Math 533 Winter 2021, Lecture 5: Rings and ideals

website: `https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

1. Rings and ideals (cont'd)

1.1. The Chinese Remainder Theorem ([DF, §7.6]) (cont'd)

Last time, we have stated the following result, which we have not proved yet:

> **Theorem 1.1.1** (The Chinese Remainder Theorem for two ideals)**.** Let I and J be two comaximal ideals of a commutative ring R. (Recall that "comaximal" means that $I + J = R$.) Then:
>
> **(a)** We have $I \cap J = IJ$.
>
> **(b)** We have $R/(IJ) \cong (R/I) \times (R/J)$.
>
> **(c)** More precisely, there is a ring isomorphism
>
> $$R/(IJ) \to (R/I) \times (R/J)$$
>
> that sends each residue class $r + IJ$ to the pair $(r + I, r + J)$.

Let us now prove this. Before we do so, let us agree on a convention that will save us some parentheses:

> **Convention 1.1.2.** The "/" sign will have higher precedence than the "×" sign, but lower precedence than the "implied · sign". Thus, the expression "$(R/I) \times (R/J)$" can be abbreviated as "$R/I \times R/J$" (without worrying that it might be misunderstood as "$R/(I \times R)/J$", whatever this would mean), and similarly the expression "$R/(IJ)$" can be abbreviated as "R/IJ" (without worrying that it might be misunderstood as "$(R/I)J$").

Proof of Theorem 1.1.1. We have $1 \in R = I + J$ (since I and J are comaximal). In other words, there exist $i \in I$ and $j \in J$ with $1 = i + j$. Consider these i and j.

(a) We know that $IJ \subseteq I \cap J$ (see homework set #1 Exercise 8 **(b)**); thus, we only need to show that $I \cap J \subseteq IJ$.

So let $a \in I \cap J$. Thus, $a \in I$ and $a \in J$. Now,

$$a = a \cdot \underbrace{1}_{=i+j} = a \cdot (i + j) = \underbrace{ai}_{\substack{=ia \in IJ \\ \text{(since } i \in I \text{ and } a \in J)}} + \underbrace{aj}_{\substack{\in IJ \\ \text{(since } a \in I \text{ and } j \in J)}} \in IJ + IJ = IJ.$$

(The last equality relied on the fact that $K + K = K$ for any ideal K of R. This is an easy consequence of the fact that K is a subgroup of the additive group $(R, +, 0)$.)

Forget that we fixed a. We thus have shown that $a \in IJ$ for each $a \in I \cap J$. In other words, $I \cap J \subseteq IJ$. As we said above, this completes the proof of part **(a)**.

(c) Consider the map[1]

$$\begin{aligned} f : R &\to R/I \times R/J, \\ r &\mapsto (r + I, r + J) . \end{aligned}$$

It is straightforward to see that this map f is a ring morphism (from R to the direct product $R/I \times R/J$).

Moreover, we claim that $\operatorname{Ker} f = I \cap J$. Indeed, let $x \in \operatorname{Ker} f$. Thus, $f(x) = 0_{R/I \times R/J} = (0 + I, 0 + J)$. Since $f(x)$ was defined to be $(x + I, x + J)$, this means that $(x + I, x + J) = (0 + I, 0 + J)$. In other words, $x + I = 0 + I$ and $x + J = 0 + J$. In other words, $x \in I$ and $x \in J$. In other words, $x \in I \cap J$.

Forget that we fixed x. We thus have shown that $x \in I \cap J$ for each $x \in \operatorname{Ker} f$. In other words, $\operatorname{Ker} f \subseteq I \cap J$. Reading this argument in reverse shows that $I \cap J \subseteq \operatorname{Ker} f$. Thus, $\operatorname{Ker} f = I \cap J$. Since $I \cap J = IJ$ by part **(a)**, we thus obtain $\operatorname{Ker} f = IJ$.

Now, we claim that f is surjective. Indeed, $1 = i + j$, so that $1 - i = j \in J$ and thus $1 + J = i + J$. Now, $i + I = 0 + I$ (since $i \in I$) and $i + J = 1 + J$ (since $1 + J = i + J$). But the definition of f yields $f(i) = (i + I, i + J) = (0 + I, 1 + J)$ (since $i + I = 0 + I$ and $i + J = 1 + J$). Similarly, $f(j) = (1 + I, 0 + J)$. Now, for every $x \in R$ and $y \in R$, we have

$$\begin{aligned} f(xi + yj) &= \underbrace{f(x)}_{\substack{=(x+I,x+J) \\ \text{(by the definition of } f\text{)}}} \underbrace{f(i)}_{=(0+I,1+J)} + \underbrace{f(y)}_{\substack{=(y+I,y+J) \\ \text{(by the definition of } f\text{)}}} \underbrace{f(j)}_{=(1+I,0+J)} \\ &\qquad \text{(since } f \text{ is a ring morphism)} \\ &= \underbrace{(x + I, x + J)(0 + I, 1 + J)}_{=(x\cdot 0+I,x\cdot 1+J)=(0+I,x+J)} + \underbrace{(y + I, y + J)(1 + I, 0 + J)}_{=(y\cdot 1+I,y\cdot 0+J)=(y+I,0+J)} \\ &= (0 + I, x + J) + (y + I, 0 + J) = (0 + y + I, x + 0 + J) = (y + I, x + J) . \end{aligned}$$

Thus, every element of the form $(y + I, x + J)$ for some $y \in R$ and $x \in R$ lies in the image of f. Since every element of $R/I \times R/J$ has this form, we thus conclude that every element of $R/I \times R/J$ lies in the image of f. In other words, f is surjective.

