Math 332 Winter 2023, Lecture 17: Rings

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

1. Rings and ideals (cont'd)

1.14. An introduction to divisibility theory (cont'd)

1.14.7. Irreducible and prime elements (cont'd)

Recall one of the definitions from Lecture 16:

Definition 1.14.13. Let R be a commutative ring. Let $r \in R$ be nonzero and not a unit.

(a) We say that r is **irreducible** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $ab = r$, at least one of a and b is a unit.

(b) We say that r is **prime** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $r \mid ab$, we have $r \mid a$ or $r \mid b$.

Both of these notions "irreducible" and "prime" generalize prime numbers (up to sign).

The following connection between "irreducible" and "prime" has already been noticed in Lecture 16:

Proposition 1.14.15. Let R be an integral domain. Then, any prime element of R is irreducible.

In a PID (= integral domain where each ideal is principal), this goes both ways:

Proposition 1.14.16. Let R be a PID (for example, a Euclidean domain). Let $r \in R$. Then, r is prime if and only if r is irreducible.

One proof of this proposition is given in the text (Proposition 2.15.4); we shall give another. This latter proof will rely on the following two general lemmas:

Lemma 1.14.17. Let R be an integral domain. Let $a, b, c \in R$ be such that $a \neq 0$. If $ab \mid ac$, then $b \mid c$.

Proof. Assume that $ab \mid ac$. In other words, $ac = abr$ for some $r \in R$. Consider this r. We have $a(c - br) = ac - abr = 0$ (since $ac = abr$). Since R is an integral domain, we thus conclude that $c - br = 0$ (since $a \neq 0$). In other words, $c = br$. This entails that $b \mid c$. Thus, Lemma 1.14.17. □

Lemma 1.14.18. Let R be an integral domain. Let $a, b, c \in R$ be such that $a \neq 0$. Assume that the elements ab and ac have a gcd g. Then, the elements b and c have a gcd h such that $g = ah$.

Proof. The element a is a common divisor of ab and ac (obviously), and thus must divide g (by the definition of a gcd, since g is a gcd of ab and ac). In other words, there exists some $r \in R$ such that $g = ar$. Consider this r.

Since g is a gcd of ab and ac, we have $g \mid ab$ and $g \mid ac$. From $ar = g \mid ab$, we obtain $r \mid b$ (by Lemma 1.14.17, applied to r and b instead of b and c). Similarly, $r \mid c$. Thus, r is a common divisor of b and c.

Now, let s be any common divisor of b and c. Then, $s \mid b$, so that $b = sb'$ for some $b' \in R$. This b' then satisfies $a \underbrace{b}_{=sb'} = asb'$, so that $as \mid ab$. Similarly, $as \mid ac$. Hence, as is a common divisor of ab and ac. Therefore, as divides g (since g is a gcd of ab and ac). In other words, $as \mid g = ar$. Hence, Lemma 1.14.17 (applied to s and r instead of b and c) yields $s \mid r$.

Forget that we fixed s. We thus have shown that any common divisor s of b and c satisfies $s \mid r$. In other words, any common divisor of b and c divides r. Since we also know that r is a common divisor of b and c, we thus conclude that r is a gcd of b and c (by the definition of a gcd). Hence, the elements b and c have a gcd h such that $g = ah$ (namely, $h = r$), since we know that $g = ar$. This proves Lemma 1.14.18. □

Proof of Proposition 1.14.16. $\Longrightarrow$: This follows from Proposition 1.14.15.

$\Longleftarrow$: Assume that r is irreducible. We must prove that r is prime.

So let $a, b \in R$ be such that $r \mid ab$. We must show that $r \mid a$ or $r \mid b$.

If $a = 0$, then this is obvious (since $r \mid 0$). Thus, we WLOG assume that $a \neq 0$.

Theorem 1.14.11 in Lecture 16 shows that ab and ar have a gcd in R. Let g be this gcd. Then, $g \mid ab$ and $g \mid ar$.

We have $r \mid ab$ (by assumption) and $r \mid ar$ (obviously). Hence, r is a common divisor of ab and ar. Thus, r divides g (by the definition of a gcd, since g is a gcd of ab and ar). That is, $r \mid g$.

