Math 332 Winter 2023, Lecture 14: Rings

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

1. Rings and ideals (cont'd)

1.12. The Chinese Remainder Theorem (cont'd)

1.12.4. The story so far

Let us recapitulate the results of Lecture 13.

We began by observing that

$$\mathbb{Z}/\left(nm\right) \cong \mathbb{Z}/n \times \mathbb{Z}/m$$

(by our convention, the right hand side means $\left(\mathbb{Z}/n\right) \times \left(\mathbb{Z}/m\right)$) whenever n and m are two coprime integers.

We generalized this by replacing $\mathbb{Z}$ by an arbitrary commutative ring and replacing n and m by two comaximal ideals.

Two ideals I and J of a ring R are said to be **comaximal** if $I + J = R$. If $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ for two integers n and m, then this condition is equivalent to n and m being coprime. (See Proposition 1.11.3 in Lecture 12 for a dictionary between ideal arithmetic for principal ideals of $\mathbb{Z}$ and elementary number theory for integers.)

We proved the Chinese Remainder Theorem for two ideals: If I and J are two comaximal ideals of a commutative ring R, then $I \cap J = IJ$ and there is a ring isomorphism

$$\begin{aligned} R/\left(IJ\right) &\to R/I \times R/J, \\ \overline{r} &\mapsto \left(\overline{r}, \overline{r}\right). \end{aligned}$$

Today, we will extend this result to k mutually comaximal ideals rather than just two.

1.12.5. Interlude: Multiplying comaximal ideals

First, we need some auxiliary results.

Recall the classical fact from elementary number theory saying that if i, j, k are three integers such that each of i and j is coprime to k (that is, such that $\gcd\left(i,k\right) = 1$ and $\gcd\left(j,k\right) = 1$), then ij is also coprime to k (that is, $\gcd\left(ij,k\right) = 1$).

More generally, for any three integers i, j, k, we have

$$\gcd\left(ij,k\right) \mid \gcd\left(i,k\right)\gcd\left(j,k\right).$$

These facts can be generalized to arbitrary ideals of any ring:

Proposition 1.12.4. Let I, J and K be three ideals of a ring R. Then:
(a) We have $(I+K)(J+K) \subseteq IJ+K$.
(b) If $I+K=R$ and $J+K=R$, then $IJ+K=R$.

Proof. The sets $I+K$, $J+K$ and $IJ+K$ are ideals of R (by Proposition 1.11.2 **(a)** in Lecture 12), and thus are closed under finite sums.

(a) The ideal $(I+K)(J+K)$ is defined as the set of all finite sums of $(I+K,\ J+K)$-products. Thus, in order to prove that it is a subset of $IJ+K$, it suffices to show that any $(I+K,\ J+K)$-product belongs to $IJ+K$ (because $IJ+K$ is closed under finite sums, and thus any sum of elements of $IJ+K$ will again lie in $IJ+K$).

An $(I+K,\ J+K)$-product is an element of the form xy, where $x \in I+K$ and $y \in J+K$. So we must show that

$$xy \in IJ+K \qquad \text{for any } x \in I+K \text{ and } y \in J+K.$$

To prove this, we let $x \in I+K$ and $y \in J+K$. Thus, $x = i+a$ for some $i \in I$ and some $a \in K$. Likewise, $y = j+b$ for some $j \in J$ and $b \in K$. Consider these i, a, j, b. Multiplying the equalities $x = i+a$ and $y = j+b$, we obtain

$$\begin{aligned} xy = (i+a)(j+b) = &\underbrace{ij}_{\substack{\in IJ \\ (\text{since } i \in I \\ \text{and } j \in J)}} + \underbrace{ib}_{\substack{\in K \\ (\text{since } b \in K \\ \text{and since } K \\ \text{is an ideal})}} + \underbrace{aj}_{\substack{\in K \\ (\text{since } a \in K \\ \text{and since } K \\ \text{is an ideal})}} + \underbrace{ab}_{\substack{\in K \\ (\text{since } b \in K \\ \text{and since } K \\ \text{is an ideal})}} \\ \in IJ + &\underbrace{K+K+K}_{\substack{\subseteq K \\ (\text{since } K \text{ is closed under finite sums})}} \subseteq IJ+K, \end{aligned}$$

as desired. This completes the proof of part **(a)** as explained above.