Now, recall the First isomorphism theorem for rings (which we met and proved in Lecture 4). Applying it to our ring morphism $f : R \to R/I \times R/J$, we obtain $R/\operatorname{Ker} f \cong f(R)$; more precisely, we obtain that the universal property of quotient rings (applied to the ideal $\operatorname{Ker} f$ of R) yields a ring morphism $f' : R/\operatorname{Ker} f \to R/I \times R/J$, which (if we restrict its target to its actual image $f(R)$) is a ring isomorphism from $R/\operatorname{Ker} f$ to $f(R)$.

Fortunately, in our case right now, we have $f(R) = R/I \times R/J$ (since f is surjective), so we don't need to restrict the target of f' (this target is already

[1] Recall that "$R/I \times R/J$" means "$(R/I) \times (R/J)$".

$f(R)$). We thus conclude that f' is a ring isomorphism $R/\operatorname{Ker} f \to R/I \times R/J$. Since $\operatorname{Ker} f = IJ$, we can rewrite this as follows: f' is a ring isomorphism $R/IJ \to R/I \times R/J$. Moreover, if we recall how f' was constructed, we conclude that f' sends each residue class $r + \operatorname{Ker} f = r + IJ$ to $f(r) = (r + I, r + J)$ (by the definition of f). Thus, we have found a ring isomorphism

$$R/IJ \to R/I \times R/J$$

that sends each residue class $r + IJ$ to the pair $(r + I, r + J)$ (namely, f'). This proves part **(c)** of Theorem 1.1.1. Of course, part **(b)** thus follows. □

You can get rid of the commutativity requirement on R in Theorem 1.1.1 if you replace IJ by $IJ + JI$. (Checking this is a nice exercise on making sure you understand the above proof.)

As a corollary of Theorem 1.1.1, we can now prove the good old number-theoretical Chinese Remainder Theorem:

> **Theorem 1.1.3** (The Chinese Remainder Theorem for two integers)**.** Let n and m be two coprime integers. Then,
>
> $$\mathbb{Z}/(nm) \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m) \qquad \text{as rings.}$$
>
> More precisely, there is a ring isomorphism
>
> $$\mathbb{Z}/(nm) \to (\mathbb{Z}/n) \times (\mathbb{Z}/m)$$
>
> that sends each residue class $\overline{r}$ to $(\overline{r}, \overline{r})$ (or, to use somewhat less ambiguous notation, sends each residue class $r + nm\mathbb{Z}$ to the pair $(r + n\mathbb{Z}, r + m\mathbb{Z})$).

Proof. Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$. One of the propositions from Lecture 4 then yields $IJ = nm\mathbb{Z}$ and $I \cap J = \operatorname{lcm}(n,m)\mathbb{Z}$ and $I + J = \gcd(n,m)\mathbb{Z}$. Since n and m are coprime, we have $\gcd(n,m) = 1$; thus, $I + J = \underbrace{\gcd(n,m)}_{=1}\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$. In other words, the ideals I and J of $\mathbb{Z}$ are comaximal. Hence, part **(b)** of Theorem 1.1.1 yields $R/(IJ) \cong (R/I) \times (R/J)$. In view of $\underbrace{R}_{=\mathbb{Z}} / \underbrace{(IJ)}_{=nm\mathbb{Z}} = \mathbb{Z}/(nm\mathbb{Z}) = \mathbb{Z}/(nm)$ and $\underbrace{R}_{=\mathbb{Z}} / \underbrace{I}_{=n\mathbb{Z}} = \mathbb{Z}/(n\mathbb{Z}) = \mathbb{Z}/n$ and $\underbrace{R}_{=\mathbb{Z}} / \underbrace{J}_{=m\mathbb{Z}} = \mathbb{Z}/(m\mathbb{Z}) = \mathbb{Z}/m$, this rewrites as $\mathbb{Z}/(nm) \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m)$. This proves the first claim of Theorem 1.1.3. The "More precisely" claim likewise follows from part **(c)** of Theorem 1.1.1. □

As its name suggests, Theorem 1.1.1 can be generalized to k ideals. First, a convention:

Definition 1.1.4. Let $I_1, I_2, \ldots, I_k$ be k ideals of a ring R. We say that these k ideals $I_1, I_2, \ldots, I_k$ are **mutually comaximal** if $I_i + I_j = R$ holds for all $1 \leq i < j \leq k$.

In other words, k ideals $I_1, I_2, \ldots, I_k$ are mutually comaximal if I_i and I_j are comaximal for every $i < j$. When $k > 2$, this is a **much stronger** statement than $I_1 + I_2 + \cdots + I_k = R$.

For example, if $n_1, n_2, \ldots, n_k$ are k integers, then the k principal ideals $n_1\mathbb{Z}, n_2\mathbb{Z}, \ldots, n_k\mathbb{Z}$ are mutually comaximal if $n_1, n_2, \ldots, n_k$ are mutually coprime (that is, n_i is coprime to n_j for all $i < j$). When $k > 2$, this is a **much stronger** statement than $\gcd(n_1, n_2, \ldots, n_k) = 1$. Be warned! Lots of mistakes have been made by mistaking "mutually coprime" for "gcd of all k numbers is 1".