Lemma 1.14.18 (applied to $c = r$) yields that the elements b and r have a gcd h such that $g = ah$. Consider this h. Since h is a gcd of b and r, we have $h \mid b$ and $h \mid r$.

In particular, $h \mid r$. In other words, there exists some $k \in R$ such that $r = kh$. Consider this k.

So we have $kh = r$. Since r is irreducible, this entails that at least one of the elements k and h is a unit (by the definition of "irreducible"). Thus, we are in one of the following cases:

Case 1: The element k is a unit.

Case 2: The element h is a unit.[1]

[1] Cases 1 and 2 cannot overlap, because if k and h were both units, then their product $kh = r$ would be a unit as well, but r is irreducible and thus not a unit. But we don't care about this, since cases in a proof can overlap.

Let us first consider Case 1. In this case, the element k is a unit. Hence, k has an inverse k^{-1}. From $r = kh$, we thus obtain $h = rk^{-1}$, so that $r \mid h \mid b$. Thus, $r \mid a$ or $r \mid b$. So we are done in Case 1.

Let us next consider Case 2. In this case, the element h is a unit. Hence, h has an inverse h^{-1}. From $g = ah$, we thus obtain $a = gh^{-1}$. Thus, $g \mid a$. Hence, $r \mid g \mid a$. Thus, $r \mid a$ or $r \mid b$. So we are done in Case 2.

Hence, in both cases, we have shown that $r \mid a$ or $r \mid b$. As we explained, this completes the proof of the "$\Longleftarrow$" direction of Proposition 1.14.16. □

1.14.8. Irreducible factorizations and UFDs

The following theorem generalizes the classical "Fundamental Theorem of Arithmetic" (i.e., the fact that each positive integer has a prime factorization, which is unique up to reordering the factors):

Theorem 1.14.19. Let R be a PID. Then, any nonzero element $r \in R$ can be decomposed (up to associates) into a product of irreducible (i.e., prime) elements of R. Moreover, this product is unique up to order and associateness.

In detail: Let $r \in R$ be a nonzero element. Then, there is a tuple $(p_1, p_2, \ldots, p_n)$ of irreducible (i.e., prime) elements of R such that

$$r \sim p_1 p_2 \cdots p_n.$$

If $(p_1, p_2, \ldots, p_n)$ and $(q_1, q_2, \ldots, q_m)$ are two such tuples, then $(p_1, p_2, \ldots, p_n)$ can be obtained from $(q_1, q_2, \ldots, q_m)$ by reordering the entries and replacing them by associate entries.

Proof. See a textbook, e.g., [DumFoo04, §8.3, Theorem 14] or [Knapp16, Theorem 8.15]. Just a few words about the proof:

Uniqueness is proved just as for integers.

Existence is tricky: Just as for integers, you start with r and keep factoring it further and further (avoiding unit factors) until no more divisors remain. But you have to argue that this factoring process won't go on forever, and this is no longer as easy as for integers. (It is easy when R has a "multiplicative norm", i.e., a map $N : R \to \mathbb{N}$ such that $N(a) < N(ab)$ whenever $a, b \in R$ are nonzero and b is not a unit. For example, if $R = \mathbb{Z}[i]$, then the Euclidean norm $N : \mathbb{Z}[i] \to \mathbb{N}$ defined by $N(a + bi) = a^2 + b^2$ has this property.) □

Integral domains R in which the claim of Theorem 1.14.19 holds are called **UFDs** (short for **unique factorization domains**). This class is wider than the PIDs. For instance, the polynomial rings $\mathbb{Z}[x]$ (the ring of all univariate polynomials in x with integer coefficients) and $\mathbb{Q}[x, y]$ (the ring of all polynomials in two variables x and y with rational coefficients) are UFDs but not PIDs.

We will not focus on UFDs in this course, but we briefly note that they have some (but not all) of the nice properties of PIDs. In particular, in a UFD, any two elements have a gcd and an lcm. (But we shall not prove this.)

