Chapter 5

Classification of quaternion algebras

Due to time constraints, this chapter contains less than what I hoped. For instance, some proofs are omitted, and some are just done over $\mathbb{Q}$. Still, I think the arguments over $\mathbb{Q}$ are nice, where one go though things a bit more explicitly, and use tricks to simplify things that don't quite work in the general case. I may add more to this in the future, but as far as expanding these notes go (which I am slowly doing though the course is over), my priorities now are toward later chapters.

5.1 Quaternion algebras over local fields

Here we classify quaternion algebras over F where F is a local field of characteristic 0, i.e., F is a p-adic field or $\mathbb{R}$ or $\mathbb{C}$. The case where F is archimedean was already done in Section 2.6, so it suffices to work out the classification when F is p-adic. For F p-adic, let ϖ_F denote a uniformizer of F. This will be a special case of Theorem 2.7.3.

Here is the general statement.

Theorem 5.1.1. *Let F be a local field of characteristic 0. If $F = \mathbb{C}$, then the only quaternion algebra over F (up to isomorphism) is $M_2(\mathbb{C})$. Put $B = \mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ if $F = \mathbb{R}$ and $B = \left(\frac{u,\varpi_F}{F}\right)$ if F is p-adic where $u \in \mathcal{O}_F^\times$ is a nonsquare. If $F \neq \mathbb{C}$, then, up to isomorphism, there are exactly two quaternion algebras over F: $M_2(F)$ and the unique quaternion division algebra B.*

Implicit in the statement in the p-adic case is that B does not depend upon the choice of u or the uniformizer ϖ_F.

Lemma 5.1.2. *Let F be a p-adic field, and B/F a quaternion algebra. Then B contains the unique unramified quadratic extension K/F.*

Proof. This is a special case of Corollary 4.3.5, which we did not prove. Either $B \simeq M_2(F)$ or B is division. If $B \simeq M_2(F)$, then the result is true by Proposition 2.4.1. So assume B is division.

For simplicity, we will just complete the proof when $F = \mathbb{Q}_p$ with p odd. In this case, there are 3 nontrivial square classes represented by u, p, and up, where $u \in \mathbb{Z}_p^\times$ is not a square (cf. Proposition 1.2.12). Recall $\mathbb{Q}_p(\sqrt{u})$ is the unique quadratic unramified extension of $\mathbb{Q}_p$.

We may thus assume $B = \left(\frac{a,b}{\mathbb{Q}_p}\right)$ where $a, b \in \{u, p, up\}$. It suffices to show we can take $a = u$. If not, then we may assume $a, b \in \{p, up\}$, so $B = \left(\frac{pu_1, pu_2}{\mathbb{Q}_p}\right)$ where $u_1, u_2 \in \{1, u\}$. But since $\left(\frac{a,b}{F}\right) \simeq \left(\frac{-ab,b}{F}\right)$ (cf. Corollary 3.3.3), we have $B = \left(\frac{-p^2u_1u_2, pu_2}{F}\right) = \left(\frac{-u_1u_2, pu_2}{F}\right)$. Since B is not split, it must be that $-u_1u_2$ is in the same square class as u, so indeed we can take $a = u$. □

Exercise 5.1.1. Prove the above lemma when $F = \mathbb{Q}_2$.

This takes care of the lemma when F is a "prime" p-adic field, i.e., F is some $\mathbb{Q}_p$. We omit the proof in the case F is an extension of some $\mathbb{Q}_p$.

Proof of theorem. It suffices to show that there is a unique quaternion division algebra in the p-adic case, and that it is given in the above form.

Again, for simplicity, we will just complete the proof when $F = \mathbb{Q}_p$ with p odd. Then, from the proof of the lemma we know any quaternion division algebra over $\mathbb{Q}_p$ is of the form $B = \left(\frac{u,b}{\mathbb{Q}_p}\right)$, where $b \in \{u, p, up\}$. Note $B = \left(\frac{u,u}{\mathbb{Q}_p}\right)$ is split by Proposition 3.3.7 since the norm map $\mathbb{Q}_p(\sqrt{u})^\times \to \mathbb{Q}_p^\times$ is surjective on integral units (Corollary 1.2.15).