Enough of the warning labels; here is the theorem:

Theorem 1.1.5 (The Chinese Remainder Theorem for k ideals)**.** Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a commutative ring R. Then:

(a) We have $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$.

(b) We have $R / (I_1 I_2 \cdots I_k) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k$.

(c) More precisely, there is a ring isomorphism

$$R / (I_1 I_2 \cdots I_k) \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

that sends each residue class $r + I_1 I_2 \cdots I_k$ to the k-tuple $(r + I_1, r + I_2, \ldots, r + I_k)$.

Proof. We proceed by induction on k:

Induction base: You can take $k = 1$ as a base case (it is utterly trivial), or even $k = 0$ if you are brave enough[2].

Induction step: Let n be a positive integer. (You can assume $n > 1$ if it makes you sleep better.) Assume (as the IH[3]) that the theorem holds for $k = n - 1$. We must now prove that the theorem holds for $k = n$.

So let $I_1, I_2, \ldots, I_n$ be n mutually comaximal ideals of a commutative ring R. Then, the IH yields that Theorem 1.1.5 holds for $I_1, I_2, \ldots, I_{n-1}$. In particular, part **(a)** of Theorem 1.1.5 shows that

$$I_1 \cap I_2 \cap \cdots \cap I_{n-1} = I_1 I_2 \cdots I_{n-1}, \tag{1}$$

and part **(b)** of Theorem 1.1.5 shows that

$$R / (I_1 I_2 \cdots I_{n-1}) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}. \tag{2}$$

[2] Make sure to understand the empty product of ideals of R to be R itself, since R is the neutral element of the monoid of ideals of R under multiplication (see Exercise 8 **(d)** on homework set #1).

[3] "IH" means "induction hypothesis".

Finally, part **(c)** of Theorem 1.1.5 shows that there is a ring isomorphism

$$R/\left(I_1I_2\cdots I_{n-1}\right) \to R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1} \tag{3}$$

that does what you would expect it to do (viz., sends each residue class $r + I_1I_2\cdots I_{n-1}$ to the $(n-1)$-tuple $(r+I_1, r+I_2, \ldots, r+I_{n-1})$).

Now, we shall show that the two ideals $I_1I_2\cdots I_{n-1}$ and I_n are comaximal. Indeed, recall that the ideals $I_1, I_2, \ldots, I_n$ are mutually comaximal. Hence, for each $p \in \{1,2,\ldots,n-1\}$, the ideals I_p and I_n are comaximal, i.e., satisfy $I_p + I_n = R$. Hence, for each $p \in \{1,2,\ldots,n-1\}$, there exist some $i_p \in I_p$ and $j_p \in I_n$ satisfying $1 = i_p + j_p$ (since $1 \in R = I_p + I_n$). Consider these i_p and j_p. Now, multiplying the $n-1$ equalities $1 = i_p + j_p$ for all $p \in \{1,2,\ldots,n-1\}$, we obtain

$$\begin{aligned} 1 &= \prod_{p=1}^{n-1}\left(i_p + j_p\right) \\ &= i_1i_2\cdots i_{n-1} + \left(\text{a sum of } 2^{n-1}-1 \text{ other products of } i_p\text{'s and } j_p\text{'s}\right). \end{aligned}$$

On the right hand side of this equality, the first addend $i_1i_2\cdots i_{n-1}$ belongs to $I_1I_2\cdots I_{n-1}$ (since $i_p \in I_p$ for each p). As to the $2^{n-1}-1$ other products, they all belong to I_n, because each of them contains at least one factor in the ideal I_n (since each of them contains at least one j_p as a factor, but each j_p lies in I_n). Hence, all these $2^{n-1}-1$ products lie in I_n; therefore, so does their sum. Thus, we obtain

$$\begin{aligned} 1 &= \underbrace{i_1i_2\cdots i_{n-1}}_{\in I_1I_2\cdots I_{n-1}} + \underbrace{\left(\text{a sum of } 2^{n-1}-1 \text{ other products of } i_p\text{'s and } j_p\text{'s}\right)}_{\in I_n} \\ &\in I_1I_2\cdots I_{n-1} + I_n. \end{aligned}$$

Since $I_1I_2\cdots I_{n-1} + I_n$ is an ideal of R, this entails that any multiple of 1 must lie in $I_1I_2\cdots I_{n-1} + I_n$ as well. In other words, any element of R must lie in $I_1I_2\cdots I_{n-1} + I_n$ (since any element of R is a multiple of 1). In other words, $R \subseteq I_1I_2\cdots I_{n-1} + I_n$, so that $I_1I_2\cdots I_{n-1} + I_n = R$. In other words, the two ideals $I_1I_2\cdots I_{n-1}$ and I_n are comaximal.

