# Algebraic Number Theory, a Computational Approach

William Stein

May 5, 2019

# Chapter 1

# The Chinese Remainder Theorem

In this chapter, we prove the Chinese Remainder Theorem (CRT) for arbitrary commutative rings, then apply CRT to prove that every ideal in a Dedekind domain $R$ is generated by at most two elements. We also prove that $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is (noncanonically) isomorphic to $R/\mathfrak{p}$ as an $R$-module, for any nonzero prime ideal $\mathfrak{p}$ of $R$. The tools we develop in this chapter will be used frequently to prove other results later.

## 1.1 The Chinese Remainder Theorem

### 1.1.1 CRT in the Integers

The classical CRT asserts that if $n_1, \ldots, n_r$ are integers that are coprime in pairs, and $a_1, \ldots, a_r$ are integers, then there exists an integer $a$ such that $a \equiv a_i \pmod{n_i}$ for each $i = 1, \ldots, r$. Here "coprime in pairs" means that $\gcd(n_i, n_j) = 1$ whenever $i \neq j$; it does *not* mean that $\gcd(n_1, \ldots, n_r) = 1$, though it implies this. In terms of rings, CRT asserts that the natural map

$$\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_r\mathbb{Z}) \tag{1.1}$$

that sends $a \in \mathbb{Z}$ to its reduction modulo each $n_i$, is an isomorphism.

This map is *never* an isomorphism if the $n_i$ are not coprime. Indeed, the cardinality of the image of the left hand side of (1.1) is $\mathrm{lcm}(n_1, \ldots, n_r)$, since it is the image of a cyclic group and $\mathrm{lcm}(n_1, \ldots, n_r)$ is the largest order of an element of the right hand side, whereas the cardinality of the right hand side is $n_1 \cdots n_r$.

The isomorphism (1.1) can alternatively be viewed as asserting that any system of linear congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_r \pmod{n_r}$$

with pairwise coprime moduli has a unique solution modulo $n_1 \cdots n_r$.

Before proving the CRT in more generality, we prove (1.1). There is a natural map

$$\phi : \mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_r\mathbb{Z})$$

given by projection onto each factor. Its kernel is

$$n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z}.$$

If $n$ and $m$ are integers, then $n\mathbb{Z} \cap m\mathbb{Z}$ is the set of multiples of both $n$ and $m$, so $n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{lcm}(n, m)\mathbb{Z}$. Since the $n_i$ are coprime,

$$n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z} = n_1 \cdots n_r\mathbb{Z}.$$

Thus we have proved there is an inclusion

$$i : \mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z} \hookrightarrow (\mathbb{Z}/n_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_r\mathbb{Z}). \tag{1.2}$$

This is half of the CRT; the other half is to prove that this map is surjective. In this case, it is clear that $i$ is also surjective, because $i$ is an injective map between finite sets of the same cardinality. We will, however, give a proof of surjectivity that doesn't use finiteness of the above two sets.

To prove surjectivity of $i$, note that since the $n_i$ are coprime in pairs,

$$\gcd(n_1, n_2 \cdots n_r) = 1,$$

so there exists integers $x, y$ such that

$$xn_1 + yn_2 \cdots n_r = 1.$$

To complete the proof, observe that $yn_2 \cdots n_r = 1 - xn_1$ is congruent to 1 modulo $n_1$ and 0 modulo $n_2 \cdots n_r$. Thus $(1, 0, \ldots, 0) = i(yn_2 \cdots n_r)$ is in the image of $i$. By a similar argument, we see that $(0, 1, \ldots, 0)$ and the other similar elements are all in the image of $i$, so $i$ is surjective, which proves CRT.

### 1.1.2 CRT in General

Recall that *all rings in this book are commutative with unity*. Let $R$ be such a ring.

**Definition 1.1.1** (Coprime)**.** Ideals $I$ and $J$ of $R$ are *coprime* if $I+J=(1)$.

**Exercise 1.1.2.** Let $a_1 = 1+i$, $a_2 = 3+2i$, and $a_3 = 3+4i$ as elements of $\mathbb{Z}[i]$.

1. Prove that the ideals $I_1 = (a_1)$, $I_2 = (a_2)$, and $I_3 = (a_3)$ are coprime in pairs.

2. Compute the cardinality of $\mathbb{Z}[i]/(I_1 I_2 I_3)$.

3. Find a single element in $\mathbb{Z}[i]$ that is congruent to $n$ modulo $I_n$, for each $n \leq 3$.

For example, if $I$ and $J$ are nonzero ideals in a Dedekind domain, then they are coprime precisely when the prime ideals that appear in their two (unique) factorizations are disjoint.

