Chapter 4

Sums of Squares

In this chapter, will get our first major theorem about Diophantine equations: Fermat's determination of when a number is a sum of two squares. This will put together much of what we have learned in previous chapters, which were in some sense preliminaries to this and later theorems. The proof will use unique factorization in $\mathbb{Z}[i]$, norms, and modular arithmetic.

Then we will consider some related questions also studied by Fermat: when is a number of the form $x^2 + dy^2$, e.g., $x^2 + 2y^2$ or $x^2 + 3y^2$. For this, we will need two major theorems in elementary number theory: the Chinese Remainder Theorem and Quadratic Reciprocity. (Really, the main use of the Chinese Remainder Theorem is to prove Quadratic Reciprocity, which is one of Gauss's major contributions to number theory.) This will allow us to say some things about numbers of the form $x^2 + dy^2$, but a complete answer is not so easy.

Finally, we will briefly discuss the problems of when a number is a sum of three or four squares, which were answered by Gauss and Lagrange.

4.1 Sums of Two Squares

In this section, we will give a complete answer to the question: *what numbers are sums of two squares?* i.e., for what $n \in N$ does

$$x^2 + y^2 = n \tag{4.1.1}$$

have a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. The answer was known to Fermat, though our approach, which comes via unique factorization in $\mathbb{Z}[i]$, did not come until after Gauss. Recall the following, which we will repeatedly use:

Fact 4.1.1. *An integer n is a sum of two squares if and only if $n = x^2+y^2 = (x+yi)(x-yi) = N(x + yi)$ is a norm from $\mathbb{Z}[i]$.*

The fact above immediately yields the

Proposition 4.1.2. (Composition law) *If m and n are sums of two squares, so is mn.*

Proof. If m and n are sums of two squares, then $m = N(\alpha)$ and $n = N(\beta)$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Then $mn = N(\alpha)N(\beta) = N(\alpha\beta)$ by multiplicativity of the norm, when mn is also a norm, i.e., a sum of two squares. □

Exercise 4.1.1. If $m = x^2 + y^2$ and $n = z^2 + w^2$, explicitly find u, v (in terms of x, y, z, w) such that $mn = u^2 + v^2$.

We also recall from Proposition 3.2.4 that (4.1.1) does not have a solution if $n \equiv 3 \bmod 4$.

The composition law suggests that the essential case of (4.1.1) is when $n = p$ prime. Indeed this is true, and we will first treat $n = p$. Since $2 = 1^2 + 1^2$, it suffices to answer this for $p \equiv 1 \bmod 4$. Here, a couple of auxiliary results will be useful.

Proposition 4.1.3. (Wilson's theorem) *Let p be a prime. Then $(p-1)! \equiv -1 \bmod p$.*

Proof. This is clear when $p = 2$, so assume p is odd. Recall each $1 \leq a \leq p-1$ is invertible mod p. Further a is its own inverse mod p if and only if $a^2 \equiv 1 \bmod p$, i.e., $p|(a^2 - 1)$. By the prime divisor property, this happens exactly when $p|(a-1)$ or $p|(a+1)$, but the bounds on a imply this happens if and only if $a = 1$ or $a = p-1$. So

$$(p-1)! \equiv \prod_{a=1}^{p-1} a \equiv 1 \cdot (p-1) \prod_{a=2}^{p-2} a \bmod p.$$

Now in the latter product (which must consist of an even number of terms, 0 if $p = 3$), each $2 \leq a \leq p-2$ has an inverse mod p which is some $2 \leq a^{-1} \leq p-2$ with $a^{-1} \neq a$. By uniqueness of inverses, we can group this latter product in to pairs of the form (aa^{-1}), whence the latter product is 1 mod p, so $(p-1)! \equiv -1 \bmod p$. □

Lemma 4.1.4. (Lagrange's lemma) *Let $p \equiv 1 \bmod 4$. Then -1 is a square mod p, i.e., there exists $m \in \mathbb{Z}$ such that $p|(m^2 + 1)$.*

Proof. First note that -1 is a square mod p means there exists $m \in \mathbb{Z}$ such that $m^2 \equiv -1 \bmod p$, i.e., $m^2 + 1 \equiv 0 \bmod p$, so indeed the two assertions in the statement of the lemma are equivalent.

Write $p = 4k + 1$ for some $k \in \mathbb{N}$. By Wilson's theorem,

$$(4k)! \equiv -1 \bmod p.$$

On the other hand,

$$\begin{aligned}(4k)! \equiv (2k)! \times (2k+1)(2k+2)\cdots(4k) &\equiv (2k)! \times (-2k)(-2k+1)\cdots(-1) \\ &\equiv (2k)!(-1)^{2k}(2k)! \equiv ((2k)!)^2 \bmod p,\end{aligned}$$

hence -1 is a square mod p. □

Theorem 4.1.5 (Fermat)**.** *Let p be prime. Then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.*

Proof. As remarked above, we already know $2 = 1^2 + 1^2$ and p is not a sum of 2 squares if $p \equiv 3 \bmod 4$ by Proposition 3.2.4. Thus it suffices to assume $p \equiv 1 \bmod 4$ and show p is a sum of 2 squares, i.e., show p is a norm from $\mathbb{Z}[i]$.

Note that if p is a reducible element of $\mathbb{Z}[i]$, we can write $p = ab$ for some $a, b \in \mathbb{Z}[i]$ with $N(a), N(b) > 1$. Since $N(a)N(b) = N(p) = p^2$, this means p is a norm from $\mathbb{Z}[i]$.

Suppose p is not a norm from $\mathbb{Z}[i]$. By the last paragraph, this means p is an irreducible element of $\mathbb{Z}[i]$. By unique factorization for $\mathbb{Z}[i]$, this means p is a prime of $\mathbb{Z}[i]$ (Theorem 2.5.1). Now by Lagrange's lemma, there exists $m \in \mathbb{Z}$ such that $p|(m^2+1) = (m+i)(m-i)$. Since p is prime in $\mathbb{Z}[i]$, this means $p|(m+i)$or $p|(m-i)$. But this is impossible as $\frac{m}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, contradicting the hypothesis that p is a norm from $\mathbb{Z}[i]$. □

Exercise 4.1.2. Let p be a prime of $\mathbb{N}$. Show p is a prime of $\mathbb{Z}[i]$ if and only if $p \equiv 3 \bmod 4$.

Exercise 4.1.3. Let p be a prime of $\mathbb{N}$. If $p = 2$ or $p \equiv 1 \bmod 4$, show that the irreducible factorization of p in $\mathbb{Z}[i]$ is of the form $p = \pi\overline{\pi}$, where π is any element of $\mathbb{Z}[i]$ of norm p.

Exercise 4.1.4. Show that the primes (i.e., irreducibles) of $\mathbb{Z}[i]$ are precisely the elements of the form (i) up where $u \in \{\pm 1, \pm i\}$ and $p \equiv 3 \bmod 4$ is a prime of $\mathbb{N}$, or (ii) an element of $\mathbb{Z}[i]$ of norm 2 or some prime $p \equiv 1 \bmod 4$. Further, show if π is an irreducible of the second type, then $u\pi \notin \mathbb{Z}$ for any unit u.

The next exercise is about counting the number of solutions to our favorite Diophantine equation.

Exercise 4.1.5. Let p be a prime of $\mathbb{N}$.
(i) Determine the number of irreducible elements of norm p in $\mathbb{Z}[i]$.
(ii) Deduce that for $p = 2$, there are exactly 4 solutions to $x^2 + y^2 = p$ with $x, y \in \mathbb{Z}$, and exactly 1 solution with $x, y \in \mathbb{N}$.
(iii) Deduce that for $p \equiv 1 \bmod 4$, there are exactly 8 solutions to $x^2 + y^2 = p$ with $x, y \in \mathbb{Z}$, and exactly 2 solutions with $x, y \in \mathbb{N}$.

Theorem 4.1.6. (Fermat's two square theorem) *Let $n \in \mathbb{N}$. Then n is a sum of two squares, i.e., $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$, if and only if each prime which is 3 mod 4 appears to an even power in the prime-power factorization of n.*

Proof. Let us write the prime-power factorization of n as

$$n = \prod p_i^{e_i} \prod q_j^{f_j}$$

where each $p_i \equiv 3 \bmod 4$ and each q_j is 2 or 1 mod 4.

($\Leftarrow$) First suppose the latter condition is satisfied, i.e., each e_i is even. Then $\prod p_i^{e_i}$ is a square, whence a sum of two squares. Also, by Theorem 4.1.5, we know each q_j is a sum of two squares. Then by the composition law, n is a sum of two squares.

($\Rightarrow$) To prove the converse direction, we essentially want a kind of converse to the composition law—that if rs is a sum of two squares then r and s must each be sums of two squares. This is obviously not true if $r = s$, but it turns out to be true if r and s are relatively prime, which the following argument shows. (See corollary below.)