Hence, we can apply Theorem 1.1.1 to these two ideals. We thus obtain (from part **(a)** of Theorem 1.1.1) that[4]

$$I_1I_2\cdots I_{n-1} \cap I_n = \left(I_1I_2\cdots I_{n-1}\right)I_n; \tag{4}$$

furthermore, we obtain (from part **(b)**) that

$$R/\left(\left(I_1I_2\cdots I_{n-1}\right)I_n\right) \cong R/\left(I_1I_2\cdots I_{n-1}\right) \times R/I_n; \tag{5}$$

[4] The notation "$I_1I_2\cdots I_{n-1} \cap I_n$" is to be understood as "$\left(I_1I_2\cdots I_{n-1}\right) \cap I_n$".

and finally we obtain (from part **(c)**) that there is a ring isomorphism

$$R/\left(\left(I_1 I_2 \cdots I_{n-1}\right) I_n\right) \to R/\left(I_1 I_2 \cdots I_{n-1}\right) \times R/I_n \qquad (6)$$

that does what you expect (viz., sends each residue class $r + \left(I_1 I_2 \cdots I_{n-1}\right) I_n$ to the pair $\left(r + I_1 I_2 \cdots I_{n-1}, r + I_n\right)$).

Now, let us combine what we have learned. We have

$$\begin{aligned} I_1 \cap I_2 \cap \cdots \cap I_n &= \underbrace{\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right)}_{\substack{= I_1 I_2 \cdots I_{n-1} \\ \text{(by (1))}}} \cap I_n = I_1 I_2 \cdots I_{n-1} \cap I_n \\ &= \left(I_1 I_2 \cdots I_{n-1}\right) I_n \qquad \text{(by (4))} \\ &= I_1 I_2 \cdots I_n; \end{aligned}$$

this proves part **(a)** of Theorem 1.1.5 for $k = n$. Finishing off the other two parts requires a little bit of yak-shaving. We will need the following lemma:

> **Lemma 1.1.6.** Let A, B, C be three rings.
>
> **(a)** If $A \cong B$, then $A \times C \cong B \times C$.
>
> **(b)** More specifically: If $f : A \to B$ is a ring isomorphism, then $f \times \operatorname{id}_C : A \times C \to B \times C$ (this is the map that sends each $(a, c) \in A \times C$ to $\left(f(a), \operatorname{id}_C(c)\right) = \left(f(a), c\right) \in B \times C$) is a ring isomorphism, too.

This lemma simply says that if you replace a ring in a direct product by an isomorphic one, then the whole direct product too stays isomorphic. I won't offend your intellect with the proof of this lemma; it is a purely paint-by-numbers affair. Such lemmas are a dime a dozen, and you are supposed to invent one whenever you need it. The idea behind this lemma is simply that isomorphisms behave like equalities.

So let us go back to our proof of Theorem 1.1.5. We have

$$\begin{aligned} R/\left(I_1 I_2 \cdots I_n\right) &= R/\left(\left(I_1 I_2 \cdots I_{n-1}\right) I_n\right) \\ &\cong \underbrace{R/\left(I_1 I_2 \cdots I_{n-1}\right)}_{\substack{\cong R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1} \\ \text{(by (2))}}} \times R/I_n \qquad \text{(by (5))} \\ &= \left(R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}\right) \times R/I_n \qquad \text{(by Lemma 1.1.6 } \textbf{(a)}\text{)} \\ &\cong R/I_1 \times R/I_2 \times \cdots \times R/I_n; \end{aligned}$$

this proves part **(b)** of Theorem 1.1.5 for $k = n$.

It remains to prove part **(c)**. Here we will need Lemma 1.1.6 **(b)**. Indeed, (3) gives us a ring isomorphism $R/\left(I_1 I_2 \cdots I_{n-1}\right) \to R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}$; thus, Lemma 1.1.6 **(b)** yields a ring isomorphism

$$R/\left(I_1 I_2 \cdots I_{n-1}\right) \times R/I_n \to \left(R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}\right) \times R/I_n.$$

Now, we compose the arrows in our quiver:

$$\begin{aligned}
&R/\left(I_1I_2\cdots I_n\right)\\
&= R/\left(\left(I_1I_2\cdots I_{n-1}\right)I_n\right)\\
&\to R/\left(I_1I_2\cdots I_{n-1}\right)\times R/I_n \qquad \text{(this is the morphism from (6))}\\
&\to \left(R/I_1\times R/I_2\times\cdots\times R/I_{n-1}\right)\times R/I_n\\
&\qquad \text{(this is the isomorphism we just constructed using Lemma 1.1.6 } \textbf{(b)}\text{)}\\
&\to R/I_1\times R/I_2\times\cdots\times R/I_n.
\end{aligned}$$

All these arrows are ring isomorphisms; hence, so is their composition. It remains to show that this isomorphism does what you expect (i.e., sends $r + I_1I_2\cdots I_n$ to $(r+I_1, r+I_2, \ldots, r+I_n)$). This is completely straightforward, and becomes even more so if you drop the details and just write $\overline{r}$ for all possible cosets $r+J$ no matter what J is: Following a coset $\overline{r} = r + I_1I_2\cdots I_n$ through the above arrows, we obtain

$$\overline{r} = \overline{r} \mapsto (\overline{r}, \overline{r}) \mapsto ((\overline{r}, \overline{r}, \ldots, \overline{r}), \overline{r}) \mapsto (\overline{r}, \overline{r}, \ldots, \overline{r}).$$

While the different $\overline{r}$'s mean different things (viz., cosets for different ideals), we are never in any danger of confusing them for one another, since we know what sets these maps go between. So the $(\overline{r}, \overline{r}, \ldots, \overline{r})$ at the end of this computation must be $(r+I_1, r+I_2, \ldots, r+I_n)$, since it is an element of $R/I_1 \times R/I_2 \times \cdots \times R/I_n$. So our isomorphism sends $r + I_1I_2\cdots I_n$ to $(r+I_1, r+I_2, \ldots, r+I_n)$. Thus, part **(c)** of Theorem 1.1.5 is proved for $k = n$.