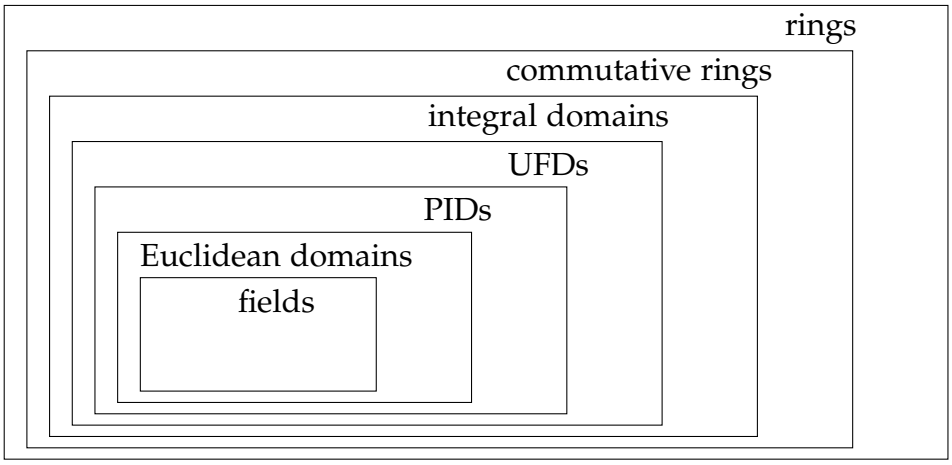
1.14.9. A synopsis

The following corollary combines several results we have seen above in a convenient hierarchy:

Corollary 1.14.20. We have

$$\{\text{fields}\} \subseteq \{\text{Euclidean domains}\} \subseteq \{\text{PIDs}\} \subseteq \{\text{UFDs}\}$$
$$\subseteq \{\text{integral domains}\} \subseteq \{\text{commutative rings}\} \subseteq \{\text{rings}\}.$$

Let us illustrate this hierarchy in a symbolic picture:



All the "$\subseteq$" signs in Corollary 1.14.20 are strict inclusions; let us briefly recall some examples showing this:

- The rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{-2}\right]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ and the polynomial ring $\mathbb{Q}[x]$ are Euclidean domains, but not fields.
- The ring $\mathbb{Z}[\alpha]$ for $\alpha = \dfrac{1+\sqrt{-19}}{2}$ is a PID, but not a Euclidean domain.
- The polynomial rings $\mathbb{Q}[x,y]$ and $\mathbb{Z}[x]$ are UFDs, but not PIDs.
- The rings $\mathbb{Z}[2i]$ and $\mathbb{Z}\left[\sqrt{-3}\right]$ are integral domains, but not UFDs.
- The ring $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$ is a commutative ring, but not an integral domain.
- The matrix ring $\mathbb{Q}^{2\times 2}$ and the ring of quaternions $\mathbb{H}$ are not commutative.

1.15. Application: Fermat's $p = x^2 + y^2$ theorem

As an application of some of the above, we will show a result of Fermat:

Theorem 1.15.1 (Fermat's two-squares theorem)**.** Let p be a prime number[2] such that $p \equiv 1 \bmod 4$. Then, p can be written as a sum of two perfect squares.

For example,

$$5 = 1^2 + 2^2;$$
$$13 = 2^2 + 3^2;$$
$$17 = 1^2 + 4^2;$$
$$29 = 2^2 + 5^2.$$

I will prove Theorem 1.15.1 using rings (specifically, the ring $\mathbb{Z}/p$ of residue classes and the ring $\mathbb{Z}[i]$ of Gaussian integers). The first ingredient of the proof is a curious fact about primes, known as **Wilson's theorem**:

Theorem 1.15.2 (Wilson's theorem)**.** Let p be a prime. Then, $(p-1)! \equiv -1 \bmod p$.

Proof. We must show that $\overline{(p-1)!} = \overline{-1}$ in $\mathbb{Z}/p$.