Thus either $B = \left(\frac{u,p}{\mathbb{Q}_p}\right)$ or $B = \left(\frac{u,up}{\mathbb{Q}_p}\right)$. It suffices to show that these are isomorphic. From the fact that $\left(\frac{a,b}{F}\right) = \left(\frac{a,-ab}{F}\right)$ (Corollary 3.3.3), they are isomorphic if -1 is a square in $\mathbb{Q}_p$, i.e., if $p \equiv 1 \bmod 4$.

Assume that -1 is not a square in $\mathbb{Q}_p$, in which case we may take $u = -1$. Then we want to show the associated restricted norm forms $x^2 - py^2 - pz^2$ and $x^2 + py^2 + pz^2$ are equivalent. There exist $r, s \in \mathbb{Q}_p$ such that $r^2 + s^2 = -1$. (This follows, for instance, from Corollary 1.2.15 or knowing that $\left(\frac{-1,-1}{\mathbb{Q}_p}\right)$ is split and using Proposition 3.3.7.) Then the change of variables $y \mapsto ry + sz$, $z \mapsto sy - rz$ transforms $x^2 - py^2 - pz^2$ to $x^2 + py^2 + pz^2$, as desired. □

Exercise 5.1.2. Prove the above theorem when $F = \mathbb{Q}_2$.

Note that in the above proof, we showed that $\left(\frac{-1,-1}{\mathbb{Q}_p}\right)$ is split for p odd. In fact, we can say precisely when $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is split now.

Exercise 5.1.3. Suppose p is an odd rational prime and $a, b \in \mathbb{Z}$ are nonzero and squarefree. Assume $v_p(a) \le v_p(b)$. Show $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is division (i.e., ramified) if and only if

(1) $p \nmid a$, $p|b$, and a is a nonsquare mod p; or

(2) $p|a$, $p|b$ and $-a^{-1}b$ is a nonsquare mod p.

Exercise 5.1.4. Let $F = \mathbb{Q}_p$, p odd. Show any quadratic field extension K/F embeds in the quaternion division algebra B/F.

5.2 Quaternion algebras over number fields

In this section, let F be a number field and B denote a quaternion algebra over F.

Recall that B is *split* at a place v of F if B_v is split, i.e., isomorphic to $M_2(F_v)$; otherwise we say B *ramifies* at v, or just B_v is ramified. For quaternion algebras B, B being ramified at v is equivalent to B_v being a division algebra. Note that B can only ramify at non-complex places. Let

$$\mathrm{Ram}(B) = \{v : B_v \text{ is ramified}\}.$$

Proposition 5.2.1. *The ramification set* $\mathrm{Ram}(B)$ *of a quaternion algebra B over a number field F is finite. Furthermore,* $\mathrm{Ram}(B)$ *determines B up to isomorphism.*

Proof. Write $B = \left(\frac{a,b}{F}\right)$ for some $a, b \in F^\times$. We may assume in fact that $a, b \in \mathcal{O}_F$. (We may also assume that a, b are squarefree, though we do not need to for the proof.) Let S be the set primes of F which divide a or b union with the set of all even primes. Then for any finite $v \notin S$, we claim B_v is split.

For simplicity, we just show this when $F_v = \mathbb{Q}_p$, p odd. Indeed, we have $B_v = \left(\frac{a,b}{\mathbb{Q}_p}\right)$ where $a, b \in \mathbb{Z}_p^\times$. If a or b are squares, B_v is split, so assume they are not. Then, because v is odd, there are only two square classes in $\mathbb{Z}_p^\times$ and $K_v = \mathbb{Q}_p(\sqrt{a})$ is the unramified quadratic extension. Then, as in the proof of Theorem 5.1.1, $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ must be split because b is a norm from K_v.

For the last part, suppose B' is another quaternion algebra such that $\mathrm{Ram}(B') = \mathrm{Ram}(B)$. By the local classification Theorem 5.1.1, this implies $B_v \simeq B'_v$ for all v. Then the local-global principle Theorem 3.4.2 implies $B \simeq B'$. □

This is analogous to the fact that the ramification sets of quadratic fields $\mathbb{Q}(\sqrt{d})$ are finite and determine the field up to isomorphism.

For the next result about $\mathrm{Ram}(B)$, we need an important result from algebraic number theory.