All three parts of the theorem are thus proved for $k = n$. This completes the induction step, and thus the proof. □

We can again apply this to $R = \mathbb{Z}$:

Theorem 1.1.7 (The Chinese Remainder Theorem for k integers)**.** Let $n_1, n_2, \ldots, n_k$ be k mutually coprime integers. ("Mutually coprime" means that n_i is coprime to n_j whenever $i < j$). Then,

$$\mathbb{Z}/\left(n_1n_2\cdots n_k\right) \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k.$$

More precisely, there is a ring isomorphism

$$\mathbb{Z}/\left(n_1n_2\cdots n_k\right) \to \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k$$

that does what you expect.

Proof. This can be derived from Theorem 1.1.5, in the same way as we derived Theorem 1.1.3 from Theorem 1.1.1. Details are LTTR. □

Corollary 1.1.8. Let $p_1, p_2, \ldots, p_k$ be k distinct primes. Let $i_1, i_2, \ldots, i_k$ be k nonnegative integers. Then,

$$\mathbb{Z} / \left(p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k} \right) \cong \mathbb{Z} / p_1^{i_1} \times \mathbb{Z} / p_2^{i_2} \times \cdots \times \mathbb{Z} / p_k^{i_k}.$$

More precisely, there is a ring isomorphism

$$\mathbb{Z} / \left(p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k} \right) \to \mathbb{Z} / p_1^{i_1} \times \mathbb{Z} / p_2^{i_2} \times \cdots \times \mathbb{Z} / p_k^{i_k}$$

that does what you expect.

Proof. The prime powers $p_1^{i_1}, p_2^{i_2}, \ldots, p_k^{i_k}$ are mutually coprime; so we can apply Theorem 1.1.7 to $n_j = p_j^{i_j}$. □

Note that it is important that the primes be distinct in Corollary 1.1.8. For example, $\mathbb{Z}/p^2$ is not isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$ (not even as additive groups, let alone as rings).

The Chinese Remainder Theorem has many down-to-earth consequences. For example, in Exercise 7 on homework set #0, I have given you two positive integers n (namely, 7 and 14), and asked you to count how many of the numbers $0, 1, \ldots, n-1$ appear as remainders of a perfect square divided by n. It is not hard to see that this question is equivalent to asking how many elements of the ring $\mathbb{Z}/n$ are squares in this ring. Here I am using the following terminology:

Definition 1.1.9. Let R be a ring. An element $r \in R$ is said to be a **square** (in R) if there exists some $u \in R$ such that $r = u^2$.

For example, the squares in $\mathbb{R}$ are the nonnegative reals, whereas the squares in $\mathbb{Z}$ are the perfect squares.

If n is a positive integer, then an element $i \in \{0, 1, \ldots, n-1\}$ is the remainder of some perfect square divided by n if and only if the element $\overline{i} = i + n\mathbb{Z}$ is a square in $\mathbb{Z}/n$. Thus, counting distinct remainders of perfect squares divided by n is equivalent to counting squares in $\mathbb{Z}/n$.

Now, I claim that the latter can be done easily when the prime factorization of n is known. The way to do it is in three steps:

1. Answer the question (i.e., "how many squares does $\mathbb{Z}/n$ have?") when n is prime.

2. Extend the answer to the case when n is a prime power (i.e., a number of the form p^i with p prime and $i \in \mathbb{N}$).

3. Finally, extend the answer to all positive integers n.

This three-step program is a standard strategy for answering number-theoretical questions. Typically, the three steps each have methods tailored to them:

1. When n is prime, the ring $\mathbb{Z}/n$ is a field. This makes many tactics available that would otherwise not work; e.g., Gaussian elimination works over fields but not generally over arbitrary rings (we will learn more about this later).

2. There are many tools for "lifting" results about primes to analogous results about prime powers.

3. Here, the Chinese Remainder Theorem becomes useful. Any positive integer $\mathbb{Z}/n$ is a product of finitely many mutually coprime prime powers $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$. Thus, the Chinese Remainder Theorem (more precisely, Corollary 1.1.8) yields
$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}. \tag{7}$$

For our specific question (counting squares in $\mathbb{Z}/n$), you are going to do Step 1 on homework set #1 (Exercise 10 **(c)**). (More precisely, that exercise covers the case when n is odd. But the only even prime is 2, and you can count the squares in $\mathbb{Z}/2$ on your hands. Not fingers, hands.) Step 2 will not be done in this course in full, but you will see the case of $n = p^2$ in homework set #2 (Exercise 4). Step 3 is now easy (assuming Steps 1 and 2 are done): If $A_1, A_2, \ldots, A_k$ are rings, then the squares in the direct product $A_1 \times A_2 \times \cdots \times A_k$ are just the k-tuples $(a_1, a_2, \ldots, a_k)$ where each a_i is a square in A_i; thus,
$$\begin{aligned}&(\text{the number of squares in } A_1 \times A_2 \times \cdots \times A_k)\\ &= \prod_{i=1}^{k} (\text{the number of squares in } A_i)\,.\end{aligned} \tag{8}$$