In $\mathbb{Z}/p$, we have

$$\overline{(p-1)!} = \overline{1 \cdot 2 \cdot \cdots \cdot (p-1)} = \overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1}. \tag{1}$$

Recall that every ring R has a group of units, which is denoted by $R^\times$. (Its elements are the units of R, and its operation is multiplication.) Since the ring $\mathbb{Z}/p$ is a field (because p is prime), its group of units $(\mathbb{Z}/p)^\times$ consists of all nonzero elements of $\mathbb{Z}/p$. Thus,

$$(\mathbb{Z}/p)^\times = \left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\},$$

with all the $p-1$ elements $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ being distinct. Hence, the product of all units of $\mathbb{Z}/p$ is

$$\prod_{a \in (\mathbb{Z}/p)^\times} a = \overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1}.$$

Comparing this with (1), we find

$$\overline{(p-1)!} = \prod_{a \in (\mathbb{Z}/p)^\times} a. \tag{2}$$

[2] in the sense of classical number theory, i.e., an integer $p > 1$ with no positive divisors other than 1 and p

Now, recall that any unit a of $\mathbb{Z}/p$ (or of any other ring) has an inverse a^{-1}, which is also a unit and satisfies $\left(a^{-1}\right)^{-1} = a$. Thus, the units of $\mathbb{Z}/p$ can be paired up in pairs $\left\{a, a^{-1}\right\}$ consisting of a unit a and its inverse a^{-1}. The only units left unpaired will be the units that are their own inverses. These units are the elements $a \in \mathbb{Z}/p$ that satisfy $a^2 = \overline{1}$, and a moment of thought reveals that they are $\overline{1}$ and $\overline{-1}$ (because $a^2 = \overline{1}$ entails $0 = a^2 - \overline{1} = \left(a - \overline{1}\right)\left(a + \overline{1}\right)$, and since $\mathbb{Z}/p$ is an integral domain, this equality can only hold if either $a - \overline{1}$ or $a + \overline{1}$ is 0). Thus, all units other than $\overline{1}$ and $\overline{-1}$ are paired. Hence, in the product of all units of $\mathbb{Z}/p$, we can pair up each factor other than $\overline{1}$ and $\overline{-1}$ with its inverse:

$$\prod_{a \in (\mathbb{Z}/p)^\times} a = \underbrace{\left(a_1 \cdot a_1^{-1}\right)}_{=1} \cdot \underbrace{\left(a_2 \cdot a_2^{-1}\right)}_{=1} \cdot \cdots \cdot \underbrace{\left(a_k \cdot a_k^{-1}\right)}_{=1} \cdot \overline{1} \cdot \overline{-1} = \overline{-1}.$$

Hence, (2) can be rewritten as $\overline{(p-1)!} = \overline{-1}$, which means precisely that $(p-1)! \equiv -1 \bmod p$. This proves Theorem 1.15.2.

(Caution: The above argument breaks down a bit for $p = 2$, but this case is trivial anyway.) □

Corollary 1.15.3. Let p be an odd prime (i.e., a prime distinct from 2). Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Then, $u!^2 \equiv -(-1)^u \bmod p$.

Proof. Theorem 1.15.2 yields

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

However,

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdot \cdots \cdot (p-1) \\
&= \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \cdot \left(\underbrace{\left(\frac{p-1}{2}+1\right)}_{\equiv -\frac{p-1}{2} \bmod p} \cdot \cdots \cdot \underbrace{(p-2)}_{\equiv -2 \bmod p} \cdot \underbrace{(p-1)}_{\equiv -1 \bmod p} \right) \\
&\equiv \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \cdot \left(\left(-\frac{p-1}{2}\right) \cdot \cdots \cdot (-2) \cdot (-1)\right) \\
&= (1 \cdot 2 \cdot \cdots \cdot u) \cdot \underbrace{((-u) \cdot \cdots \cdot (-2) \cdot (-1))}_{\substack{=(-1)^u \cdot (u \cdots 2 \cdot 1) \\ =(-1)^u \cdot (1 \cdot 2 \cdots u)}} \qquad \left(\text{since } \frac{p-1}{2} = u\right) \\
&= (1 \cdot 2 \cdot \cdots \cdot u) \cdot (-1)^u \cdot (1 \cdot 2 \cdot \cdots \cdot u) \\
&= (-1)^u \cdot \left(\underbrace{1 \cdot 2 \cdot \cdots \cdot u}_{=u!}\right)^2 = (-1)^u \cdot u!^2 \bmod p,
\end{aligned}$$

so that

$$(-1)^u \cdot u!^2 \equiv (p-1)! \equiv -1 \bmod p.$$

Multiplying both sides of this congruence by $(-1)^u$, we obtain

$$u!^2 \equiv -(-1)^u \bmod p.$$

This proves Corollary 1.15.3. □

Corollary 1.15.4. Let p be a prime such that $p \equiv 1 \bmod 4$. Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Then, $u!^2 \equiv -1 \bmod p$.