(b) Assume that $I+K=R$ and $J+K=R$. Then, $(I+K)(J+K) = RR$. However, $RR = R$ (since each $r \in R$ satisfies $r = \underbrace{1}_{\in R} \cdot \underbrace{r}_{\in R} \in RR$). Thus, $(I+K)(J+K) = RR = R$.

However, Proposition 1.12.4 **(a)** yields that $(I+K)(J+K) \subseteq IJ+K$. In view of $(I+K)(J+K) = R$, this can be rewritten as $R \subseteq IJ+K$. Since $IJ+K$ is a subset of R, we thus conclude that $IJ+K=R$. Thus, Proposition 1.12.4 **(b)** is proved. □

We can extend Proposition 1.12.4 **(b)** to products of k ideals:

Proposition 1.12.5. Let $I_1, I_2, \ldots, I_k$ be k ideals of a ring R. Let K be a further ideal of R. Assume that

$$I_i + K = R \qquad \text{for each } i \in \{1,2,\ldots,k\}.$$

Then, $I_1 I_2 \cdots I_k + K = R$.

Proof. Induct on k. The base case ($k = 0$) is an exercise in triviality (an empty product of ideals of R is R by definition, and we have $R + K = R$). The induction step uses Proposition 1.12.4 **(b)** in a straightforward way ($I_1 I_2 \cdots I_k = (I_1 I_2 \cdots I_{k-1}) I_k$). See §2.12.4 in the text for more details. □

1.12.6. The Chinese Remainder Theorem for k ideals

Let us now define the proper condition for the Chinese Remainder Theorem for k ideals:

Definition 1.12.6. 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 $i < j$.

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 requirement is **much stronger** than requiring $I_1 + I_2 + \cdots + I_k = R$.

For instance, if $n_1, n_2, \ldots, n_k$ are k arbitrary integers, then the k principal ideals $n_1\mathbb{Z}$, $n_2\mathbb{Z}$, $\ldots$, $n_k\mathbb{Z}$ are mutually comaximal if and only if $\gcd\left(n_i, n_j\right) = 1$ for all $i < j$. This is a **much stronger** condition than $\gcd\left(n_1, n_2, \ldots, n_k\right) = 1$. (For a concrete example, $6, 10, 15$ are not mutually coprime – even worse, no two of them are coprime! – but they satisfy $\gcd\left(6, 10, 15\right) = 1$.)

This being said, we can state a generalization of the Chinese Remainder Theorem to k ideals:

Theorem 1.12.7 (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

$$R/\left(I_1 I_2 \cdots I_k\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

(c) More concretely, there is a ring isomorphism

$$\begin{aligned} R/\left(I_1 I_2 \cdots I_k\right) &\to R/I_1 \times R/I_2 \times \cdots \times R/I_k, \\ \overline{r} &\mapsto \left(\overline{r}, \overline{r}, \ldots, \overline{r}\right). \end{aligned}$$

Proof. Induct on k. The induction step uses

- Proposition 1.12.5 to argue that $I_1 I_2 \cdots I_{k-1}$ is comaximal to I_k;
- the Chinese Remainder Theorem for two ideals (Theorem 1.12.3 in Lecture 13);

- the pretty simple fact that if three rings A, B, C satisfy $A \cong B$, then $A \times C \cong B \times C$ (and, to be more concrete: if $f : A \to B$ is a ring isomorphism, then there is a ring isomorphism $A \times C \to B \times C$ that sends each pair (a, c) to $(f(a), c)$).