**Lemma 1.1.3.** *If $I$ and $J$ are coprime ideals in a ring $R$, then $I \cap J = IJ$.*

*Proof.* Choose $x \in I$ and $y \in J$ such that $x+y=1$. If $c \in I \cap J$ then

$$c = c \cdot 1 = c \cdot (x+y) = cx + cy \in IJ + IJ = IJ,$$

so $I \cap J \subset IJ$. The other inclusion is obvious by the definition of an ideal. □

**Lemma 1.1.4.** *Suppose $I_1, \ldots, I_s$ are pairwise coprime ideals. Then $I_1$ is coprime to the product $I_2 \cdots I_s$.*

*Proof.* In the special case of a Dedekind domain, we could easily prove this lemma using unique factorization of ideals as products of primes (Theorem **??**); instead, we give a direct general argument.

It suffices to prove the lemma in the case $s=3$, since the general case then follows from induction. By assumption, there are $x_1 \in I_1, y_2 \in I_2$ and $a_1 \in I_1, b_3 \in I_3$ such

$$x_1 + y_2 = 1 \qquad \text{and} \qquad a_1 + b_3 = 1.$$

Multiplying these two relations yields

$$x_1 a_1 + x_1 b_3 + y_2 a_1 + y_2 b_3 = 1 \cdot 1 = 1.$$

The first three terms are in $I_1$ and the last term is in $I_2 I_3 = I_2 \cap I_3$ (by Lemma 1.1.3), so $I_1$ is coprime to $I_2 I_3$. □

Next we prove the general Chinese Remainder Theorem. We will apply this result with $R = \mathcal{O}_K$ in the rest of this chapter.

**Theorem 1.1.5** (Chinese Remainder Theorem)**.** *Suppose $I_1, \ldots, I_r$ are nonzero ideals of a ring $R$ such $I_m$ and $I_n$ are coprime for any $m \neq n$. Then the natural homomorphism $R \to \bigoplus_{n=1}^r R/I_n$ induces an isomorphism*

$$\psi : R/\prod_{n=1}^{r} I_n \to \bigoplus_{n=1}^{r} R/I_n.$$

*Thus given any $a_n \in R$, for $n = 1, \ldots, r$, there exists some $a \in R$ such that $a \equiv a_n \pmod{I_n}$ for $n = 1, \ldots, r$; moreover, $a$ is unique modulo $\prod_{n=1}^r I_n$.*

*Proof.* Let $\varphi : R \to \bigoplus_{n=1}^r R/I_n$ be the natural map induced by reduction modulo the $I_n$. An inductive application of Lemma 1.1.3 implies that the kernel $\cap_{n=1}^r I_n$ of $\varphi$ is equal to $\prod_{n=1}^r I_n$, so the map $\psi$ of the theorem is injective.

Each projection $R \to R/I_n$ is surjective, so to prove that $\psi$ is surjective, it suffices to show that $(1, 0, \ldots, 0)$ is in the image of $\varphi$, and similarly for the other factors. By Lemma 1.1.4, $J = \prod_{n=2}^r I_n$ is coprime to $I_1$, so there exists $x \in I_1$ and $y \in J$ such that $x + y = 1$. Then $y = 1 - x$ maps to 1 in $R/I_1$ and to 0 in $R/J$, hence to 0 in $R/I_n$ for each $n \geq 2$, since $J \subset I_n$. $\square$

## 1.2 Structural Applications of the CRT

Let $\mathcal{O}_K$ be the ring of integers of some number field $K$, and suppose $I$ is a nonzero ideal of $\mathcal{O}_K$. As an abelian group $\mathcal{O}_K$ is free of rank $[K : \mathbb{Q}]$, and $I$ is of finite index in $\mathcal{O}_K$, so $I$ is generated by $[K : \mathbb{Q}]$ generators as an abelian group, so as an $R$-ideal $I$ requires at most $[K : \mathbb{Q}]$ generators. The main result of this section asserts something better, namely that $I$ can be generated *as an ideal* by at most two elements. Moreover, our result is more general, since it applies to an arbitrary Dedekind domain $R$. Thus, for the rest of this section, $R$ is any Dedekind domain, e.g., the ring of integers of either a number field or function field. We use CRT to prove that every ideal of $R$ can be generated by two elements.