Suppose n is a sum of two squares, i.e., $n = N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. By the above exercises, each p_i is irreducible in $\mathbb{Z}[i]$ and an irreducible factorization of any q_j looks like $q_j = \pi_j \overline{\pi}_j$ where π_j is an element of norm q_j in $\mathbb{Z}[i]$. So an irreducible factorization of n in $\mathbb{Z}[i]$ looks like

$$n = \prod p_i^{e_i} \prod \pi_j^{f_j} \prod \overline{\pi}_j^{f_j}.$$

Now write an irreducible factorization of $\alpha \in \mathbb{Z}[i]$ as

$$\alpha = u \prod r_i^{h_i} \prod \phi_j^{k_j},$$

where u is a unit and, by Exercise 4.1.4, we may assume each r_i is a prime of $\mathbb{N}$ with $r_i \equiv 3 \bmod 4$ and each ϕ_j is an element of $\mathbb{Z}[i]$ of s_j, where s_j is a prime of $\mathbb{N}$ which is 2 or 1 mod 4. Then, by multiplicativity of the norm,

$$n = N(\alpha) = N(u) \prod N(r_i)^{h_i} \prod N(\phi_j)^{k_j} = \prod r_i^{2h_i} \prod s_j^{k_j}.$$

Now, by unique factorization in $\mathbb{Z}$, we have up to reordering each $r_i = p_i$, $2h_i = e_i$, $s_j = q_j$ and $k_j = f_j$. Hence each e_i is even, which is precisely the latter condition in the theorem. □

The following structural result (a converse to the composition law) follows directly from the theorem:

Corollary 4.1.7. *Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Then mn is a sum of two squares if and only if both m and n are.*

Exercise 4.1.6. Suppose $p_1, \dots, p_r$ are distinct primes which are all 1 mod 4. Determine the number of solutions to $x^2 + y^2 = p_1 \cdots p_r$.

Exercise 4.1.7. Suppose $p \equiv 3 \bmod 4$ and $q \equiv 1 \bmod 4$ are primes. Determine the number of solutions to $x^2 + y^2 = p^e q^f$ for $e, f \in \mathbb{N}$.

4.2 Pythagorean Triples

We can also apply the ideas from the last section to the determination of **Pythagorean triples** (x, y, z), i.e., positive integer solutions[1] to

$$x^2 + y^2 = z^2. \tag{4.2.1}$$

We say a Pythagorean triple $(x, y, z) \in \mathbb{N}^3$ is **primitive** if $\gcd(x, y) = 1$. If (x', y', z') is a triple and $\lambda = \gcd(x', y')$, then also $\lambda | z'$ and we can write $(x', y', z') = (\lambda x, \lambda y, \lambda z)$. Moreover (x', y', z') is a Pythagorean triple if and only if (x, y, z) is a primitive Pythagorean triple, so it suffices to determine primitive Pythagorean triples.

[1] We could also look at integer solutions to (4.2.1), but if (x, y, z) is a solution, then so is $(\pm x, \pm y, \pm z)$, and if one of x, y, z is 0, then the solutions are trivial—e.g., all integer solutions with $y = 0$ are $(x, 0, \pm x)$ for $x \in \mathbb{Z}$. Hence we get all (algebraically) interesting solutions to the Pythagorean equation by assuming $x, y, z > 0$, where this equation has the usual interpretation in terms of right-angled triangles.

Lemma 4.2.1. *Suppose (x, y, z) is a primitive Pythagorean triple. Then $x + yi$ and $x - yi$ are relatively prime in $\mathbb{Z}[i]$, i.e., they have no common prime divisors in $\mathbb{Z}[i]$.*

Proof. Suppose instead, $x + yi$ and $x - yi$ have a common prime divisor $\pi \in \mathbb{Z}[i]$. Then π divides their sum $2x$ and their difference $2yi$. Note if $\pi|x$ and $\pi|y$ then $1 < N(\pi)|N(x) = x^2$ and $1 < N(\pi)|N(y) = y^2$, but this is impossible if $\gcd(x, y) = 1$. Hence, $\pi|2$, i.e., $\pi = \pm(1 \pm i)$. Then

$$N(\pi) = \pi\overline{\pi} = 2|(x + yi)(x - yi) = x^2 + y^2 = z^2.$$

This means z is even, so $x^2 + y^2 \equiv z^2 \equiv 0 \bmod 4$, which implies x and y are also both even (use the same argument as in Proposition 3.2.5), contradicting primitivity. □

Lemma 4.2.2. *Suppose $\alpha, \beta \in \mathbb{Z}[i]$ are relatively prime. If $\alpha\beta = \gamma^2$ is a square in $\mathbb{Z}[i]$, then $u\alpha$ and $u^{-1}\beta$ are squares for some unit u of $\mathbb{Z}[i]$.*

Proof. Note that this is trivial if γ is a unit (and vacuous if $\gamma = 0$). So assume $\alpha\beta$ is the square of some $\gamma \in \mathbb{Z}[i]$, where γ is a non-zero non-unit. Then γ has a prime factorization in $\mathbb{Z}[i]$:

$$\gamma = \prod \pi_i^{e_i}.$$

Thus the prime factorization of $\alpha\beta$ is

$$\alpha\beta = \prod \pi_i^{2e_i}.$$

Up to a reordering of primes, we have

$$\alpha = u^{-1}\pi_1^{2e_1} \cdots \pi_j^{2e_j}$$

$$\beta = u\pi_{j+2}^{2e_{j+1}} \cdots \pi_k^{2e_k}$$

for some unit u. □

Exercise 4.2.1. Give an example of relatively prime non-units α, β in $\mathbb{Z}[i]$ such that $\alpha\beta$ is a square in $\mathbb{Z}[i]$, but α and β are not squares in $\mathbb{Z}[i]$.

Exercise 4.2.2. Show that if $u, v \in \mathbb{N}$ are relatively prime with $2|uv$, then $(u^2-v^2, 2uv, u^2+v^2)$ is a primitive Pythagorean triple.

Proposition 4.2.3. *(x, y, z) is a primitive Pythagorean triple if and only if x and y are (in some order) $u^2 - v^2$ and $2uv$ for u, v relatively prime in $\mathbb{N}$ with $u > v$ and u, v not both odd. In this case, $z = u^2 + v^2$.*

Proof. ($\Leftarrow$) This is Exercise 4.2.2.

($\Rightarrow$) Suppose (x, y, z) is a primitive Pythagorean triple, so $x^2+y^2 = (x+yi)(x-yi) = z^2$. By the Lemma 4.2.1, $x + yi$ and $x - yi$ are relatively prime, and by Lemma 4.2.2 they are units times squares. In particular $x+yi = \pm\alpha^2$ or $x+yi = \pm i\alpha^2$ for some $\alpha \in \mathbb{Z}[i]$. Since -1

is a square in $\mathbb{Z}[i]$, we may absorb the possible minus sign into α and write either $x+yi = \alpha^2$ or $x + yi = i\alpha^2$.

Write $\alpha = u + vi$, and we get that either

$$x + yi = (u + vi)^2 = u^2 - v^2 + 2uvi$$

or

$$x + yi = i(u + vi)^2 = -2uv + (u^2 - v^2)i.$$

In the first case we have $x = u^2 - v^2$, $y = 2uv$. In the second, we may replace u by $-u$ to write $x = 2uv$, $y = u^2 - v^2$. It is easy to see the conditions $\gcd(u, v) = 1$, $u > v$ and u, v not both odd are necessary from the facts that $\gcd(x, y)$ and $x, y > 0$. (You will probably see this in the course of doing Exercise 4.2.2.)

In this setting, we have $z^2 = x^2+y^2 = N(x+yi) = N((u+vi)^2) = N(u+vi)^2 = (u^2+v^2)^2$, so $z = u^2 + v^2$. □

Corollary 4.2.4. *Let $p \in \mathbb{N}$ be prime. Then p occurs as the hypoteneuse of a right-angle triangle with integer length sides if and only if $p > 2$ is a sum of two squares, which is true if and only if $p \equiv 1 \bmod 4$.*

Proof. The second equivalence is Fermat's two square theorem, so it suffices to prove the first.

($\Rightarrow$) Suppose p is such a hypotenuse. Clearly $p \neq 2$. Now $x^2 + y^2 = p^2$. This implies $\gcd(x, y) = 1$. Hence by the proposition $p = u^2 + v^2$ for some u, v.

($\Leftarrow$) Suppose $p = u^2+v^2$ is odd. Then $u \neq v$ and u and v are not both odd. Furthermore, we may assume $u > v$. By the proposition $(u^2 - v^2, 2uv, p)$ is a primitive Pythagorean triple. □

Exercise 4.2.3. Let p, q be distinct primes. Determine when pq is the hypoteneuse of a right-angle triangle with integer length sides.