Theorem 5.2.2 (Quadratic Hilbert Reciprocity)**.** *Let $a, b \in F^\times$. Then the product of local quadratic Hilbert symbols is* $\prod_v (a,b)_{F_v} = 1$.

Proof. See, e.g., [Neu99, Thm VI.8.1]. (This reference is a more general version than what we need, covering n-th power Hilbert symbols. Also, Neukirch's definition of the Hilbert symbol is a little different from ours, but can be seen to be equivalent from his Proposition V.3.2 or Exercise V.3.1.) □

The Hilbert reciprocity law is a generalization of Gauss's classical quadratic reciprocity. Specifically, quadratic Hilbert reciprocity can be viewed as a version of quadratic reciprocity over arbitrary number fields.[1]

[1] General Hilbert reciprocity is a law for n-th power residue symbols, but only over number fields which contain all n-th roots of unity. This generalizes other classical reciprocity laws, such as Eisenstein's cubic reciprocity over $\mathbb{Z}[\zeta_3]$. Hilbert reciprocity was further generalized by Artin through the development of class field theory.

> **Exercise 5.2.1.** Deduce the classical statement of quadratic reciprocity from Hilbert reciprocity, namely: if p, q are odd (positive) rational primes, deduce
>
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$
>
> (Cf. Exercise 3.3.8 and Exercise 3.3.9.).

Corollary 5.2.3. *For a quaternion algebra B over a number field, the cardinality of* $\mathrm{Ram}(B)$ *is finite and even and contains no complex places.*

Proof. Recall $v \in \mathrm{Ram}(B)$ if and only if $(a,b)_{F_v} = -1$ from Corollary 3.3.8. Now apply Hilbert's reciprocity law and Proposition 5.2.1. □

We now have enough results to determine if two rational quaternion algebras (i.e., quaternion algebras over $\mathbb{Q}$) are isomorphic. Consider $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ and $B' = \left(\frac{a',b'}{\mathbb{Q}}\right)$. We may modify a, b, a', b' by squares to assume that $a, b, a', b' \in \mathbb{Z}$ and are all squarefree.

To determine if $B \simeq B'$ it suffices to determine their ramification sets.

First, recall $\infty \in \mathrm{Ram}(B)$ if and only if B is definite by Sylvester's law of inertia, which happens if and only if $a, b < 0$.

Next, for an odd prime p, a computationally simple criterion for $p \in \mathrm{Ram}(B)$ was given in Exercise 5.1.3: $p \in \mathrm{Ram}(B)$ if and only if (i) p divides exactly one of a, b and the other is a nonsquare mod p or (ii) p divides both and $-a^{-1}b$ is a nonsquare mod p. As a special case, we get the following criterion can be useful as a first pass to determine the ramification set of B.

> **Example 5.2.1.** Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ where $a, b \in \mathbb{Z}$ squarefree. Then the set of odd primes in $\mathrm{Ram}(B)$ is contained in the set of primes dividing ab. (Note: this gives a simpler proof of the first part of Proposition 5.2.1 when $F = \mathbb{Q}$.)

Last, to determine whether $2 \in \mathrm{Ram}(B)$, the corollary implies we don't need to do anything else! We just count the number of odd and infinite places at which B ramifies—then B also ramifies at 2 if and only if this number is odd. So for checking isomorphism, we don't even need to worry about the place 2. (Note this trick does not work for general number fields.)

Hence $B \simeq B'$ if and only if

(1) both $a, b < 0$ if and only if both $a', b' < 0$; and

(2) the finite odd primes ramified in B are precisely the finite odd primes ramified in B' (use Exercise 5.1.3).

In special cases, we can write down relatively simple necessary and sufficient isomorphism criteria.

> **Example 5.2.2.** Let $B = \left(\frac{-1,b}{\mathbb{Q}}\right)$ and $B' = \left(\frac{-1,b'}{\mathbb{Q}}\right)$ where $b, b' \in \mathbb{Z}$ squarefree. Then $B \simeq B'$ if and only if b and b' have the same sign and are divisible by the same set of primes which are 3 mod 4.

> To see this, first note that checking they have the same ramification at infinity implies means b, b' must have the same sign. Then, for an odd prime $p|b$, $p \in \mathrm{Ram}(B)$ if and only if -1 is a nonsquare mod p, i.e., if and only if $p \equiv 3 \bmod 4$.