Proof. Apply Corollary 1.15.3, and observe that $(-1)^u = 1$ (since $p \equiv 1 \bmod 4$, so that u is even). Corollary 1.15.4 follows. □

Corollary 1.15.4 brings us somewhat closer to our goal: Its claim $u!^2 \equiv -1 \bmod p$ can be rewritten as $p \mid u!^2 + 1 = u!^2 + 1^2$. Now, if we could somehow turn this divisibility into an equality...

Of course, we cannot do this directly. But let us recall the Gaussian integers and their ring $\mathbb{Z}[i]$. In this ring, the equality $p = u!^2 + 1^2$ can be rewritten as $p = (u! + i)(u! - i)$, which is promising.

To get any mileage out of this, we recall our favorite Euclidean norm N on $\mathbb{Z}[i]$. This is the map

$$\begin{aligned} N : \mathbb{Z}[i] &\to \mathbb{N}, \\ a+bi &\mapsto a^2+b^2 = |a+bi|^2 \qquad (\text{for } a,b \in \mathbb{Z}). \end{aligned}$$

It has a further nice property (which is not part of its Euclideanness):

Proposition 1.15.5. We have

$$N(\alpha\beta) = N(\alpha)\,N(\beta) \qquad \text{for any } \alpha,\beta \in \mathbb{Z}[i].$$

Proof. Straightforward computation (write α as $\alpha = a+bi$ and write β as $\beta = c+di$, and multiply). □

Corollary 1.15.6. Let α and β be two Gaussian integers such that $\alpha \mid \beta$ in $\mathbb{Z}[i]$. Then, $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$.

Proof. We have $\beta = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[i]$ (since $\alpha \mid \beta$). This γ then satisfies $N(\beta) = N(\alpha\gamma) = N(\alpha)\,N(\gamma)$ (by Proposition 1.15.5). Profit. □

Corollary 1.15.7. The units of $\mathbb{Z}[i]$ are exactly the elements $\alpha \in \mathbb{Z}[i]$ satisfying $N(\alpha) = 1$, and these elements are precisely 1, i, -1, $-i$.

Proof. Easy exercise (specifically, [21w, homework set #2, Exercise 6 **(d)**]). The fact that the Gaussian integers 1, i, -1, $-i$ are the only elements $\alpha \in \mathbb{Z}[i]$ satisfying $N(\alpha) = 1$ is easily checked (what are the integer solutions of the equations $x^2+y^2=1$) ? Clearly, these elements are units. Conversely, any unit α of $\mathbb{Z}[i]$ satisfies $\alpha \mid 1$ in $\mathbb{Z}[i]$ and therefore $N(\alpha) \mid N(1)$ in $\mathbb{Z}$ (by Corollary 1.15.6), which means $N(\alpha) \mid N(1) = 1$ and therefore $N(\alpha) = 1$. □

Lemma 1.15.8. Let α and β be Gaussian integers such that $\alpha \neq 0$. Then, $\alpha \mid \beta$ in $\mathbb{Z}[i]$ if and only if $\dfrac{\beta}{\alpha} \in \mathbb{Z}[i]$.

Proof. Trivial. □

We are now ready to prove Fermat's two-squares theorem:

Proof of Theorem 1.15.1. Let $u = \dfrac{p-1}{2}$. This $u \in \mathbb{N}$ since p is odd. Furthermore, Corollary 1.15.4 yields $u!^2 \equiv -1 \bmod p$. Thus, $p \mid u!^2+1$ in $\mathbb{Z}$, so that $p \mid u!^2+1 = (u!+i)(u!-i)$ in $\mathbb{Z}[i]$.

However, $p \nmid u!+i$ (by Lemma 1.15.8), since $\dfrac{u!+i}{p} = \dfrac{u!}{p} + \dfrac{1}{p}i \notin \mathbb{Z}[i]$. Similarly, $p \nmid u!-i$.