4.3 The Chinese Remainder Theorem

Recall that a key component of Fermat's two squares theorem was the determination of when -1 is a square mod p. To generalize Fermat's 2 squares theorem to other situations, e.g., what numbers (or primes) are of the form $x^2 + dy^2$, one is naturally led to the problem of what numbers are squares mod p.

This is addressed by Gauss's famous law of quadratic reciprocity, which Gauss called the "golden theorem." It first appeared in his *Disquisitiones Arithmeticae* (1804, but written in 1801 when he was 21). He thought it so important that he published 6 different proofs (now there are at least 240 proofs!), and it is commonly regarded as the crown jewel of elementary number theory.

The proof we will give (in the next section) uses another famous result (much much older) from elementary number theory, the Chinese remainder theorem (CRT). This goes back over 1500 years ago to a book by Sun Tzu (no, not that Sun Tzu) from somewhere between the

3rd and 5th centuries. (Fun fact: now even in Chinese it's called (what translates to) the Chinese remainder theorem.) Another use of the CRT is to compute $\phi(n)$.

Theorem 4.3.1. (Chinese Remainder Theorem (CRT)) *Let $m, n \geq 2$ be relatively prime. Consider the map $\alpha : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ defined by sending any $a + mn\mathbb{Z}$ to $(a + m\mathbb{Z}, a + n\mathbb{Z})$ for any $a \in \mathbb{Z}$. Then α is a bijection, and moreover, restricted to $(\mathbb{Z}/mn\mathbb{Z})^\times$ gives a bijection of $(\mathbb{Z}/mn\mathbb{Z})^\times$ with $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.*[2]

Proof. First note that α is well defined, i.e., if $a \equiv b \bmod mn$, then $a + m\mathbb{Z} = b + m\mathbb{Z}$ and $a + n\mathbb{Z} = b + n\mathbb{Z}$, so $\alpha(a + mn\mathbb{Z})$ does not depend upon the choice the element a within a class $C = a + mn\mathbb{Z}$.

To show α is a bijection of $\mathbb{Z}/mn\mathbb{Z}$ with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, since both sets have size mn, it suffices to show it is an injection, i.e., it is one-to-one, i.e., no two elements of $\mathbb{Z}/mn\mathbb{Z}$ go to the same element of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ under α. Suppose $\alpha(a + mn\mathbb{Z}) = \alpha(b + mn\mathbb{Z})$. We may assume $0 \leq a \leq b < mn$. Then $a \equiv b \bmod m$ and $a \equiv b \bmod n$. Hence $b - a$ is divisible by both m and n, and thus by mn since m and n are relatively prime (here unique factorization is used too). But $0 \leq b - a < mn$, so this is only possible if $b - a = 0$, i.e., $a = b$, which proves α is one-to-one.

Last, we show α is a bijection of $(\mathbb{Z}/mn\mathbb{Z})^\times$ with $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Recall that $a + mn\mathbb{Z} \in (\mathbb{Z}/mn\mathbb{Z})^\times$ if and only if $\gcd(a, mn) = 1$, i.e., if and only if $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Hence for such an a, $\alpha(a + mn\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Conversely, given any element of $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, we can write this element in the form $(a+m\mathbb{Z}, a+n\mathbb{Z})$ for some $a \in \mathbb{Z}$ using the fact that α is a bijection of $\mathbb{Z}/mn\mathbb{Z}$ with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (really, we only need that α is surjective, i.e. onto, for this). Similarly, for such a we have $\gcd(a, m) = \gcd(a, n) = 1$, which means $a + mn\mathbb{Z} \in (\mathbb{Z}/mn\mathbb{Z})^\times$. Now we have shown that α maps $(\mathbb{Z}/mm\mathbb{Z})^\times$ both into and onto $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. From the previous paragraph, we also know α restricted to invertible elements is an injection, so it must be a bijection. □

Corollary 4.3.2. *Let $m, n \geq 2$ be relatively prime. Then $\phi(mn) = \phi(m)\phi(n)$.*

Note this corollary gives $\phi(pq) = (p-1)(q-1)$ for distinct primes p, q as a special case, which was Exercise 3.3.5. Moreover, applying this corollary repeatedly gives us a formula for $\phi(n)$: if $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

$$\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_r^{e_r}). \tag{4.3.1}$$

(In a similar manner, we could state the CRT for $\mathbb{Z}/n_1 n_2 \cdots n_r\mathbb{Z}$ where the n_i's are relatively prime.) If each $e_i = 1$ (so n is square-free), then we just get $\phi(n) = (p_1-1)(p_2-1)\cdots(p_r-1)$. For arbitrary n, you can combine (4.3.1) with Exercise 3.3.4, to write down a similar formula $\phi(n)$ in terms of only the p_i's and e_i's, giving a definite answer to Exercise 3.3.7.

Exercise 4.3.1. Use (4.3.1) to compute $\phi(60)$.

[2] For those who have had some algebra, in fact α is a ring isomorphism from $\mathbb{Z}/mn\mathbb{Z}$ to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ and restricts to a group isomorphism from $(\mathbb{Z}/mn\mathbb{Z})^\times$ to $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. In this way, the second statement (group isomorphism) follows from the first by restricting to the unit groups of the appropriate rings. The group isomorphism part (without using this terminology) is also Exercise 4.3.5.

Exercise 4.3.2. If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, write an explicit formula for $\phi(n)$ in terms of only the p_i's and e_i's.

Exercise 4.3.3. How many numbers $1 \leq n \leq 100$ are both 3 mod 4 and 2 mod 5?

Exercise 4.3.4. Use the CRT to help determine all numbers $1 \leq n \leq 100$ such that $n \equiv 1 \bmod 5$ and $n \equiv 2 \bmod 7$.

Exercise 4.3.5. Let $m, n \geq 2$ be coprime. Show the restriction $\alpha : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ satisfies $\alpha(1 + mn\mathbb{Z}) = (1 + m\mathbb{Z}, 1 + n\mathbb{Z})$ and α is multiplicative: $\alpha(ab + mn\mathbb{Z}) = \alpha(a + mn\mathbb{Z})\alpha(b + mn\mathbb{Z})$.

The next exercise may seem a bit contrived, but it can be viewed as an analogue of the highly useful Wilson's theorem to $n = pq$ and it is related to the trick we use for proving quadratic reciprocity.

Exercise 4.3.6. Let p, q be distinct odd primes. Let $P \in \mathbb{Z}/pq\mathbb{Z}$ be the product of all elements of $(\mathbb{Z}/pq\mathbb{Z})^\times$. Use the previous exercise together with Wilson's theorem to show $P \equiv 1 \bmod pq$. (*Hint:* Compute the product over $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ by first doing a product over $(\mathbb{Z}/p\mathbb{Z})^\times$, and then over $(\mathbb{Z}/q\mathbb{Z})^\times$.)

4.4 Quadratic Reciprocity

While the CRT provides nice closure to the problem of computing $\phi(n)$, our real goal is to apply it to quadratic reciprocity. It turns out that determining whether a is a square mod n essentially boils down to determining whether p is a square mod q, for primes p and q. Quadratic reciprocity says that, for odd primes p and q, whether p is a square mod q is determined by the reverse question of whether q is a square mod p. For the precise statement, the following notation will be helpful.

Definition 4.4.1. *Let p be an odd prime. The* **Legendre symbol**, *or* **quadratic residue symbol** $(\bmod p)$ *is defined for $a \in \mathbb{Z}$ by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a nonzero square mod} p \\ 0 & a \equiv 0 \bmod p \\ -1 & \text{else.} \end{cases}$$

So if a is relatively prime to p, then $\left(\frac{a}{p}\right)$ is 1 or -1, according to whether a is a square mod p or not. Note that $\left(\frac{a}{p}\right)$ depends only upon the congruence class of a mod p.

Example 4.4.1. For $p = 3$, we have $\left(\frac{0}{3}\right) = 0$, $\left(\frac{1}{3}\right) = 1$ and $\left(\frac{2}{3}\right) = -1$. (See Example 3.2.4.)

Example 4.4.2. For odd p, we have $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \bmod 4$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \bmod 4$ by Lagrange's lemma (Lemma 4.1.4). Note we can write this in a uniform way as saying

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

In this formulation, Lagrange's lemma is also called the **first supplemental law to quadratic reciprocity**.

The following exercise says that for a prime to p, $\left(\frac{a}{p}\right)$ is 1 half of the time and -1 half of the time.

Exercise 4.4.1. Let p be an odd prime. Show that map $x \mapsto x^2$ on $(\mathbb{Z}/p\mathbb{Z})^\times$ is 2-to-1. Conclude that the number of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ is equal to the number of nonsquares.