> **Exercise 5.2.2.** Let $B = \left(\frac{3,b}{\mathbb{Q}}\right)$ and $B' = \left(\frac{3,b'}{\mathbb{Q}}\right)$ where $b, b' \in \mathbb{Z}$ squarefree. Determine necessary and sufficient conditions on b, b' for $B \simeq B'$.

> **Exercise 5.2.3.** Determine the ramification sets of the following rational quaternion algebras: $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, $\left(\frac{-1,2}{\mathbb{Q}}\right)$, $\left(\frac{2,3}{\mathbb{Q}}\right)$, $\left(\frac{-3,-5}{\mathbb{Q}}\right)$ and $\left(\frac{-3,-6}{\mathbb{Q}}\right)$.

Now we know that any quaternion algebra over a number field F is determined (up to isomorphism) by its ramification set S, which must be a finite set of even cardinality containing only non-complex places. At least when $F = \mathbb{Q}$, we also saw how to determine S from the Hilbert symbol representations. The following result completes the classification of quaternion algebras over number fields by saying to all such sets S, there is a quaternion algebra with S as its ramification set.

Theorem 5.2.4. *Let F be a number field. Given any finite set S of non-complex places of F of even cardinality, there exists a unique (up to isomorphism) quaternion algebra B/F such that $\mathrm{Ram}(B) = S$. If $S = \emptyset$, then $B \simeq M_2(F)$; otherwise B is a division algebra.*

To prove this, the following intermediary result is useful.

Lemma 5.2.5. *Let F be a number field and S any finite set of non-complex places. There exists a quadratic extension K/F such that K is not split at any $v \in S$.*

Proof. For simplicity, we just show this when $F = \mathbb{Q}$, so S can be any set of places. Let $p_1, \dots, p_r$ denote the finite places in S. Then $K = \mathbb{Q}(\sqrt{\pm p_1 \cdots p_r})$ is ramified, and therefore not split, at each p_i. If $\infty \in S$, choosing the $\pm$ sign to be $-$ means K is also ramified at ∞. □

The above lemma is a special case of an important result of Grunwald–Wang, which implies given any n and finite set of finite places S of F, there exists a cyclic extension K/F of degree n with whatever ramification/splitting type we want for each $v \in S$. (Note we wrote the above proof for $F = \mathbb{Q}$ in a way to make it clear you can specify the ramification type at ∞.) Here is a quadratic example of what we mean by specifying the ramification/splitting type.

> **Exercise 5.2.4.** Show there exists a quadratic field $K/\mathbb{Q}$ which is ramified at $2, 3, \infty$, inert at $5, 7$ and split at $11, 13$. (Cf. Proposition 1.3.10 and the subsequent paragraph.)

Proof of theorem. We may assume S is nonempty. By the lemma, we may take some quadratic extension $K = F(\sqrt{a})$ which is not split at any $v \in S$. Now we want to take

$B = \left(\frac{a,b}{F}\right)$ for a suitable $b \in F^\times$. Specifically, we want to choose b so that locally b is not a norm from K at v if and only if $v \in S$, i.e.,

$$\{v : K_v/F_v \text{ not split and } b \notin N_{K_v/F_v}(K_v^\times)\} = S.$$

Then by Proposition 3.3.7, we will have $\mathrm{Ram}(B) = S$ as desired.

Let T be S union the infinite places of F union all places where K/F is ramified. Recall from Corollary 1.2.15 that for $v < \infty$ if K_v/F_v is unramified then $N_{K_v/F_v}(\mathcal{O}_{K_v}^\times) = \mathcal{O}_{F_v}^\times$. First choose b such that $b \in \mathcal{O}_{F_v}^\times$ for all $v \notin T$ with K_v/F_v nonsplit. This means $\mathrm{Ram}(B) \subset T$.