See §2.12.5 in the text for more details (although stated in a slightly more general context). □

1.12.7. Applying to integers again

Applying Theorem 1.12.7 to principal ideals of $R = \mathbb{Z}$, we obtain the following:

Theorem 1.12.8 (The Chinese Remainder Theorem for k integers)**.** Let $n_1, n_2, \ldots, n_k$ be k mutually coprime integers (i.e., any k integers satisfying $\gcd(n_i, n_j) = 1$ for all $i < j$). Then,

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

More concretely, there is a ring isomorphism

$$\begin{aligned} \mathbb{Z}/(n_1 n_2 \cdots n_k) &\to \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k, \\ \overline{r} &\mapsto (\overline{r}, \overline{r}, \ldots, \overline{r}). \end{aligned}$$

Proof. Since the integers $n_1, n_2, \ldots, n_k$ are mutually coprime, the corresponding principal ideals $n_1\mathbb{Z}$, $n_2\mathbb{Z}$, $\ldots$, $n_k\mathbb{Z}$ are mutually comaximal (by Proposition 1.11.3 **(c)** in Lecture 12). Hence, we can apply Theorem 1.12.7 to $R = \mathbb{Z}$ and $I_i = n_i\mathbb{Z}$. Specifically, parts **(b)** and **(c)** of this theorem yield the claims of Theorem 1.12.8. (Part **(a)** of Theorem 1.12.7 yields that $\operatorname{lcm}(n_1, n_2, \ldots, n_k) = |n_1 n_2 \cdots n_k|$, which is also nice.) □

Corollary 1.12.9. Let n be a positive integer with prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes, and where $a_1, a_2, \ldots, a_k$ are nonnegative integers. Then,

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}.$$

More concretely, there is a ring isomorphism

$$\begin{aligned} \mathbb{Z}/n &\to \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}, \\ \overline{r} &\mapsto (\overline{r}, \overline{r}, \ldots, \overline{r}). \end{aligned}$$

For instance, the prime factorization of 72 is $72 = 2^3 \cdot 3^2$, so that Corollary 1.12.9 yields

$$\mathbb{Z}/72 \cong \mathbb{Z}/2^3 \times \mathbb{Z}/3^2 \qquad \text{(as rings)}.$$

This cannot be broken up any further: Neither of the rings $\mathbb{Z}/2^3$ and $\mathbb{Z}/3^2$ is isomorphic to a direct product. (In particular, $\mathbb{Z}/3^2$ is not $(\mathbb{Z}/3) \times (\mathbb{Z}/3)$, since 3 and 3 are not coprime.)

Proof of Corollary 1.12.9. Apply Theorem 1.12.8 to $n_j = p_j^{a_j}$ (since powers of distinct primes are coprime). □

Corollary 1.12.9 allows us to break rings of the form $\mathbb{Z}/n$ down into simpler rings (as long as n is not itself a prime power). This has several applications:

- Counting squares (or, more generally, solutions to polynomial equations) in $\mathbb{Z}/n$.

  Exercise 7 on homework set #0 asked, for a given integer $n > 0$, how many of the numbers $0, 1, \ldots, n-1$ appear as remainders of a perfect square divided by n. This is equivalent to asking for the number of squares in the ring $\mathbb{Z}/n$. Here, a **square** in a ring R means an element of the form r^2 with $r \in R$. For instance, if $n = 5$, then there are 3 squares in $\mathbb{Z}/n$, namely $\overline{0}$, $\overline{1}$ and $\overline{4}$. Can we answer this question for general n, without having to count the squares in $\mathbb{Z}/n$ one by one?

  It is easy to see that a square in a direct product $A \times B$ of two rings is the same thing as a pair (a, b) consisting of a square $a \in A$ and a square $b \in B$. Thus,

  $$(\#\text{ of squares in } A \times B) = (\#\text{ of squares in } A) \cdot (\#\text{ of squares in } B).$$

  Also, isomorphic rings have the same # of squares. Thus, if n has the prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then the isomorphism

  $$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}$$

  in Corollary 1.12.9 entails

  $$\begin{aligned} &(\#\text{ of squares in } \mathbb{Z}/n) \\ &= \left(\#\text{ of squares in } \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}\right) \\ &= \prod_{i=1}^{k} \left(\#\text{ of squares in } \mathbb{Z}/p_i^{a_i}\right). \end{aligned} \tag{1}$$

  Hence, it remains to compute the # of squares in $\mathbb{Z}/p^a$ for any prime p and any positive integer a.