Furthermore, isomorphic rings have the same number of squares (since any ring morphism sends squares to squares). Thus, (7) yields
$$\begin{aligned}&(\text{the number of squares in } \mathbb{Z}/n)\\ &= \left(\text{the number of squares in } \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}\right)\\ &= \prod_{i=1}^{k} \left(\text{the number of squares in } \mathbb{Z}/p_i^{a_i}\right) \qquad (\text{by (8)})\,.\end{aligned}$$

Remark 1.1.10. Theorem 1.1.5 becomes false if we drop the assumption that R be commutative. However, we can tweak this theorem to make it work for noncommutative rings R as well:

Theorem 1.1.11. Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a (not necessarily commutative) ring R. Let $I_1 * I_2 * \cdots * I_k$ denote the sum of all the $k!$ products $J_1 J_2 \cdots J_k$, where $J_1, J_2, \ldots, J_k$ are the k ideals $I_1, I_2, \ldots, I_k$ in some order. (For example, if $k = 3$, then $I_1 * I_2 * I_3 = I_1 I_2 I_3 + I_1 I_3 I_2 + I_2 I_1 I_3 + I_2 I_3 I_1 + I_3 I_1 I_2 + I_3 I_2 I_1$.)

Now:

(a) We have $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 * I_2 * \cdots * I_k$.

(b) We have $R / (I_1 * I_2 * \cdots * I_k) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k$.

(c) More precisely, there is a ring isomorphism

$$R / (I_1 * I_2 * \cdots * I_k) \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

that sends each residue class $r + I_1 * I_2 * \cdots * I_k$ to the k-tuple $(r + I_1, r + I_2, \ldots, r + I_k)$.

We leave the proof of this theorem to the reader. (It is a not-too-difficult adaptation of our above proof of Theorem 1.1.5.)

1.2. Euclidean domains ([DF, §8.1])

We have talked about ideals of $\mathbb{Z}$ a lot (they give rise to modular arithmetic), but you might have noticed that all of them were principal. This is no accident:

Proposition 1.2.1. Any ideal of $\mathbb{Z}$ is principal.

Proof. Let I be an ideal of $\mathbb{Z}$. We must show that I is principal.

If $I = \{0\}$, then this is clear (since $I = 0\mathbb{Z}$ in this case). So we WLOG assume that $I \neq \{0\}$. Since I always contains 0, this means that I must contain a nonzero integer as well. Hence, I contains a positive integer (because if I contains a negative integer a, then I must also contain $(-1)\,a$, which is positive). Let $b \in I$ be the **smallest** positive integer that I contains. Hence, I cannot contain any positive integer smaller than b. However, I contains b, and thus contains every multiple of b (since I is an ideal). In other words, $b\mathbb{Z} \subseteq I$.

We will now show that $I \subseteq b\mathbb{Z}$. Indeed, let $a \in I$. Let r be the remainder of a divided by b. Then, $r \in \{0, 1, \ldots, b-1\}$ and $r \equiv a \bmod b$. Now, from $r \equiv a \bmod b$, we obtain $b \mid r - a$ and thus $r - a \in b\mathbb{Z} \subseteq I$. Hence, $r = \underbrace{r-a}_{\in I} + \underbrace{a}_{\in I} \in I + I = I$ (since I is an ideal of $\mathbb{Z}$). Hence, r cannot be a positive integer smaller than b (since I cannot contain any positive integer smaller than b). In other words, $r \notin \{1, 2, \ldots, b-1\}$. Contrasting this with $r \in \{0, 1, \ldots, b-1\}$, we obtain $r = 0$. Thus, $b \mid \underbrace{r}_{=0} - a = 0 - a \mid -a \mid a$, so that $a \in b\mathbb{Z}$.

Forget that we fixed a. We thus have shown that $a \in b\mathbb{Z}$ for each $a \in I$. In other words, $I \subseteq b\mathbb{Z}$. Combined with $b\mathbb{Z} \subseteq I$, this yields $I = b\mathbb{Z}$. Thus, I is principal, qed. □

The key to making this proof work was clearly the concept of division with remainder. Not every ring has this feature. However, many rings different from $\mathbb{Z}$ have it; thus, it is worth defining a word for them:

Definition 1.2.2. Let R be a commutative ring.

(a) A **norm** on R means a function $N : R \to \mathbb{N}$ with $N(0) = 0$.

(b) A norm N on R is said to be **Euclidean** if for any $a \in R$ and any nonzero $b \in R$, there exist elements $q, r \in R$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(b)).$$

(c) We say that R is a **Euclidean domain** if R is an integral domain and has a Euclidean norm.

You can think of the norm as a measure of the "size" of an element of R, similar to the absolute value of an integer or to the degree of a polynomial. (These will indeed be particular cases.) Note that we are **not** requiring that the norm have any nice algebraic properties (such as $N(ab) = N(a)N(b)$, which will be true for some Euclidean norms but not for others). Note that we are also **not** requiring the q and the r in the definition of a Euclidean norm to be unique.

Some examples will help illustrate the definition:

- Any field F is a Euclidean domain. Indeed, any map $N : F \to \mathbb{N}$ with $N(0) = 0$ is a Euclidean norm on F.

