle = \langle 1, a, b, c, ab, ac, bc, abc\rangle .$$

3.1. Proposition. *Let* $a, b, c \in \mathbf{Q}^{\times}$. *Then* $\langle\langle a, b, c\rangle\rangle$ *is hyperbolic over* $\mathbf{Q}$ *if and only if* a, b, c *are not all positive.*

Proof. If $\langle\langle a, b, c\rangle\rangle$ is hyperbolic, then consideration of $\langle\langle a, b, c\rangle\rangle$ over the field of real numbers shows at least one of a, b, c is negative.

Now suppose $a < 0$. Then the Main Theorem implies $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ and $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$ by Lemma 1.2(b). A theorem of Pfister ([La], p. 279] implies $\langle\langle a, b, c\rangle\rangle$ is hyperbolic over $\mathbf{Q}$.