  A good first step is counting the squares in $\mathbb{Z}/p$ for any prime p. Their number turns out to be

  $$\begin{cases} 2, & \text{if } p = 2; \\ \dfrac{p+1}{2}, & \text{if } p \neq 2. \end{cases}$$

This is not hard to show by observing that each square x in $\mathbb{Z}/p$ other than $\overline{0}$ is taken twice (i.e., there are exactly two elements $y \in \mathbb{Z}/p$ satisfying $y^2 = x$), whereas the square $\overline{0}$ is taken only once. (Exception: if $p = 2$, then the square $\overline{1}$ is also taken only once.)[1]

The next step is counting squares in $\mathbb{Z}/p^2$, where p is again a prime. Their number turns out to be

$$\begin{cases} 2, & \text{if } p = 2; \\ \dfrac{p^2 - p}{2} + 1, & \text{if } p \neq 2. \end{cases}$$

This is again not hard to prove[2].

Now you can probably trust me that the analogous problem is solvable for $\mathbb{Z}/p^a$ when a is an arbitrary positive answer. Unfortunately, this solution is painful and quite tricky, but still doable. See [Stangl96] for one way to find and prove a formula (albeit using primitive roots, which we have not seen yet in this course, but which can be avoided with some more careful counting). Alas, the formula is rather ugly: For any prime p and any integer $a \geq 1$, it says that the number of squares in $\mathbb{Z}/p^a$ is

$$\begin{cases} \dfrac{p^{a+1} + p + 2}{2(p+1)}, & \text{if } p \neq 2 \text{ and if } a \text{ is even;} \\ \dfrac{p^{a+1} + 2p + 1}{2(p+1)}, & \text{if } p \neq 2 \text{ and if } a \text{ is odd;} \\ \dfrac{2^{a-1} + 4}{3}, & \text{if } p = 2 \text{ and if } a \text{ is even;} \\ \dfrac{2^{a-1} + 5}{3}, & \text{if } p = 2 \text{ and if } a \text{ is odd.} \end{cases}$$

[3] Plugging this into (1), we obtain a formula for the # of squares in $\mathbb{Z}/n$.

- What is an integer a that leaves the remainder 3 when divided by 5, the remainder 2 when divided by 6 and the remainder 9 when divided by 23 ?

  This is just asking for an integer a that satisfies $\overline{a} = \overline{3}$ in $\mathbb{Z}/5$, satisfies $\overline{a} = \overline{2}$ in $\mathbb{Z}/6$ and satisfies $\overline{a} = \overline{9}$ in $\mathbb{Z}/23$. In other words, this is asking

[1] See the solution to Exercise 5 on homework set #6 of my Spring 2019 Math 4281 class for a detailed version of this proof.

[2] See the solution to Exercise 4 on homework set #2 of my Winter 2021 Math 533 class for a proof.

[3] Don't be surprised about the denominators in the fractions; those are obtained by summing geometric sequences.

for an integer a whose image under the ring morphism

$$\begin{aligned} \mathbb{Z} &\to (\mathbb{Z}/5) \times (\mathbb{Z}/6) \times (\mathbb{Z}/23), \\ r &\mapsto (\overline{r}, \overline{r}, \overline{r}) \end{aligned}$$

is the triple $\left(\overline{3}, \overline{2}, \overline{9}\right)$.