Thus, p divides a product of two elements of $\mathbb{Z}[i]$ (namely, the product of $u! + i$ and $u! - i$), but does not divide any of the two factors. This shows that p is not prime in $\mathbb{Z}[i]$. But $\mathbb{Z}[i]$ is a PID, and thus the prime elements of $\mathbb{Z}[i]$ are precisely the irreducible elements of $\mathbb{Z}[i]$ (by Proposition 1.14.16). Therefore, p is not irreducible in $\mathbb{Z}[i]$. In other words, p can be written as $p = ab$ for two non-units a and b of $\mathbb{Z}[i]$. Consider these non-units a and b.

From $p = ab$, we obtain

$$N(p) = N(ab) = N(a)\,N(b) \qquad \text{(by Proposition 1.15.5)},$$

so that

$$N(a)\,N(b) = N(p) = p^2 + 0^2 = p^2.$$

Since $N(a)$ and $N(b)$ are nonnegative integers, this entails that we have

$$\begin{aligned}&\text{either } \Big(N(a) = 1 \text{ and } N(b) = p^2\Big)\\ &\text{or } \big(N(a) = p \text{ and } N(b) = p\big)\\ &\text{or } \Big(N(a) = p^2 \text{ and } N(b) = 1\Big)\end{aligned}$$

(because the Fundamental Theorem of Arithmetic shows that the only ways to decompose p^2 as a product of two nonnegative integers are $1 \cdot p^2$ and $p \cdot p$ and $p^2 \cdot 1$). However, the first of these three options is impossible (because $N(a) = 1$ would force a to be a unit[3], contradicting the fact that a is a non-unit). Similarly, the third option is impossible. Hence, the second option must hold. In other words, we have $N(a) = p$ and $N(b) = p$.

Now, write the Gaussian integer a as $a = x + yi$ for $x, y \in \mathbb{Z}$. Then, the definition of N yields $N(a) = x^2 + y^2$, so that $x^2 + y^2 = N(a) = p$. Thus, Theorem 1.15.1 is proved! □

Theorem 1.15.1 is the tip of a deep iceberg, which took several centuries to explore (and still appears to be less than fully mapped). The most obvious next step is extending it to non-primes:

Theorem 1.15.9. Let n be a positive integer with prime factorization $n = 2^a p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes larger than 2, and where $a, b_1, b_2, \ldots, b_k$ are nonnegative integers. (In particular, if n is odd, then $a = 0$.)

Then:

(a) The number n can be written as a sum of two perfect squares if and only if the following condition holds: For each $i \in \{1, 2, \ldots, k\}$ satisfying $p_i \equiv 3 \bmod 4$, the exponent b_i is even.

[3] by Corollary 1.15.7

(b) If this condition holds, then the number of ways to write n as a sum of two perfect squares (to be more precise: the number of pairs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfying $n = x^2 + y^2$) is $4 \cdot \prod_{\substack{i \in \{1,2,\ldots,k\}; \\ p_i \equiv 1 \bmod 4}} (b_i + 1)$.

For a proof of this theorem, see [Grinbe19, Theorem 4.2.62] or [DumFoo04, §8.1, Corollary 19]. (The proof again uses Gaussian integers in a rather neat way. Actually, proving the "if" part of Theorem 1.15.9 **(a)** is a neat exercise[4].)

More about decompositions of integers into sums of perfect squares can be found

- in [DumFoo04, §8.3];
- in Keith Conrad's `https://kconrad.math.uconn.edu/math5230f12/handouts/Zinotes.pdf` ;
- in [Grinbe19, §4.2].

Instead of writing integers n in the form $n = x^2 + y^2$, we can try to write them in the form $x^2 + 2y^2$ or $x^2 + 3y^2$ or $x^2 + 4y^2$ or $x^2 + 5y^2$ or $x^2 + xy + y^2$ or $\left|x^2 - 2y^2\right|$ or many other such forms. Each time, we can ask when this is possible, and how many ways there are. These questions vary widely in difficulty, and even their most basic variants (which prime numbers can be written in a given form?) can be extremely hard. A whole book [Cox22] has been written entirely about the question of writing prime(!) numbers in the form $x^2 + ny^2$ for positive integers n; just answering these questions for different n requires rather advanced mathematics. Here is a summary of answers for certain values of n (see [Cox22] for proofs of these and many more results):

Theorem 1.15.10. Let p be a prime number.