The usefulness of the Legendre symbol notation is because of the following result.

Proposition 4.4.2. *Let p be odd. The function $\left(\frac{\cdot}{p}\right)$ is (totally) multiplicative, i.e., for any $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. Note that if $p|a$ or $p|b$, both sides of the equality are zero, so assume a, b are both coprime to p.

First suppose $\left(\frac{a}{p}\right) = 1$. Then $a \equiv x^2 \bmod p$ for some $x \in \mathbb{Z}$, $x \not\equiv 0 \bmod p$. It is easy to see that ab is a square mod p if and only if $ab(x^{-1})^2$ is a square mod p, but $ab(x^{-1})^2 \equiv b \bmod p$. Whence $\left(\frac{ab}{p}\right) = \left(\frac{b}{p}\right)$, which is the desired equality.

The same argument applies if $\left(\frac{b}{p}\right) = 1$, so we are reduced to treating the case that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, where we need to show $\left(\frac{ab}{p}\right) = 1$. We can use a counting argument together with the previous exercise.

Assume $\left(\frac{a}{p}\right) = -1$. Note we can view multiplication by a as a map from $(\mathbb{Z}/p\mathbb{Z})^\times$ to itself: $x \mapsto ax$. Further, it is easy to see this is a bijection. By the case $\left(\frac{b}{p}\right) = 1$, we know ax is a nonsquare whenever x is a square. By the previous exercise, this must account for all $\frac{p-1}{2}$ times ax is a square as x ranges over $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus if $x = b$ with b a nonsquare ($\left(\frac{b}{p}\right) = -1$), we have that $ax = ab$ must be a square, i.e., $\left(\frac{ab}{p}\right) = 1 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Consequently, if $q_1^{e_1} \cdots q_r^{e_r}$ is the prime-power factorization of $a \in \mathbb{N}$, to determine whether a is a square mod p (an odd prime), it suffices to determine whether each $\left(\frac{q_i}{p}\right)$ is 1 or -1 as

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_r}{p}\right)^{e_r}.$$

If a is even, one of these q_i's will be 2, but we can instead replace a with $a + p$ (or $a - p$ or $p - a$ or ...) which is odd, to assume each q_i is odd (or alternatively keep a the same

and compute as $\left(\frac{2}{p}\right) = \left(\frac{p+2}{p}\right)$, factoring $p+2$ into odd primes). So to determine whether a number is a square mod p, it suffices to determine $\left(\frac{q}{p}\right)$ for each odd prime q. Of course $\left(\frac{p}{p}\right) = 0$, so we may also assume $q \neq p$.

We will need one more auxiliary result to prove quadratic reciprocity, which in turn requires a basic fact about polynomials over fields.

Exercise 4.4.2. Let F be a field and $f(x)$ a polynomial of degree n over F, i.e., $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x^1 + a_0$, where each $a_i \in F$ and $a_n \neq 0$.

(i) Prove that $x - b$ divides $f(x)$ (i.e., $f(x) = (x-b)g(x)$ for a polynomial $g(x)$ over F of degree $n-1$) if and only if $f(b) = 0$. (*Suggestion:* Use polynomial division and Fermat descent on the degree of $f(x)$.)

(ii) Conclude that there are at most n distinct roots of F.

Proposition 4.4.3. (Euler's criterion) *Let p be an odd prime and $a \in \mathbb{Z}$ be relatively prime to p. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof. Recall by Fermat's little theorem, we have $x^{p-1} \equiv 1 \bmod p$ for all x which are invertible mod p. So if a is a square mod p, i.e., $a \equiv x^2 \bmod p$ for some such x, then

$$\left(\frac{a}{p}\right) \equiv 1 \equiv x^{p-1} \equiv a^{\frac{p-1}{2}} \bmod p. \tag{4.4.1}$$

So it suffices to treat the case where a is not a square mod p.

Equivalently, we want to show if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is not a square, then $a^{\frac{p-1}{2}} = -1$. (For the rest of the proof, we work in $\mathbb{Z}/p\mathbb{Z}$ rather than $\mathbb{Z}$.) Since $(a(p-1)/2)^2 = 1$, we always have $a^{(p-1)/2} = \pm 1$ since the only elements whose square is 1 in $\mathbb{Z}/p\mathbb{Z}$ are ± 1. (We've seen this in the proof of Wilson's theorem, as $x^2 = 1$ is equivalent to $x \in \mathbb{Z}/p\mathbb{Z}$ being its own inverse. Alternatively, apply the above exercise to the polynomial $f(x) = x^2 - 1$ over $F = \mathbb{Z}/p\mathbb{Z}$.) So it suffices to show $a^{(p-1)/2} \neq 1$ for any nonsquare $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

By the previous exercise, the polynomial $f(x) = x^{(p-1)/2} - 1$ over $F = \mathbb{Z}/p\mathbb{Z}$ has at most $\frac{p-1}{2}$ roots in $\mathbb{Z}/p\mathbb{Z}$. By (4.4.1) we know each square $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a root of $f(x)$. But there are precisely $\frac{p-1}{2}$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ by Exercise 4.4.1. Thus whenever a is a nonsquare, a is not a root of $f(x)$, i.e., $a^{(p-1)/2} \neq 1$. □

Exercise 4.4.3. Use Euler's criterion to give an alternative proof of Proposition 4.4.2.

As an aside, the ideas in the proof of Euler's criterion can also be used to determine the group structure of $(\mathbb{Z}/p\mathbb{Z})^\times$, something you would do in an algebra class. We won't use this in our course, but I'll leave it as:

Exercise 4.4.4. Prove that for any prime p, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. (*Suggestion:* Try contradiction.)

Exercise 4.4.5. Use the previous exercise to show $(\mathbb{Z}/pq\mathbb{Z})^\times$ is cyclic for any distinct primes p, q.

Theorem 4.4.4. (Law of quadratic reciprocity) *Let p and q be distinct odd primes. Then*

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

In other words, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ unless $p \equiv q \equiv 3 \bmod 4$, in which case $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Sometimes, for symmetry, quadratic reciprocity is stated as $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. While this is a very practical result for computing $\left(\frac{a}{p}\right)$ (see below), the real beauty of it lies in the symmetry—it gives us a relation between squares mod p and squares mod q that seems completely miraculous. By this I mean, there is no obvious reason why p being a square mod q should affect whether q is a square mod p, but in fact one determines the other (once we know their congruence classes mod 4). Since there is no obvious reason why these are related, there is no simple direct proof—all known proofs either use some clever trickery or more advanced mathematics. (I suspect part of the reason Gauss looked for several proofs was to find a "good" reason why this law holds, though I don't know to what extent he was satisfied with his proofs.) We'll give a tricky proof, that I first learned from [Sti03], and is a variant of Rousseau's proof published in 1991 [Rou91].

Proof. Let p, q be distinct odd primes. Set

$$S = \left\{1 \le x \le \frac{pq-1}{2} | \gcd(x, pq) = 1\right\},$$

so we may regard $(\mathbb{Z}/pq\mathbb{Z})^\times = S \cup -S$, where $-S = \{-x | x \in S\}$. We will consider $\prod_{x\in S} x$ both mod p and mod q.

Note that mod p, we can list the elements of S as $\frac{q-1}{2}$ full sequences $1, 2, \dots, p-1 \bmod p$ and the half sequence $1, 2, \dots, \frac{p-1}{2} \bmod p$, excluding the multiples $q, 2q, \dots, \frac{p-1}{2}q$ of q. E.g., if $p = 5$ and $q = 7$, then $S = \{1 \le x \le 17 : \gcd(x, 35) = 1\}$ which we can write in rows as

1	2	3	4	~~5~~
6	~~7~~	8	9	~~10~~
11	12	13	~~14~~	~~15~~
16	17			

corresponding to the 3 full sequences mod p and 1 half sequence mod p, where we've crossed out the numbers to be excluded.

Hence

$$\prod_{x\in S} x \equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!/q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \bmod p,$$

where the second equivalence comes from Wilson's theorem, along with the fact that $1/q^{\frac{p-1}{2}} \equiv \pm 1 \equiv q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod p$, and Euler's criterion. Similarly

$$\prod_{x \in S} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \bmod q.$$

In other words, writing $\alpha(x) = (x \bmod p, x \bmod q)$ as the map $\alpha : (\mathbb{Z}/pq\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ from the statement of the Chinese Remainder theorem, we have

$$\prod_{x \in S} \alpha(x) \equiv \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\right) \bmod (p, q) \tag{4.4.2}$$

(Here we write $\bmod (p,q)$ to mean mod p in the first component and mod q in the second.)