Since the integers $5, 6, 23$ are mutually coprime, the Chinese Remainder Theorem (Theorem 1.12.8) shows that there is a ring isomorphism

$$\begin{aligned} \mathbb{Z}/\left(5 \cdot 6 \cdot 23\right) &\to (\mathbb{Z}/5) \times (\mathbb{Z}/6) \times (\mathbb{Z}/23), \\ \overline{r} &\mapsto (\overline{r}, \overline{r}, \overline{r}). \end{aligned}$$

By tracking our way through the proof of this theorem, we can obtain an algorithm for constructing the inverse of this isomorphism[4], and thus we can find that the preimage of the triple $\left(\overline{3}, \overline{2}, \overline{9}\right) \in (\mathbb{Z}/5) \times (\mathbb{Z}/6) \times (\mathbb{Z}/23)$ under this isomorphism is $\overline{308}$. Thus, the integer a we are looking for satisfies $\overline{a} = \overline{308}$ in $\mathbb{Z}/\left(5 \cdot 6 \cdot 23\right)$, and conversely, any integer a satisfying $\overline{a} = \overline{308}$ in $\mathbb{Z}/\left(5 \cdot 6 \cdot 23\right)$ will work. The simplest answer is of course $a = 308$, but there are infinitely many others.

Problems like this are how the Chinese Remainder Theorem got its name.

- A more down-to-earth application of the Chinese Remainder Theorem is a technique known as **Chinese remaindering**. It can be used to parallelize computations with large integers, saving both on running time and on memory usage. A real-life example of this is given in [Vogan07, pp. 1031–1033].

[4]Specifically, we recall that Theorem 1.12.8 is proved using Theorem 1.12.7, which in turn is proved by induction using Proposition 1.12.5 and using the Chinese Remainder Theorem for two ideals twice. All these results have been proved constructively, so reading their proofs will give us algorithms for all the isomorphisms they claim.

Explicitly, re-reading the proof of the Chinese Remainder Theorem for two ideals (Lecture 13), we see that if I and J are two comaximal ideals of a ring R, then the inverse of the isomorphism

$$\begin{aligned} f' : R/\left(IJ\right) &\to R/I \times R/J, \\ \overline{r} &\mapsto (\overline{r}, \overline{r}) \end{aligned}$$

sends each pair $(\overline{x}, \overline{y})$ to $\overline{yi + xj}$, where $i \in I$ and $j \in J$ are two elements chosen to satisfy $1 = i + j$. Thus, in order to compute preimages under this isomorphism, we need to find two elements $i \in I$ and $j \in J$ satisfying $1 = i + j$ (that is, "witnessing" the comaximality of I and J). In our case, I and J are principal ideals of $\mathbb{Z}$, and thus we can find our i and j using the extended Euclidean algorithm (which takes two integers a and b as inputs and produces integers x and y satisfying $xa + yb = \gcd(a, b)$). Specifically, this algorithm lets us write 1 in the form $x \cdot 5 + y \cdot 6$ (which is needed to invert the isomorphism $\mathbb{Z}/\left(5 \cdot 6\right) \to (\mathbb{Z}/5) \times (\mathbb{Z}/6)$) and write 1 in the form $x \cdot 5 \cdot 6 + y \cdot 23$ (which is needed to invert the isomorphism $\mathbb{Z}/\left(5 \cdot 6 \cdot 23\right) \to (\mathbb{Z}/5) \times (\mathbb{Z}/6) \times (\mathbb{Z}/23)$).

Since this is not a course on computational algebra, I will leave it at these laconic hints.

Let us here give a toy example.

Assume we want to compute

$$a := 77^2 \cdot 80^2 - 78^2 \cdot 79^2.$$

Assume that we are unable/unwilling to do arithmetic with numbers this high (OMG 8 digits!), and also unwilling to simplify our life by finding a factorization[5]. However, for some theoretical reasons, we know that the magnitude of a is not too high: say, $-50\,000 < a < 50\,000$. (Such estimates often fall out of theoretical considerations.)

What can we do?