- The ring $\mathbb{Z}$ is a Euclidean domain. Indeed, a Euclidean norm on $\mathbb{Z}$ is given by the map $N : \mathbb{Z} \to \mathbb{N}$, $a \mapsto |a|$. The fact that it is Euclidean follows from division with remainder. However, q and r are not unique! For $a = 7$ and $b = 5$, there are **two** pairs $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(b)).$$

  These two pairs are $(1, 2)$ and $(2, -3)$. The second pair has negative r, which is why it does not qualify as a quotient-remainder pair in the sense of high school arithmetic; but it qualifies for the definition of a Euclidean norm.

- If F is a field, then the ring $F[x]$ of univariate polynomials over F is a Euclidean domain. We will discuss this later in more detail, when we study polynomials. However, polynomial rings in more than 1 variable are not Euclidean domains; neither are polynomial rings over non-fields.

- The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain. Indeed, we claim that the map

$$N : \mathbb{Z}[i] \to \mathbb{N}, \qquad a + bi \mapsto a^2 + b^2 \text{ (where } a, b \in \mathbb{Z})$$

is a Euclidean norm.

To prove this, we must show that for any $\alpha \in \mathbb{Z}[i]$ and any nonzero $\beta \in \mathbb{Z}[i]$, there exist elements $q, r \in \mathbb{Z}[i]$ with

$$\alpha = q\beta + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(\beta)). \tag{9}$$

So let us fix an $\alpha \in \mathbb{Z}[i]$ and a nonzero $\beta \in \mathbb{Z}[i]$. We are looking for elements $q, r \in \mathbb{Z}[i]$ that satisfy (9). We can even replace the "$r = 0$ or $N(r) < N(\beta)$" condition in (9) by the stronger condition "$N(r) < N(\beta)$".

To find the elements q, r we are seeking, we make the following observation: The absolute value $|z|$ of a complex number $z = a + bi$ (with $a, b \in \mathbb{R}$) is defined as $|z| = \sqrt{a^2 + b^2} = \sqrt{z\overline{z}}$. Thus, any $z \in \mathbb{Z}[i]$ satisfies $N(z) = |z|^2$. Hence, we have the following chain of equivalences:

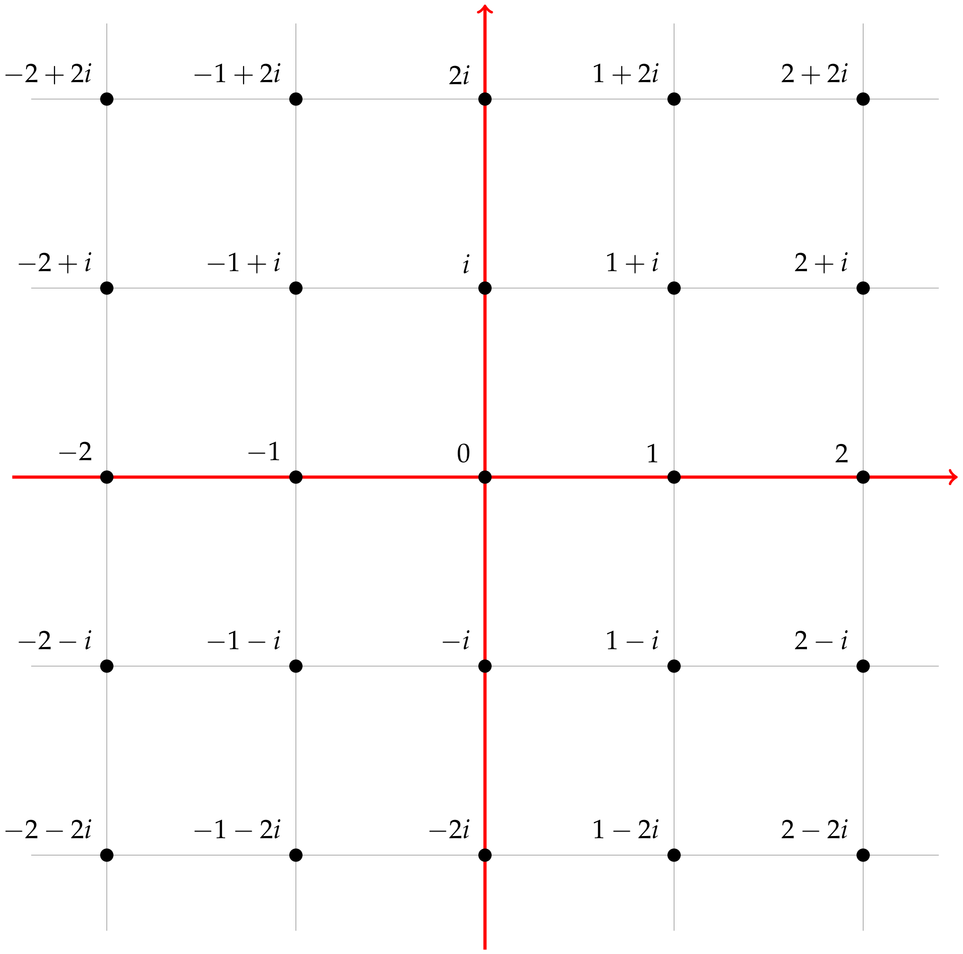
$$\begin{aligned}(N(r) < N(\beta)) &\iff \left(|r|^2 < |\beta|^2\right) \iff (|r| < |\beta|) \iff \left(\frac{|r|}{|\beta|} < 1\right) \\ &\iff \left(\left|\frac{r}{\beta}\right| < 1\right)\end{aligned} \tag{10}$$