Recall the Chinese Remainder Theorem says that α is a bijection of $(\mathbb{Z}/pq\mathbb{Z})^\times$ with $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Since $(\mathbb{Z}/pq\mathbb{Z})^\times = S \cup -S$, this means that $\alpha(S) = \{\alpha(x) | x \in S\}$ contains exactly one of (a,b) and $(-a,-b)$ for each (a,b) in

$$T = \left\{(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times : 1 \le a \le p, 1 \le b \le \frac{q-1}{2}\right\},$$

and conversely for each $(a,b) \in \alpha(S)$ either in (a,b) or $(-a,-b)$ is in T. (Here we used that if $\alpha(x) = (a,b)$, then $\alpha(-x) = (-a,-b)$.) Hence

$$\begin{aligned}\prod_{x \in P} \alpha(x) \equiv \pm \prod_{(a,b) \in T} (a,b) &\equiv \pm \left((p-1)!^{\frac{q-1}{2}}, \left(\frac{q-1}{2}\right)!^{p-1}\right) \\ &\equiv \pm \left((-1)^{\frac{q-1}{2}}, \left(\frac{q-1}{2}\right)!^{p-1}\right) \bmod (p,q),\end{aligned}$$

where we used Wilson's theorem again in the last equivalence.

Note that

$$-1 \equiv (q-1)! \equiv 1 \cdot 2 \cdots \frac{q-1}{2} \cdot (-1)(-2) \cdots (-\frac{q-1}{2}) \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q-1}{2}\right)!^2 \bmod q,$$

hence

$$\left(\frac{q-1}{2}\right)!^{p-1} \equiv \left(\left(\frac{q-1}{2}\right)!^2\right)^{\frac{p-1}{2}} \equiv \left((-1)(-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \bmod q.$$

Thus

$$\prod_{x \in P} \alpha(x) \equiv \pm \left((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \bmod (p,q). \tag{4.4.3}$$

Dividing (4.4.2) by (4.4.3), we get

$$(1,1) \equiv \pm \left(\left(\frac{q}{p}\right), (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)\right) \bmod (p,q).$$

Since p and q are odd, this means that both $\left(\frac{q}{p}\right)$ and $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ (which are both ± 1 in $\mathbb{Z}$) must both be $+1$ or both be -1, whence

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

which is precisely the Quadratic Reciprocity Law. □

One application is, if p is large, this lets us determine if something is a square mod p quite quickly, much faster than trying to compute all squares mod p.

Example 4.4.3. Determine if 15 is a square mod 103.

First, by multiplicativity

$$\left(\frac{15}{103}\right) = \left(\frac{3}{103}\right)\left(\frac{5}{103}\right).$$

Now by quadratic reciprocity, we have

$$\left(\frac{3}{103}\right) = -\left(\frac{103}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

and

$$\left(\frac{5}{103}\right) = \left(\frac{103}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Thus $\left(\frac{15}{103}\right) = (-1)(-1) = 1$, so 15 is a square mod 103, even though we didn't determine what it's a square of.

Example 4.4.4. Determine if 94 is a square mod 101.

We could write $94 = 2 \cdot 47$ and try to compute $\left(\frac{2}{101}\right)$ and $\left(\frac{47}{101}\right)$. The latter we can use quadratic reciprocity for. There is a **second supplementary law** to compute $\left(\frac{2}{p}\right)$ as well, so this is possible, though we will not prove it in this course (see the next section for a statement). Instead we compute

$$\left(\frac{94}{101}\right) = \left(\frac{-7}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{7}{101}\right) = 1 \cdot \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -1,$$

using both the first supplementary law and quadratic reciprocity. Thus we see 94 is not a square mod 101.

Example 4.4.5. Determine for what primes p is 3 a square mod p.

We know 3 is a square mod 2 and mod 3, so it suffices to consider odd primes $p > 3$. By quadratic reciprocity we have

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Now $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \bmod 3$ and is -1 if $p \equiv 2 \bmod 3$. On the other hand $(-1)^{(p-1)/2}$ is 1 if $p \equiv 1 \bmod 4$ and -1 if $p \equiv 3 \bmod 4$. So $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \bmod 3$ and $p \equiv 1 \bmod 4$ or

$p \equiv 2 \bmod 3$ and $p \equiv 3 \bmod 4$.

Hence 3 is a square mod p if and only if $p = 2, 3$ or $p \equiv 1, 11 \bmod 12$. (To combine a congruence mod 3 and and congruence mod 4 to one mod 12, you can either use the CRT or just check it by hand).

Exercise 4.4.6. Determine if 21 is a square mod 101. What about mod 103?

Exercise 4.4.7. Determine if 92 is a square mod 101. What about mod 103?

Exercise 4.4.8. Determine for what primes p we have 5 is a square mod p.

Exercise 4.4.9. Determine for what primes p we have 7 is a square mod p.

4.5 Numbers of the form $x^2 + dy^2$

Fermat not only studied what numbers are of the form x^2+y^2, but also considered questions like what numbers are of the form $x^2 + 2y^2$ and $x^2 + 3y^2$? (Geometrically, the case $x^2 + 2y^2$ corresponds to asking what numbers are the sums of 3 squares where at least 2 of the squares have the same size.) In this section, we'll take a brief look at the question: For fixed $d \in \mathbb{N}$, for which $n \in \mathbb{N}$ does

$$x^2 + dy^2 = n \tag{4.5.1}$$

have a solution for $x, y \in \mathbb{Z}$. (Geometrically, this is asking when is n a sum of $d+1$ squares where all or all but one of the squares have the same size.) This will show off some of the power of quadratic reciprocity, as well as give you a glimpse into a very beautiful and rich part of number theory that occupied many great minds since Fermat.

This is a special case of Gauss's theory of **binary quadratic forms**, which are polynomials of the form

$$Q(x, y) = ax^2 + bxy + cy^2$$

for some $a, b, c \in \mathbb{Z}$. (Here binary refers to the fact that we have two variables, and more generally a **quadratic form** is a polynomial which is a sum of terms that all have degree two, i.e., a homogeneous polynomial of degree 2.) In some sense, these are the simplest kinds of Diophantine equations in 2 variables beyond the linear ones $ax + by = n$. Here the basic question is, given $Q(x, y)$ determine when $Q(x, y) = n$ has a solution, i.e., which n are **represented by** (or **of the form**) $Q(x, y)$? It turns out that a complete understanding of (4.5.1) involves looking at more general binary quadratic forms.

Without bringing in Gauss's general theory of binary quadratic forms, there are still many things we can say.[3] Here are a few simple general results.

[3] You can look at my Number Theory II notest [Marb] and the references therein for more about binary quadratic forms.

Exercise 4.5.1. Show that n is represented by x^2+dy^2, i.e., (4.5.1) has a solution if and only if n is a norm from $\mathbb{Z}[\sqrt{-d}]$, i.e., $n = N(\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{-d}]$.

Corollary 4.5.1. (Composition law) *For $d > 0$, if m and n are represented by x^2+dy^2, so is mn.*

Proof. Under the hypotheses, $m = N(\alpha)$ and $n = N(\beta)$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-d}]$. Thus $mn = N(\alpha\beta)$ by multiplicativity of the norm. □

Consequently, just like for $x^2+y^2 = n$, the most fundamental case of (4.5.1) should be when n is prime. The composition law doesn't exactly reduce the general problem to the case where n is prime. For instance if $n = pq$, we can say n is represented by x^2+dy^2 if both p and q are, but it could happen that n is still represented by x^2+dy^2 when p and q are not. As an example, $21 = 1^2 + 5 \cdot 2^2$, but neither 3 nor 7 are represented by x^2+5y^2. Recall, we used unique factorization of $\mathbb{Z}[i]$ to prove a converse to the composition law for x^2+y^2 (if mn are sum of two squares and coprime, then m and n are each sums of two squares—Corollary 4.1.7), but this example shows the composition law doesn't have a converse for x^2+5y^2.

The failure of a converse to this composition law is related to the failure of unique factorization for $\mathbb{Z}[\sqrt{-5}]$, and can be explained by Gauss's theory of binary quadratic forms. In this case, both 3 and 7 are represented by $Q(x,y) = 2x^2+2xy+3y^2$, and one can show that if coprime m and n are represented $Q(x,y)$, then mn is represented by x^2+5y^2, which gives a reason why 21 is of the form x^2+5y^2. Binary quadratic forms give a modified converse of the composition law, which says as a special case: if pq is represented by x^2+5y^2 then either both p and q are represented by x^2+5y^2 or both p and q are represented by $2x^2+2xy+3y^2$. Thus to determine which numbers are of the form x^2+5y^2 we want to determine which primes are of the form x^2+5y^2 as well as which primes are of the form $2x^2+2xy+3y^2$.

One can get some simple necessary conditions using modular arithmetic:

Exercise 4.5.2. Show that if p is represented by x^2+5y^2, then $p = 5$ or $p \equiv 1, 9 \bmod 20$. (Prove this directly—we give an alternative proof using quadratic reciprocity below.)