**Warning 1.2.1.** If we replace $R$ by an order in a Dedekind domain, i.e., by a subring of finite index, then there may be ideals that require far more than 2 generators.

Suppose that $I$ is a nonzero integral ideal of $R$. If $a \in I$, then $(a) \subset I$, so $I$ divides $(a)$ and the quotient $(a)I^{-1}$ is an integral ideal. The following lemma asserts that $(a)$ can be chosen so the quotient $(a)I^{-1}$ is coprime to any given ideal.

**Lemma 1.2.2.** *If $I$ and $J$ are nonzero integral ideals in $R$, then there exists an $a \in I$ such that the integral ideal $(a)I^{-1}$ is coprime to $J$.*

Before we give the proof in general, note that the lemma is trivial when $I$ is principal, since if $I = (b)$, just take $a = b$, and then $(a)I^{-1} = (a)(a^{-1}) = (1)$ is coprime to every ideal.

*Proof.* Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime divisors of $J$. For each $n$, let $v_n$ be the largest power of $\mathfrak{p}_n$ that divides $I$. Since $\mathfrak{p}_n^{v_n} \neq \mathfrak{p}_n^{v_n+1}$, we can choose an element $a_n \in \mathfrak{p}_n^{v_n}$ that is not in $\mathfrak{p}_n^{v_n+1}$. By Theorem 1.1.5 applied to the $r+1$ coprime integral ideals

$$\mathfrak{p}_1^{v_1+1}, \ldots, \mathfrak{p}_r^{v_r+1},\ I \cdot \left(\prod \mathfrak{p}_n^{v_n}\right)^{-1},$$

there exists $a \in R$ such that

$$a \equiv a_n \pmod{\mathfrak{p}_n^{v_n+1}}$$

for all $n = 1, \ldots, r$ and also

$$a \equiv 0 \quad \left(\bmod\ I \cdot \left(\prod \mathfrak{p}_n^{v_n}\right)^{-1}\right).$$

To complete the proof we show that $(a)I^{-1}$ is not divisible by any $\mathfrak{p}_n$, or equivalently, that each $\mathfrak{p}_n^{v_n}$ exactly divides $(a)$. First we show that $\mathfrak{p}_n^{v_n}$ divides $(a)$. Because $a \equiv a_n \pmod{\mathfrak{p}_n^{v_n+1}}$, there exists $b \in \mathfrak{p}_n^{v_n+1}$ such that $a = a_n + b$. Since $a_n \in \mathfrak{p}_n^{v_n}$ and $b \in \mathfrak{p}_n^{v_n+1} \subset \mathfrak{p}_n^{v_n}$, it follows that $a \in \mathfrak{p}_n^{v_n}$, so $\mathfrak{p}_n^{v_n}$ divides $(a)$. Now assume for the sake of contradiction that $\mathfrak{p}_n^{v_n+1}$ divides $(a)$; then $a_n = a - b \in \mathfrak{p}_n^{v_n+1}$, which contradicts that we chose $a_n \notin \mathfrak{p}_n^{v_n+1}$. Thus $\mathfrak{p}_n^{v_n+1}$ does not divide $(a)$, as claimed. $\square$

**Proposition 1.2.3.** *Suppose $I$ is a fractional ideal in a Dedekind domain $R$. Then there exist $a, b \in K$ such that $I = (a, b) = \{\alpha a + \beta b : \alpha, \beta \in R\}$.*

*Proof.* If $I = (0)$, then $I$ is generated by 1 element and we are done. If $I$ is not an integral ideal, then there is an $x \in K$ such that $xI$ is an integral ideal, and the number of generators of $xI$ is the same as the number of generators of $I$, so we may assume that $I$ is an integral ideal.

Let $a$ be *any* nonzero element of the integral ideal $I$. We will show that there is some $b \in I$ such that $I = (a, b)$. Let $J = (a)$. By Lemma 1.2.2, there exists $b \in I$ such that $(b)I^{-1}$ is coprime to $(a)$. Since $a, b \in I$, we have $I \mid (a)$ and $I \mid (b)$, so $I \mid (a, b)$. Suppose $\mathfrak{p}^n \mid (a, b)$ with $\mathfrak{p}$ prime and $n \geq 1$. Then $\mathfrak{p}^n \mid (a)$ and $\mathfrak{p}^n \mid (b)$, so $\mathfrak{p} \nmid (b)I^{-1}$, since $(b)I^{-1}$ is coprime to $(a)$. We have $\mathfrak{p}^n \mid (b) = I \cdot (b)I^{-1}$ and $\mathfrak{p} \nmid (b)I^{-1}$, so $\mathfrak{p}^n \mid I$. Thus by unique factorization of ideals in $R$ we have that $(a, b) \mid I$. Since $I \mid (a, b)$ we conclude that $I = (a, b)$, as claimed. □

We can also use Theorem 1.1.5 to determine the $R$-module structure of $\mathfrak{p}^n/\mathfrak{p}^{n+1}$.