Well, we can easily compute the residue class $\overline{a}$ in $\mathbb{Z}/5$ by first reducing the relevant integers 77, 80, 78, 79 to their remainders upon division by 5 (warning: do not reduce the exponents![6]) and then performing the rest of the computation (squaring, multiplying and subtracting) within $\mathbb{Z}/5$:

$$\begin{aligned}
\overline{a} &= \overline{77^2 \cdot 80^2 - 78^2 \cdot 79^2} \\
&= \overline{77}^2 \cdot \overline{80}^2 - \overline{78}^2 \cdot \overline{79}^2 \\
&= \overline{2}^2 \cdot \overline{0}^2 - \overline{3}^2 \cdot \overline{4}^2 \qquad \left(\begin{array}{c} \text{here, we reduced the numbers} \\ \text{to their remainders} \end{array} \right) \\
&= \overline{4} \cdot \overline{0} - \overline{4} \cdot \overline{1} = \overline{0} - \overline{4} = \overline{-4} = \overline{1}.
\end{aligned}$$

Likewise, we can compute the residue classes $\overline{a}$ in $\mathbb{Z}/2$ and $\mathbb{Z}/3$ and $\mathbb{Z}/7$ and $\mathbb{Z}/11$ and $\mathbb{Z}/13$ and $\mathbb{Z}/17$ and so on (there are infinitely many primes, after all, but we only need these few). Thus, we easily find the tuple

$$(\overline{a}, \overline{a}, \overline{a}, \overline{a}, \overline{a}, \overline{a}, \overline{a}) \in \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/11 \times \mathbb{Z}/13 \times \mathbb{Z}/17.$$

However, the primes $2, 3, 5, 7, 11, 13, 17$ are mutually coprime, and thus the Chinese Remainder Theorem yields a ring isomorphism

$$\begin{aligned}
\mathbb{Z}/\left(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17\right) &\to \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/11 \times \mathbb{Z}/13 \times \mathbb{Z}/17, \\
\overline{r} &\mapsto \left(\overline{r}, \overline{r}, \overline{r}, \overline{r}, \overline{r}, \overline{r}, \overline{r}\right),
\end{aligned}$$

whose inverse we can algorithmically construct. Applying this inverse to the tuple $(\overline{a}, \overline{a}, \overline{a}, \overline{a}, \overline{a}, \overline{a}, \overline{a})$ (which has already been found), we obtain the residue class $\overline{a} \in \mathbb{Z}/\left(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17\right)$. In other words, we obtain the residue class $\overline{a} \in \mathbb{Z}/\left(510\,510\right)$ (since $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 510\,510$).

[5] This is not as unrealistic as it sounds. Not all factorizations are as evident as $x^2 - y^2 = (x - y)(x + y)$, and in practice, the Chinese Remainder Theorem is often used for factoring polynomials.

[6] Of course, the exponents here are 2, so the temptation does not arise in the first place.

But we also know that $-50\ 000 < a < 50\ 000$, so that a lies in the open interval $(-50\ 000,\ 50\ 000)$. Any two distinct integers in this interval have distinct residue classes in $\mathbb{Z}/(510\,510)$, and any integer in this interval can be easily reconstructed from its residue class. Thus, we can easily reconstruct a from $\overline{a}$. In our specific example, we obtain $a = -24\,644$.

This method is particularly good for parallel computing, as the computations of $\overline{a}$ in different quotient rings $\mathbb{Z}/n$ can be done in parallel. It also saves on memory, since working in $\mathbb{Z}/n$ requires less memory than working with "big" integers. (The extended Euclidean algorithm, on which the computation of the inverse isomorphism relies, is really fast and not very memory-consuming, so the last step of the method is not a heavy burden.)

See [Knuth98, §4.3.2] for more details on Chinese remaindering.

More applications of the Chinese Remainder Theorem can be found in `https://mathoverflow.net/questions/10014/` . (As you have surely noticed, the theorem comes in many forms, some rather elementary; our Theorem 1.12.7 is one of the most general.)

References

[Knuth98] Donald Ervin Knuth, *The art of computer programming, volume 2*, Addison–Wesley 1998.

[Stangl96] Walter D. Stangl, *Counting squares in $\mathbb{Z}_n$*, Mathematics Magazine **69** (1996), no. 4 (October), pp. 285–289.

[Vogan07] David Vogan, *The Character Table for E_8*, Notices of the American Mathematical Society 2007/09.