Exercise 4.5.3. Show that if p is represented by $2x^2+2xy+3y^2$, then $p = 2$ or $p \equiv 3 \bmod 4$.

In the former exercise, the necessary conditions turn out to be sufficient, but this requires much more work to prove. For the latter exercise, sufficient conditions turn out to be $p = 2$ or $p \equiv 3, 7 \bmod 20$.

In any case, for the rest of the section we will just focus on the problem: *which primes are of the form x^2+dy^2?* Moreover, we will only focus on the much easier aspect of determining *necessary conditions*. The question about a complete characterization of primes of the form x^2+dy^2 is studied in the beautiful (though somewhat advanced) book *Primes of the form x^2+ny^2* by David Cox [Cox13].

Proposition 4.5.2. *Suppose a prime p is represented by $x^2 + dy^2$. Then $-d$ is a square mod p.*

Proof. Suppose $p = x^2 + dy^2$ for some $x, y \in \mathbb{Z}$. Since p is not a square, we can take $0 < y < p$, and thus y and y^2 are invertible mod p. Now $x^2 + dy^2 \equiv 0 \bmod p$, means $x^2 \equiv -dy^2 \bmod p$, so

$$-d \equiv x^2 y^{-2} \equiv (xy^{-1})^2 \bmod p,$$

i.e., $-d$ is a square mod p, i.e., $\left(\frac{-d}{p}\right) = 1$. □

This proposition says that prove the non-existence of solutions to $x^2 + dy^2 = p$ for a given p and various d by determining the squares mod p.

Example 4.5.1. Say $p = 5$. The squares mod p are $0, 1, 4$. So 5 is not represented by $x^2 + dy^2$ whenever $-d \equiv 2, 3 \bmod 5$, i.e., whenever $d \equiv 2, 3 \bmod 5$, i.e., $d = 2, 3, 7, 8, 12, 13, \ldots$.

The beauty of quadratic reciprocity is, *quadratic reciprocity lets us do the reverse*: given d we can say p is not represented by $x^2 + dy^2$ if p lies in certain congruence classes mod m (here $m = d$ or $m = 4d$, as we will see in examples below).

Example 4.5.2. Consider $d = 5$. Then for p an odd prime not 5, $p = x^2 + 5y^2$ does not have a solution if $\left(\frac{-5}{p}\right) = 1$. (Clearly $2 = x^2 + 5y^2$ has no solution whereas $5 = x^2 + 5y^2$ does.) We compute $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$ by quadratic reciprocity. Recall Lagrange's lemma (i.e., the first supplementary law to quadratic reciprocity) says $\left(\frac{-1}{p}\right)$ is 1 if $p \equiv 1 \bmod 4$ and -1 if $p \equiv 3 \bmod 4$. As in the example above $\left(\frac{p}{5}\right)$ is 1 if $p \equiv 1, 4 \bmod 5$ and -1 if $p \equiv 2, 3 \bmod 5$.

Now $\left(\frac{-5}{p}\right) = 1$ if and only if $\left(\frac{-1}{p}\right)$ and $\left(\frac{p}{5}\right)$ are both $+1$ or are both -1. They are both $+1$ when $p \equiv 1 \bmod 4$ and $p \equiv 1, 4 \bmod 5$, i.e., $p \equiv 1, 9 \bmod 20$. They are both -1 when $p \equiv 3 \bmod 4$ and $p \equiv 2, 3 \bmod 5$, i.e., $p \equiv 3, 7 \bmod 20$.

Hence a prime p is not of the form $x^2 + 5y^2$ unless $p = 5$ or $p \equiv 1, 9, 3, 7 \bmod 20$. This proves part of Exercise 4.5.2, but doesn't rule out primes which are $3, 7 \bmod 20$. (The primes $p \equiv 3, 7 \bmod 20$ are represented by the related form $Q(x, y) = 2x^2 + 2xy + 3y^2$, which is related to why this approach does not rule them out.) However, considering $x^2 + 5y^2 \equiv x^2 + y^2 \bmod 4$ does rule out the primes which are $3, 7 \bmod 20$, which gives an "indirect" proof of Exercise 4.5.2.

In general, if $d = q_1^{e_1} \cdots q_r^{e_r}$ with q_i's distinct primes, we want to compute

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_r}{p}\right)^{e_r}.$$

The first supplementary law tells us to compute $\left(\frac{-1}{p}\right)$ we look at $p \bmod 4$. If q_i is odd, we compute $\left(\frac{q_i}{p}\right)$ as $(-1)^{(p-1)(q_i-1)/4}\left(\frac{p}{q_i}\right)$ by quadratic reciprocity. If $q_i = 2$, we can use the following:

Proposition 4.5.3. (Second supplementary law to quadratic reciprocity *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8. \end{cases}$$

The proof is somewhat involved and we will not do it here, but we just gave the statement to give a more complete picture of the theory. In any case, one of the bottom lines is that to determine if p is of the form $x^2 + dy^2$, quadratic reciprocity and the supplementary laws tell us one should look at congruences mod $4d$ (in fact mod $4q_1 \cdots q_r$ suffices). Here we are using the Chinese Remainder Theorem to say we can rewrite a collection of congruence conditions mod 4, mod q_1, ..., mod q_r to congruence conditions mod $4q_1 \cdots q_r$. The factor of 4 here comes from needing to use the first (and sometimes second) supplementary law. (While the second supplementary law requires a congruence mod 8, it is only needed when d is even, so in the end mod $4d$ or $4q_1 \cdots q_r$ suffices.)

Here are some exercises and more remarks for primes of the form $x^2 + dy^2$ for a few small d.

Exercise 4.5.4. Use the supplementary laws and Proposition 4.5.2 to show that if $p = x^2 + 2y^2$ (has a solution over $\mathbb{Z}$), then $p = 2$ or $p \equiv 1, 3 \bmod 8$. (This is an "indirect" approach to Exercise 3.2.2.)

Exercise 4.5.5. Use quadratic reciprocity and Proposition 4.5.2 to show that if $p = x^2 + 3y^2$ (has a solution over $\mathbb{Z}$), then $p = 3$ or $p \equiv 1 \bmod 3$. (This is an "indirect" approach to Exercise 3.2.3.)

We note that Fermat showed the above conditions for p to be of the form $x^2 + 2y^2$ or $x^2 + 3y^2$ are in fact sufficient. One approach is to use the fact that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3] \supset \mathbb{Z}[\sqrt{-3}]$ both have unique factorization.

Here is a special case where we easily get necessary and sufficient conditions for a prime to be of the form $x^2 + dy^2$, also known to Fermat.

Exercise 4.5.6. (i) Show that if $p = x^2 + y^2$ and $p \neq 2$, then one of x, y must be even.
(ii) Use Fermat's two square theorem to prove that p is of the form $x^2 + 4y^2$ if and only if $p \equiv 1 \bmod 4$.

You might think that use of quadratic reciprocity is actually making things more complicated than what we did in Chapter 3, but that is only because (i) we've just explored things for small d so far where things are especially simple, and (ii) in Chapter 3 I already told you for what m you should look at $x^2 + dy^2 \bmod m$. As explained above, it's really quadratic reciprocity that tells us in general for what m we want to look at congruence conditions for numbers of the form $x^2 + dy^2$.

Exercise 4.5.7. Use quadratic reciprocity (and both supplementary laws) and Proposition 4.5.2 to determine congruence conditions for when $p = x^2 + 6y^2$ can have a solution.

Exercise 4.5.8. Use quadratic reciprocity (and both supplementary laws) and Proposition 4.5.2 to show that $p = x^2 + 14y^2$ can only have a solution if $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$.

What is interesting about the last exercise is that this is one of the first examples where the necessary congruence condition on p is *not* sufficient to guarantee p is of the form $x^2 + 14y^2$. The general theory say that one also needs to check a condition mod p. In this particular case, p is of the form $x^2 + 14y^2$ if and only if $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$ and the equation $(a^2+1)^2 \equiv 8$ has a solution (in a) mod p. On the other hand, what is true (via Gauss's theory of binary quadratic forms) is that p is of the form $x^2 + 14y^2$ or of the form $2x^2 + 7y^2$ if and only if $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$.