**Proposition 1.2.4.** *Let $\mathfrak{p}$ be a nonzero prime ideal of $R$, and let $n \geq 0$ be an integer. Then $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$ as $R$-modules.*

*Proof* [1]. Since $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$, by unique factorization, there is an element $b \in \mathfrak{p}^n$ such that $b \notin \mathfrak{p}^{n+1}$. Let $\varphi : R \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ be the $R$-module morphism defined by $\varphi(a) = ab$. The kernel of $\varphi$ is $\mathfrak{p}$ since clearly $\varphi(\mathfrak{p}) = 0$ and if $\varphi(a) = 0$ then $ab \in \mathfrak{p}^{n+1}$, so $\mathfrak{p}^{n+1} \mid (a)(b)$, so $\mathfrak{p} \mid (a)$, since $\mathfrak{p}^{n+1}$ does not divide $(b)$. Thus $\varphi$ induces an injective $R$-module homomorphism $R/\mathfrak{p} \hookrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1}$.

It remains to show that $\varphi$ is surjective, and this is where we will use Theorem 1.1.5. Suppose $c \in \mathfrak{p}^n$. By Theorem 1.1.5 there exists $d \in R$ such that

$$d \equiv c \pmod{\mathfrak{p}^{n+1}} \qquad \text{and} \qquad d \equiv 0 \pmod{(b)/\mathfrak{p}^n}.$$

We have $\mathfrak{p}^n \mid (d)$ since $d \in \mathfrak{p}^n$ and $(b)/\mathfrak{p}^n \mid (d)$ by the second displayed condition, so since $\mathfrak{p} \nmid (b)/\mathfrak{p}^n$, we have $(b) = \mathfrak{p}^n \cdot (b)/\mathfrak{p}^n \mid (d)$, hence $d/b \in R$. Finally

$$\varphi\left(\frac{d}{b}\right) \equiv \frac{d}{b} \cdot b \pmod{\mathfrak{p}^{n+1}} \equiv d \pmod{\mathfrak{p}^{n+1}} \equiv c \pmod{\mathfrak{p}^{n+1}},$$

so $\varphi$ is surjective. □

**Exercise 1.2.5.** (See [Mar77, Thm. 22(a)]) Let $R$ be a Dedekind domain and $\mathfrak{p}$ a nonzero prime ideal in $R$. Show that $\#(R/\mathfrak{p}^m) = \#(R/\mathfrak{p})^m$.

Note: $\#(R/\mathfrak{p})$ is not finite in general! For example, The ring of formal power series $k[[t]]$ for some field $k$ is a Dedekind domain and the residue field at the prime $(t)$ is $k$.

[*Hint*: Consider the exact sequence

$$0 \to \mathfrak{p}/\mathfrak{p}^m \to R/\mathfrak{p}^m \to R/\mathfrak{p}^{m-1} \to 0$$

and the chain

$$\mathfrak{p}^m \subseteq \mathfrak{p}^{m-1} \subseteq \cdots \subseteq \mathfrak{p}^2 \subseteq \mathfrak{p}.$$

]

*Remark* 1.2.6. There is one special case of the previous exercise that you probably have seen before: the size of $\mathbb{Z}/4\mathbb{Z}$ is the same as $(\mathbb{Z}/2\mathbb{Z})^2$. In fact you might have seen a proof of the fact that $\mathbb{Z}/n^m\mathbb{Z}$ has the same cardinality as $(\mathbb{Z}/n\mathbb{Z})^m$ in a standard group theory or abstract algebra course.