Next, for a finite $v \in S$, the image of the norm map $N_{K_v/F_v} : \mathcal{O}_{K_v}^\times \to \mathcal{O}_{F_v}^\times$ has index 2 in $\mathcal{O}_{F_v}^\times$. Thus the non-norms in $F_v^\times$ form an open subset $U_v \subset F_v^\times$. We want $b \in U_v$ for all such v. Last, at each infinite place $v \in S$ (thus by assumption real), we want $\sigma_v(b) < 0$, i.e., $b \in U_v = \sigma_v^{-1}(\mathbb{R})$. If we can choose such a b, then $\mathrm{Ram}(B) = S$.

For simplicity, we just demonstrate the existence of a desired b when $F = \mathbb{Q}$ and $\infty \notin S$. The case where $\infty \in S$ is similar and left as an exercise. This follows the argument given for $F = \mathbb{Q}$ given in a preliminary version of [Voi].

Let $\{p_1, \dots, p_r\}$ be the primes of S. Take $a = \prod p_i$ and $K = \mathbb{Q}(\sqrt{a})$. Then K is ramified exactly at the primes in S and also at 2 if $a \not\equiv 1 \bmod 4$. Take $b \in \mathbb{N}$ such that: (i) b is a nonsquare mod each p_i and (ii) $b \equiv 5, 1 \bmod 8$ according to whether $2 \in S$ or not. Then $\mathrm{Ram}(B) \supset S$, and no other primes except possibly those dividing b. (This follow for odd primes by Exercise 5.1.3; see the exercise below for $p = 2$.) However, by Dirichlet's theorem on primes in arithmetic progressions, we can take b to be a prime satisfying the congruences in (i) and (ii). This either $\mathrm{Ram}(B) = S$ or $\mathrm{Ram}(B) = S \cup \{b\}$. But since $|\mathrm{Ram}(B)|$ is even, we must have $\mathrm{Ram}(B) = S$! □

There are two things at the end this proof I find striking: the use of the seemingly unrelated theorem of Dirichlet on arithmetic progressions (so the theorem for $F = \mathbb{Q}$ is a consequence of nonvanishing of Dirichlet L-values!) and the final application of the evenness of $|\mathrm{Ram}(B)|$. Pause, and marvel on this.

Exercise 5.2.5. For $a, b \in \mathbb{Z}$ squarefree, show (i) $\left(\frac{a,b}{\mathbb{Q}_2}\right)$ is division if $2|a$ and $b \equiv 5 \bmod 8$; and (ii) $\left(\frac{a,b}{\mathbb{Q}_2}\right)$ is split if $b \equiv 1 \bmod 8$.

Exercise 5.2.6. Prove the above theorem when $F = \mathbb{Q}$ and $\infty \in S$.

5.3 Subfields of quaternion algebras and sums of rational squares

We will be interested in quadratic subfields of quaternion algebras. There is a nice description.

Theorem 5.3.1. *Let B be a quaternion algebra over number field F and K/F a quadratic extension. The following are equivalent:*

(1) K embeds in B;

(2) *K_v embeds in B_v for all v;*

(3) *K is not split at any (finite or infinite) place where B is ramified; and*

(4) *K splits B.*

Clearly the statement (1) $\iff$ (2) is a local-global principle for embeddings. In light of Theorem 2.4.5, one can also view (2) $\iff$ (4) as a local-global principle for splitting fields.

Proof. (1) $\implies$ (2): Obvious.

(2) $\implies$ (3): Suppose K_v embeds in B_v. If $v \in \mathrm{Ram}(B)$, then B_v is a division algebra, so K_v must also be a division algebra. Thus $K_v \not\simeq F_v \oplus F_v$, as the latter has zero divisors.

(3) $\implies$ (4): By Theorem 2.4.5, (3) implies each K_v splits B_v. Hence $(B \otimes_F K) \otimes_K K_w$ is split for all primes w of K. Thus $B \otimes_F K \simeq M_2(K)$ by Theorem 3.4.2.

(4) $\implies$ (1): See [MR03, Thm 7.3.3]. □

If we want, we can think of this as a different kind of characterization of quaternion algebras.

> **Exercise 5.3.1.** Show that two quaternion algebras B, B' over a number field F are isomorphic if and only if they contain the same subfields.

The analogue of this is not true for local fields as we have seen that the local division algebras contain all quadratic field extensions, though it would be true for quaternion algebras B, B' over p-adic fields (or $\mathbb{R}$) if you ask what semisimple quadratic algebra extensions (i.e., $F \oplus F$ and quadratic field extensions) they contain.