4.6 Sums of three and four squares

Another way to generalize Fermat's two square problem is to ask what numbers are sums of k squares for $k > 2$. As mentioned in the introduction, the answer is all positive integers are sums of k squares when $k \geq 4$ by:

Theorem 4.6.1. (Lagrange's four square theorem, 1770) *Every natural number is a sum of four squares, i.e., $n = x^2 + y^2 + z^2 + w^2$ has a solution with $x, y, z, w \in \mathbb{Z}$ for all $n \in \mathbb{N}$.*

The case of two squares is harder than that of two square or four squares, but of course the great Gauss could solve it in his *Disquisitiones* when he was 21:

Theorem 4.6.2. (Gauss's three square theorem, 1801, aka Legendre's three square theorem)[4] *Any $n \in \mathbb{N}$ is a sum of three squares, i.e., $n = x^2 + y^2 + z^2$ has a solution with $x, y, z \in \mathbb{Z}$, if and only if n is not of the form $4^k(8m+7)$.*

We won't prove Gauss's three square theorem (Gauss used binary quadratic forms) but will indicate how to prove part of it. Here is the easy direction:

Proposition 4.6.3. *If n is a sum of three squares, then n is not of the form $4^k(8m+7)$.*

Proof. Suppose $n = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Z}$ but $n = 4^k(8m+7)$. Note if $k = 0$, we already know $8m + 7$ is not a sum of three squares by Exercise 3.2.4.

So we must have $k \geq 1$. Since the squares mod 4 are just 0 and 1, for $x^2 + y^2 + z^2 \equiv 0 \bmod 4$ we need x, y, z all even. (This is similar to part of Proposition 3.2.5.) Then $\frac{n}{4} = 4^{k-1}(8m+7) = (\frac{x}{2})^2 + (\frac{y}{2})^2 + (\frac{z}{2})^2$ is also sum of three squares. By descent on k, we conclude that $8m+7$ is a sum of three squares, which is a contradiction by Exercise 3.2.4. □

For the hard direction, we can at least explain how it follows when $n = p$ is prime. Suppose p is not of the form $4^k(8m+7)$. Since $4 \nmid p$, this just means $p \not\equiv 7 \bmod 8$. If $p = 2$, this is obvious. Otherwise we have $p \equiv 1, 3, 5 \bmod 8$. If $p \equiv 1, 5 \bmod 8$, then $p \equiv 1 \bmod 4$, so $p = x^2 + y^2$ for some x, y, hence $p = x^2 + y^2 + z^2$ with $z = 0$. If $p \equiv 3 \bmod 8$ (or $1 \bmod 8$), then a result of Fermat we mentioned after Exercise 4.5.4 but did not prove says

[4] Some people, including me in the past, attribute this to Legendre. He certainly claimed he had a proof, though my current understanding is his proof was not correct. At least Gauss asserted there were serious issues with his proof.

$p = x^2 + 2y^2$ for some x, y. Then $p = x^2 + y^2 + z^2$ with $z = y$. This yields Gauss's three square theorem in the case n is prime.

Then one might hope to use a composition law and some kind of converse, as in the case of sums of two squares, to get the general case. However, it is easy to see that this is not possible: if we have two primes $p \equiv 3 \bmod 8$ and $q \equiv 5 \bmod 8$, then they are both sums of three squares by the last paragraph, but their product $pq \equiv 15 \equiv 7 \bmod 8$, so is not a sum of three squares by the above proposition/Exercise 3.2.4. Hence there is no composition law in general.

However, there is a composition law for sums of four squares, which helps makes proving Lagrange's four square theorem much easier than Gauss's three square theorem. We will explain this now.

For sums of two squares, recall we proved the composition law by using the norm map on $\mathbb{Z}[i]$, and the fact that this is multiplicative. The norm map on $\mathbb{Z}[i]$ (or any imaginary quadratic ring) is simply the restriction of the (algebraic) norm map $z \mapsto z\overline{z} = |z|^2$ from $\mathbb{C}$ to $\mathbb{R}$ to our quadratic ring. (Here $\overline{z}$ denotes the complex conjugate of z.) Recall also that multiplication by $z = re^{i\theta}$ ($r \geq 0$, $\theta \in \mathbb{R}$) in $\mathbb{C}$ acts geometrically on the complex plane by radial scaling by r and rotation about 0 by θ radians.

In the first half of the 19th century, William Rowan Hamilton tried to come up with an algebraic structure (e.g., a field) analogous to $\mathbb{C}$ which is 3-dimensional over $\mathbb{R}$, in the hopes that one could understand rotations in $\mathbb{R}^3$ algebraically. Eventually, he realized that this is not possible (the fact that it is impossible is related to the fact that there is no composition law for sums of three squares), but it is possible in 4 dimensions! However, one has to work with an algebraic structure which is non-commutative.

Definition 4.6.4. *We define* **Hamilton's quaternions** $\mathbb{H}$ *to be the four-dimensional vector space with basis* $\{1, i, j, k\}$,

$$\mathbb{H} = \{x + yi + zj + wk : x, y, z, w \in \mathbb{R}\},$$

together with an associative (vector) multiplication law which is $\mathbb{R}$*-linear and satisfies*

$$i^2 = j^2 = k^2 = ijk = -1.$$

We now explain what we mean by the multiplication law. First consider multiplication of basis elements. Multiplication of anything by 1 (the basis element 1 is the same as the real number 1) should be itself: $1 \cdot \alpha = \alpha \cdot 1 = \alpha$. The rules $i^2 = j^2 = k^2 = -1$ are evident: i, j and k are (distinct) square roots of $-1 \in \mathbb{R}$. (Hence we can think of $\mathbb{R} \oplus \mathbb{R}i$, $\mathbb{R} \oplus \mathbb{R}j$ and $\mathbb{R} \oplus \mathbb{R}k$ as distinct subspaces which are all algebraically the same as $\mathbb{C}$.) These rules combined with $ijk = -1$ then tells us how to multiply any two basis elements—e.g.

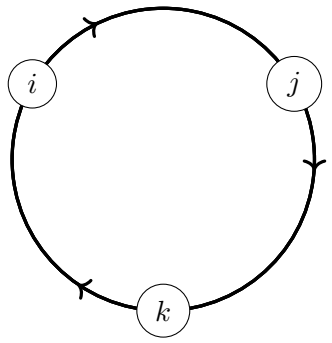
$$(ijk)k = (-1)k \implies ij(k^2) = -ij = -k \implies ij = k.$$

(Here we used that -1 commutes with each basis element, which is part of what I mean by multiplication being "$\mathbb{R}$-linear".) The following exercise tells us most of the other cases of multiplication of basis elements (with the rest being similar, which we explain with a picture below).

Exercise 4.6.1. Show $jk = i$, $ki = j$ and $ji = -ij = -k$.

In particular, the order of multiplication matters: $ij \neq ji$!

To make things easier to remember, we can visualize the multiplication table for i, j, k with the following picture:



The way to interpret this is as follows. Any of i, j, k square is -1, so say we want to multiply two distinct elements of $\{i, j, k\}$. The product will always be plus or minus the other element of $\{i, j, k\}$, and if the order of multiplication agrees with the direction of arrows in the picture, the sign is $+$, but if it disagrees, then the sign is $-$. For instance, when we multiply j and k, we will get $\pm i$. If we multiply them in the order jk, we get $+i = i$, and if we multiply them in the order kj we get $-i$.

Now we can extend this multiplication of basis elements $\{1, i, j, k\}$ to multiplication of elements of $\mathbb{H}$ in a way that is $\mathbb{R}$-linear: if $\alpha = x + yi + zj + wk$ and $\alpha' = x' + y'i + z'j + w'k$, we consider their product to be

$$\begin{aligned}\alpha\alpha' = &(x + yi + zj + wk)(x' + y'i + z'j + w'k)\\ = \;& xx' + xy'i + xz'j + x'w'k\\ &+ yx'i + yy'i^2 + yz'ij + yw'ik\\ &+ zx'j + zy'ji + zz'j^2 + zw'jk\\ &+ wx'k + wy'ki + wz'kj + ww'k^2.\end{aligned}$$

That is, we just distribute, and we are allow to commute the real numbers x, y, z, w and x', y', z', w', but we are not allowed to commute two (distinct) basis elements $\{i, j, k\}$. Then we just compute the products of the basis elements, and we can then rewrite

$$\alpha\alpha' = x'' + y''i + z''j + w''k,$$

for some $x'', y'', z'', w'' \in \mathbb{R}$. For instance, the x'' term will come from the product of basis elements of the form 1^2, i^2, j^2 and k^2, giving

$$x'' = xx' - yy' - zz' - ww'.$$

Exercise 4.6.2. In the notation above, determine y'' in terms of x, y, z, w and x', y', z', w'.

Now we can add and multiply any two elements of $\mathbb{H}$. (Contrast this with arbitrary real vector spaces, where you can only add vectors and multiply a vector with a scalar.) It is not too hard to check the following:

Proposition 4.6.5. *$\mathbb{H}$ is what is known as a* **skew field** *or a* **division ring**, *i.e., it satisfies all 6 field axioms with the sole exception of commutativity of multiplication.*

We remark that the terms skew field and division ring are interchangeable, with division ring probably being more widely used now. However, I think the term skew field is maybe more helpful to use when you are first seeing $\mathbb{H}$ to emphasize that it is like a field, i.e., like $\mathbb{R}$ or $\mathbb{C}$, only not commutative. We also remark that a structure R satisfying the 5 ring axioms with the possible exception of commutativity of multiplication is called a **noncommutative ring**. Skew fields (i.e., division rings) are special cases of noncommutative rings. When $n \geq 2$, the set of $n \times n$ matrices $M_n(\mathbb{R})$ (or $M_n(\mathbb{C})$) is an example of a noncommutative ring which is not a division ring.