## 1.3 Computing Using the CRT

In order to explicitly compute an $a$ as given by Theorem 1.1.5, usually one first precomputes elements $v_1, \ldots, v_r \in R$ such that $v_1 \mapsto (1, 0, \ldots, 0)$, $v_2 \mapsto (0, 1, \ldots, 0)$, etc. Then given any $a_n \in R$, for $n = 1, \ldots, r$, we obtain an $a \in R$ with $a_n \equiv a \pmod{I_n}$ by taking

$$a = a_1 v_1 + \cdots + a_r v_r.$$

How to compute the $v_i$ depends on the ring $R$. It reduces to the following problem: Given coprimes ideals $I, J \subset R$, find $x \in I$ and $y \in J$ such that $x + y = 1$. If $R$ is torsion free and of finite rank as a $\mathbb{Z}$-module, so $R \approx \mathbb{Z}^n$, then $I, J$ can be represented by giving a basis in terms of a basis for $R$, and finding $x, y$ such that $x + y = 1$ can then be reduced to a problem in linear algebra over $\mathbb{Z}$. More precisely, let $A$ be the matrix whose columns are the concatenation of a basis for $I$ with a basis for $J$. Suppose $v \in \mathbb{Z}^n$ corresponds to $1 \in \mathbb{Z}^n$. Then finding $x, y$ such that $x + y = 1$ is equivalent to finding a solution $z \in \mathbb{Z}^n$ to the matrix equation $Az = v$. This latter linear algebra problem can be solved using or (see [Coh93, §4.7.1]), which is a generalization over $\mathbb{Z}$ of reduced row echelon form.

Next we give an explicit example of a CRT computation using `Sage`. Let $K = \mathbb{Q}(\sqrt{-1})$ and $R = \mathcal{O}_K$. We will set $I = (1 + i)$ and $J = (3)$.

```
K.<i> = QuadraticField(-1)
d = K.degree()
I = K.ideal(1 + i)
J = K.ideal(3)
```

Number fields in `Sage` come with a $\mathbb{Q}$-vector space isomorphism $K \to \mathbb{Q}^d$, where $d = \deg K$. To turn an element $\alpha \in K$ into a vector, we use the `vector()` method. We can build the matrix $A$ described above as follows.

```
rows = [x.vector() for x in I.basis() + J.basis()]
A = Matrix(ZZ,rows).transpose()
```

Next we compute the Smith normal form $S$ of $A$, along with matrices $T, U$ such that $S = TAU$.

```
S,T,U = A.smith_form(transformation=True)
```

We have the following chain of $\mathbb{Z}$-linear maps

$$\mathbb{Z}^{2d} \xrightarrow{U} \mathbb{Z}^{2d} \xrightarrow{A} \mathbb{Z}^{d} \xrightarrow{T} \mathbb{Z}^{d}.$$

The matrix $S$ represents the composition. The cokernel of matrix $A$ is trivial since $\mathcal{O}_K/(I+J) = 0$. Therefore $S$ is of the form $\begin{pmatrix} I_d & 0 \end{pmatrix}$ (see Section **??**). In particular, $SS^t = I_d$. So we can find a solution to $Az = v$ for any $v \in \mathbb{Z}^d$ by computing $z = US^tTv$. Then $Az = AUS^tTv = T^{-1}SU^{-1}US^tTv = v$.

check transpose syntax

Next we find the solution $z$ for the equation $Az = v$ where the vector $v$ is the vector corresponding to 1.

```
v = K(1).vector()
z = T*S.transpose()*U*K(1)
```

Recall that the first half of the columns of $A$ represent a basis for $I$, and the second half represents a basis for $J$. Using the entries of **z** as coefficients, we can find elements $x \in I$ and $y \in J$ such that $x + y = 1$.

```
x = sum(z[i]*I.basis()[i] for i in range(d))
y = sum(z[d+i]*J.basis()[i] for i in range(d))
print x + y
```

```
1
```

Our value of $x$ and $y$ can be used to solve for $a \in \mathcal{O}_K$ such that $a \equiv a_1 \pmod{I}$ and $a \equiv a_2 \pmod{J}$ for any given $a_1, a_2$. We demonstrate this with $a_1 = 17 + i$ and $a_2 = 2 + 11i$.

```
a1 = 17 + i
a2 = 2 + 11*i
a = x*a2 + y*a1
print (a - a1 in I) and (a - a2 in J)
```

```
True
```

# Bibliography

[Art91] M. Artin, *Algebra*, Prentice Hall Inc., Englewood Cliffs, NJ, 1991. MR 92g:00001

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105

[KKM11] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes, *Elliptic curve cryptography: The serpentine course of a paradigm shift*, Journal of Number Theory **131** (2011), no. 5, 781 – 814, Elliptic Curve Cryptography.

[Mar77] Daniel A. Marcus, *Number Fields*, Universitext (1979), Springer, 1977.

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001. MR 2002a:11117