(a) We can write p in the form $p = x^2 + y^2$ with $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

(b) We can write p in the form $p = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 3 \bmod 8$. (The notation "$p \equiv 1, 3 \bmod 8$" is shorthand for "p is congruent to 1 or to 3 modulo 8". Similar shorthands will be used in the following parts.)

(c) We can write p in the form $p = x^2 + 3y^2$ with $x, y \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \bmod 3$.

(d) We can write p in the form $p = x^2 + 4y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$.

(e) We can write p in the form $p = x^2 + 5y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 9 \bmod 20$.

[4] Keep in mind that 0 is a perfect square.

(f) We can write p in the form $p = x^2 + 6y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 7 \bmod 24$.

(g) We can write p in the form $p = x^2 + 14y^2$ with $x, y \in \mathbb{Z}$ if and only if we have $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$ and there exists some integer z satisfying $\left(z^2+1\right)^2 \equiv 8 \bmod p$.

(h) We can write p in the form $p = x^2 + 27y^2$ with $x, y \in \mathbb{Z}$ if and only if we have $p \equiv 1 \bmod 3$ and there exists some integer z satisfying $z^3 \equiv 2 \bmod p$.

Part **(a)** of Theorem 1.15.10 follows from Theorem 1.15.1 and its fairly easy converse. Parts **(b)** and **(d)** are exercises in the text, so can be done with fairly elementary methods. (Actually, you can prove part **(d)** right now, using nothing but part **(a)** and a bit of thought.) Part **(c)** looks superficially similar, but is significantly harder to prove since $\mathbb{Z}\left[\sqrt{-3}\right]$ is not a PID (or even a UFD); nevertheless, fairly elementary proofs exist[5]. Part **(e)** is proved using genus theory of quadratic forms in [Cox22, (2.22)]. Part **(f)** requires class field theory ([Cox22, Theorem 5.33]). Parts **(g)** and **(h)** can be proved using elliptic functions from complex analysis ([Cox22, Chapters 2 and 3]). Note the additional "there exists some integer z" conditions in parts **(g)** and **(h)**; such conditions can be avoided for $x^2 + ny^2$ when n is small, but eventually become necessary. See `https://mathoverflow.net/questions/79342/` for more about the need for such conditions, and see [Cox22, Chapters 2 and 3] for their exact nature.

We can also ask about sums of more than two squares. Lagrange proved that every nonnegative integer can be written as a sum of **four** squares (that is, each $n \in \mathbb{N}$ can be written as $n = x^2 + y^2 + z^2 + w^2$ for some $x, y, z, w \in \mathbb{Z}$). These days, one of the shortest proofs of this fact uses the so-called *Hurwitz quaternions* – a quaternion analogue of Gaussian integers. See `https://en.wikipedia.org/wiki/Lagrange's_four-square_theorem` or [Haensc16] or [Schwar14] for the proof.

References

[21w] Darij Grinberg, *Math 533: Abstract Algebra I, Winter 2021*. `https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

[Cox22] David A. Cox, *Primes of the form $x^2 + ny^2$*, AMS Chelsea Publishing **387**, 3rd edition, AMS 2022.

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.
See `https://site.uvm.edu/rfoote/files/2022/06/errata_3rd_edition.pdf` for errata.

[5] See, e.g., `https://math.stackexchange.com/a/76917/` for one such proof.

[Grinbe19] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf

[Haensc16] Anna Haensch, *Quaternions and the four-square theorem*, 2016.
https://www.mathcs.duq.edu/~haensch/411Materials/Quaternions.pdf

[Knapp16] Anthony W. Knapp, *Basic Algebra*, Digital 2nd edition 2016.
http://www.math.stonybrook.edu/~aknapp/download.html

[Schwar14] Rich Schwartz, *Math 153: The Four Square Theorem*, April 12, 2014.
https://www.math.brown.edu/reschwar/M153/lagrange.pdf