We remark that G. Prasad and A. Rapinchuk asked if two quaternion *division* algebras over a field F must be the same if they contain the same subfields. This is the case for p-adic, archimedean and number fields, but several counterexamples have been found for other fields.

The above theorem gives a clean algebraic description of when a quadratic extension K/F embeds in a quaternion algebra B/F for a number field F. On the other hand, there is an elementary arithmetic criterion for this as well.

Proposition 5.3.2. *Let $d \in F^\times$ be a nonsquare and $K = F(\sqrt{d})$. Let $B = \left(\frac{a,b}{F}\right)$ be a quaternion algebra. Then K embeds in B if and only if $-d$ is represented by the restricted norm form $N_0 : -ax^2 - by^2 + abz^2$. Moreover, the number of embeddings of K into B is the number of solutions to*

$$ax^2 + by^2 - abz^2 = d, \quad x, y, z \in F,$$

i.e., the number of pure quaternions of (reduced) norm $-d$.

This is valid for an arbitrary field F of characteristic not 2, but for infinite fields the number of embeddings is typically 0 or infinite, so the last part of the proposition is not really interesting for number fields. (Recall, by Skolem–Noether the embeddings of K into B are conjugate, and conjugation gives many different embeddings—e.g., (2.3.1).). However, if the norm form is definite, then the number of integral rather than rational solutions (taking $x, y, z \in \mathfrak{o}_F$ rather than F) will be finite. We will look at such a result in the next chapter.

Proof. Suppose we have an embedding ϕ of K into B. Put $\alpha = \phi(\sqrt{d})$. Since the canonical involution must restrict to Galois conjugation on $\phi(K)$, we have that $\overline{\alpha} = \phi(-\sqrt{d}) = -\alpha$, so $\alpha \in B_0$ is a pure quaternion of norm $-\alpha^2 = \phi(-(\sqrt{d})^2) = -d$. Similarly, we can see that each pure quaternion of norm $-d$ gives a distinct embedding of K into B, which finishes the proof. □

This relation illustrates one way in which we can use the algebraic theory of quaternion algebras to shed light on classical problems in number theory. Here is a simple instance.

By the squarefree part $n \in \mathbb{N}$, we mean the number $d \in \mathbb{N}$ such that $n = dm^2$ with m maximal.

Corollary 5.3.3. *A positive integer n is a sum of three rational squares if and only if its squarefree part is not* 7 mod 8*.*

Proof. Note the restricted norm form of $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ is $x^2 + y^2 + z^2$. By the proposition, n is the sum of three (rational) squares if and only if $K = \mathbb{Q}(\sqrt{-n})$ embeds in B. Recall that B is ramified precisely at 2 and ∞. So by (3) of the theorem, n is a sum of three squares if 2 does not split in K. Let d be the squarefree part of n, and Δ be the discriminant of K, i.e. $\Delta = -d$ if $d \equiv 3 \bmod 4$ and $\Delta = -4d$ otherwise. Then 2 is split in K if and only if $\left(\frac{\Delta}{2}\right) = +1$, i.e., if and only if $\Delta \equiv \pm 1 \bmod 8$. Only $\Delta \equiv 1 \bmod 8$ is possible, which corresponds to $d \equiv 7 \bmod 8$. □

In fact this corollary is true if one restricts to the sum of three integral squares, which is Legendre's three squares theorem (usually stated in the form n is a sum of 3 integral squares if and only if n is not of the form $4^j(8k + 7)$). One can either deduce this from the above result by showing an integer is a sum of three rational squares if and only if it is a sum of three integral squares (see, e.g., [Ger08, Sec 9.4]), or prove it directly. We will give a direct proof it in the next chapter when we study orders in quaternion algebras. (There are of course non-quaternionic proofs as well.)

Exercise 5.3.2. Relate the above corollary to the usual statement of Legendre's three squares theorem by showing $n \in \mathbb{N}$ is of the form $4^j(8k + 7)$ for $j, k \in \mathbb{Z}_{\geq 0}$ if and only if the squarefree part of n is 7 mod 8.

Exercise 5.3.3. Determine what positive integers are of the form $x^2 + 3y^2 + 3z^2$ for $x, y, z \in \mathbb{Q}$.