Exercise 4.6.3. Show $M_2(\mathbb{R})$ is not a division ring. (Thus $M_2(\mathbb{R})$ is a different 4-dimensional algebraic structure than $\mathbb{H}$.)

Definition 4.6.6. *For $\alpha = x + yi + zj + wk \in \mathbb{H}$, we define the* **conjugate** *of α to be*

$$\overline{\alpha} = x - yi - zj - wk,$$

and the **norm** *of α to be*

$$N(\alpha) = \alpha\overline{\alpha} = x^2 + y^2 + z^2 + w^2.$$

Thus the norm map is defined $N : \mathbb{H} \to \mathbb{R}_{\geq 0}$.

Exercise 4.6.4. Check that for $\alpha = x + yi + zj + wk \in \mathbb{H}$, we indeed have $\alpha\overline{\alpha} = x^2 + y^2 + z^2 + w^2$.

Exercise 4.6.5. Let $\alpha = x + yi + zj + wk$ and $\beta = x' + y'i + z'j + w'k$ in $\mathbb{H}$, and write $\alpha = x + \alpha_0$, $\beta = x' + \beta_0$ where $\alpha_0 = yi + zj + wk$ and $\beta_0 = y'i + z'j + w'k$.
(i) Show $\overline{\alpha_0\beta_0} = \overline{\beta}_0 \cdot \overline{\alpha}_0$.
(ii) Deduce that $\overline{\alpha\beta} = \overline{\beta} \cdot \overline{\alpha}$.

Proposition 4.6.7. *Let $\mathbb{Z}[i,j,k] = \{x + yi + zi + wk \in \mathbb{H} : x, y, z, w \in \mathbb{Z}\}$.*
(i) For $n \in \mathbb{Z}$, we have n is a sum of four squares if and only if n is a norm from $\mathbb{Z}[i,j,k]$.
(ii) **(Composition law)** *If m and n are sums of four squares, so is mn.*

Proof. (i) This is obvious as $N(x+yi+zi+wk) = x^2+y^2+z^2+w^2$.

(ii) Suppose m and n are sums of four squares, so $m = N(\alpha)$ and $n = N(\beta)$ for some $\alpha, \beta \in \mathbb{Z}[i,j,k]$. Then from the previous exercise

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha(\beta\overline{\beta})\overline{\alpha} = N(\beta)\alpha\overline{\alpha} = N(\alpha)N(\beta).$$

(Here we used the fact that $N(\alpha), N(\beta) \in \mathbb{R}$, so they commute with everything.) Thus the norm map is multiplicative, which implies (ii) in light of (i). □

Now by the composition, proving Lagrange's four square theorem reduces to the following:

Proposition 4.6.8. *Let $p \in \mathbb{N}$ be prime. Then p is a sum of four squares.*

The proof will use the following fact, which we will take for granted. As in the case of commutative rings, we will call an nonzero element of $u \in \mathbb{Z}[i,j,k]$ a **unit** if the inverse of $u \in \mathbb{H}$ also lies in $\mathbb{Z}[i,j,k]$. It is easy to see from multiplicativity of the norm on $\mathbb{H}$ that u being a unit is equivalent to $N(u) = 1$. We say a non-zero nonunit $\alpha \in \mathbb{Z}[i,j,k]$ is **reducible** if there exist $\beta, \gamma \in \mathbb{Z}[i,j,k]$ which are both nonzero non-units such that $\alpha = \beta\gamma$, and **irreducible** otherwise.

Theorem 4.6.9. *The non-commutative ring $\mathbb{Z}[i,j,k]$ satisfies the following weak prime divisor property: if $\pi \in \mathbb{Z}[i,jk]$ is an irreducible with odd norm, and $\pi | \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i,j,k]$, then $\pi|\alpha$ or $\pi|\beta$.*

(I haven't exactly said what I mean by $\pi|\alpha$—some thought is merited since $\mathbb{Z}[i,j,k]$ is non-commutative, but we'll only apply this notion to $p|\alpha$ with $p \in \mathbb{N}$ below, and since p commutes with everything in $\mathbb{Z}[i,j,k]$, this is not an issue.)

Proof of Proposition. Clearly $2 = 1^2+1^2+0^2+0^2$, so assume p is odd. Then, because squaring is a 2-to-1 map on $(\mathbb{Z}/p\mathbb{Z})^\times$, including 0 mod p there are precisely $\frac{p+1}{2}$ squares mod p (this was Exercise 4.4.1). Hence the map $x \mapsto -1-x^2$ on $\mathbb{Z}/p\mathbb{Z}$ takes exactly $\frac{p+1}{2}$ values. But as there only $\frac{p-1}{2}$ nonsquares mod p, at least one of these values must be a square. That is, for some $x, y \in \mathbb{Z}$, $-1-x^2 \equiv y^2 \bmod p$, i.e., $p|(x^2+y^2+1)$. (This fact is another lemma of Lagrange, similar to Lemma 4.1.4.)

For x, y as above, consider $\alpha = x+yi+j \in \mathbb{Z}[i,j,k]$. Then

$$p|(x^2+y^2+1) = N(\alpha) = \alpha\overline{\alpha} = (x+yi+j)(x-yi-j).$$

Note that $\frac{x\pm yi\pm j}{p} \notin \mathbb{Z}[i,j,k]$, hence p does not divide α or $\overline{\alpha}$. By the (weak) prime divisor property in $\mathbb{Z}[i,j,k]$, this means that p must be reducible in $\mathbb{Z}[i,j,k]$, so we can write $p = \beta\gamma$ for β, γ nonzero non-units. Then

$$p^2 = N(p) = N(\beta\gamma) = N(\beta)N(\gamma).$$

Since $N(\beta)$ and $N(\gamma)$ are positive integers greater than 1, and p is prime in $\mathbb{N}$, we must have $N(\beta) = N(\gamma) = p$. In particular, p is a norm from $\mathbb{Z}[i,j,k]$, so a sum of four squares by the previous proposition. □

The numbers in $\mathbb{Z}[i,j,k]$ are called the **Lipschitz integers**. There is actually a larger set of "quaternion integers" one can work with, the **Hurwitz integers**

$$\left\{ \frac{x+yi+zj+wk}{2} : x,y,z,w \in \mathbb{Z},\ x \equiv y \equiv z \equiv w \bmod 2 \right\}.$$

(The Hurwitz integers are obtained from the Lipschitz integers by adjoining the element $\frac{1+i+j+k}{2}$.) One way of proving the Lipschitz integers satisfy the above weak prime divisor property is to first prove the Hurwitz integers satisfy the usual prime divisor property (i.e., one need not assume $N(\pi)$ is odd). This can be done by showing the Hurwitz integers possess the division property (and thus a Euclidean algorithm). (The Lipschitz integers do not satisfy the division property.) Consequently, sometimes people say that the Hurwitz integers have "unique factorization," but one needs to be more careful what one means because the order of factorization matters. See, e.g., [CS03]. (We could also present the above proof in terms of Hurwitz integers rather than Lipschitz integers, as in [Sti03] or [Mara, Ch 8].)

Anyway, we will not prove Theorem 4.6.9. The point of the above was to show that one can prove Lagrange's four square theorem using a similar approach to our proof of Fermat's two square theorem. Also, the quaternions are an interesting mathematical object. It turns out they can be used to achieve Hamilton's original goal of getting an algebraic way of treating 3-dimensional geometry. In particular, they provide an algebraic way of studying rotations in $\mathbb{R}^3$, and thus are useful in physics and engineering. One can also use the quaternions to give a proof of Gauss's three square theorem.

There are various other proofs of the four square theorem. For instance, in my earlier notes [Mara, Ch 8] I sketch out a geometric proof as well as an analytic proof.

You might also wonder about other algebraic structures beyond quaternions giving more composition laws. In fact there are such structures. For instance, there are the 8-dimensional **octonions**, which allow one to prove a composition law for sums of 8 squares. However, similar to how we lost commutativity going from $\mathbb{C}$ to $\mathbb{H}$, when you move to the octonions, you lose associativity (which is bad, but not quite as bad as it sounds at first).

Exercise 4.6.6. In the above proof we only worked with α of the form $x+yi+zj$, which has norm $x^2+y^2+z^2$. Why does the argument not imply that any prime p is a sum of three squares?

Exercise 4.6.7. How many units are there in the Lipschitz integers? What about the Hurwitz integers?