(since $\dfrac{|z|}{|w|} = \left|\dfrac{z}{w}\right|$ for any two complex numbers z and $w \neq 0$). Moreover, we have the equivalence

$$(\alpha = q\beta + r) \iff \left(\frac{\alpha}{\beta} = q + \frac{r}{\beta}\right) \iff \left(\frac{\alpha}{\beta} - q = \frac{r}{\beta}\right). \tag{11}$$

Now, recall that we are looking for elements $q, r \in \mathbb{Z}[i]$ that satisfy $\alpha = q\beta + r$ and $N(r) < N(\beta)$. In view of (10) and (11), this means that we are looking for elements $q, r \in \mathbb{Z}[i]$ that satisfy $\dfrac{\alpha}{\beta} - q = \dfrac{r}{\beta}$ and $\left|\dfrac{r}{\beta}\right| < 1$. Equivalently, we can look for a Gaussian integer $q \in \mathbb{Z}[i]$ satisfying $\left|\dfrac{\alpha}{\beta} - q\right| < 1$ (because once such a q has been found, we can set $r = \alpha - q\beta$ and obtain $\dfrac{r}{\beta} = \dfrac{\alpha - q\beta}{\beta} = \dfrac{\alpha}{\beta} - q$, so that $\dfrac{\alpha}{\beta} - q = \dfrac{r}{\beta}$ and $\left|\dfrac{r}{\beta}\right| = \left|\dfrac{\alpha}{\beta} - q\right| < 1$). But finding such a q is easy if you remember the geometric meaning of the Gaussian integers: The Gaussian integers are the lattice points of a square lattice in the plane[5]. So a Gaussian integer $q \in \mathbb{Z}[i]$ satisfying $\left|\frac{\alpha}{\beta} - q\right| < 1$ simply means a lattice point at a distance less than 1 from the point $\frac{\alpha}{\beta}$. Geometrically, it is easy to see that such a lattice point exists (since the point $\frac{\alpha}{\beta}$ must lie in one of the squares of the lattice, and then

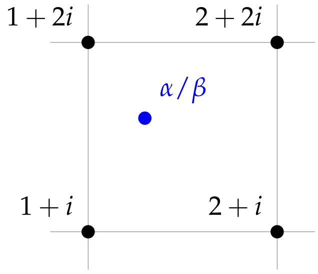
[5] Here is the square lattice I am talking about:



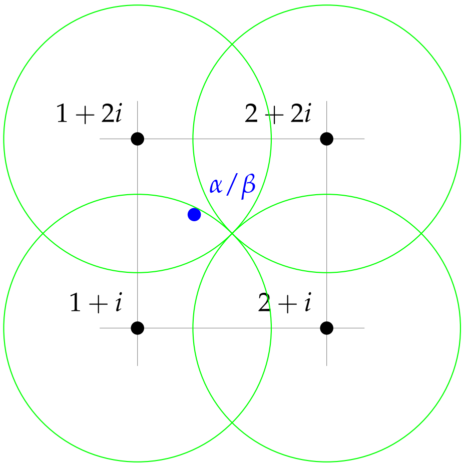
have distance $< \frac{\sqrt{2}}{2}$ from one of the four vertices of the square[6]; but this entails that $\frac{\alpha}{\beta}$ has distance < 1 from this latter vertex[7]). Thus, we have found q.

For a non-geometric proof of this fact, see the proof of Theorem 3.1 in Keith Conrad's *The Gaussian integers* (see `https://kconrad.math.uconn.edu/math5230f12/handouts/Zinotes.pdf`).

[6] Here is a close-up picture of the square (with one possible location of $\frac{\alpha}{\beta}$):



I am claiming that the point $\frac{\alpha}{\beta}$ has distance $< \frac{\sqrt{2}}{2}$ from one of the four vertices of the square in which it lies. The easiest way to see this geometrically is to draw circles of radius $\frac{\sqrt{2}}{2}$ around the vertices of the square, and convince yourself that these circles cover the entire square:



[7] since $\frac{\sqrt{2}}{2} < 1$

- The ring
$$\mathbb{Z}\left[\sqrt{-3}\right] := \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}$$
(this is another subring of $\mathbb{C}$, since $\sqrt{-3} = \sqrt{3}i$) is **not** Euclidean. (See, e.g., `https://math.stackexchange.com/questions/115934` for proofs.)

- The ring
$$\mathbb{Z}\left[\sqrt{2}\right] := \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$$
is Euclidean. An Euclidean norm for it is the map
$$\begin{aligned} &\mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{N}, \\ &a + b\sqrt{2} \mapsto \left|a^2 - 2b^2\right| \qquad (\text{with } a, b \in \mathbb{Z}). \end{aligned}$$

- The ring
$$\mathbb{Z}\left[\sqrt{14}\right] := \left\{a + b\sqrt{14} \mid a, b \in \mathbb{Z}\right\}$$
is Euclidean. An Euclidean norm for it is notoriously hard to construct (in particular, it is **not** the map sending each $a + b\sqrt{14}$ to $\left|a^2 - 14b^2\right|$). See `https://math.stackexchange.com/questions/1148364` .

- The ring $\mathbb{Z}\left[\sqrt{5}\right] := \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$ is **not** Euclidean.