Chapter 17

PID's and CRT's

17.I The Chinese Remainder Theorem, I.

We will state and prove the Chinese Remainder Theorem in 2 versions. First, as an existence (and uniqueness) theorem on solutions of simultaneous congruences. Then, as a structure theorem on quotient rings of a P.I.D.

"*Ring*" still means "commutative ring with 1".

17.I.1 Definition: Let $I_1, I_2, \ldots, I_d$ be ideals of the ring R. The **product ideal** $I_1 \cdot I_2 \cdot \ldots \cdot I_d$ is the ideal consisting of sums of products $m_1 \cdot m_2 \cdot \ldots m_d$ with $m_k \in I_k$

Obviously, the product of a sequence of ideals is itself an ideal. It is contained in each I_k, hence in their intersection, by the defining properties of ideals. If the ideals I_k are *principal ideals*, $I_k = (m_k)$, then, simply, $I_1 \cdot I_2 \cdot \ldots I_d = (m_1 \cdot m_2 \cdot \ldots \cdot m_d)$.

More generally we get a system of generators for the product ideal by multiplying generators for one ideal with generators for the other. E.g.,

$$(a, b)(c, d) = (ac, ad, bc, bd).$$

The proof of equality proceeds by mutual inclusion - a typical element of one ideal is rewritten as an element of the other.

The product may be strictly contained in the intersection. This is illustrated by the simple example $(4) \cdot (6) = (24)$, $(4) \cap (6) = (12)$. Note that $12 = 6 \cdot 4/(6, 4)$.

The typical situation in which to expect equality is given by the following definition.

17.I.2 Definition: The ideals $I_1, I_2, \ldots, I_d$ are said to be **pairwise comaximal** if, for each $i, j, i \neq j$,

$$I_i + I_j = R$$

17.I.3 Example: In a P.I.D. R two ideals $(m_1), (m_2)$ are comaximal if, and only if, the ideal generated by m_1 and m_2 contains 1, i.e., iff there are elements $\alpha_1, \alpha_2 \in R$ with

$$\alpha_1 m_1 + \alpha_2 m_2 = 1$$

i.e., iff the m_i have no non-trivial common factor. (Bézout.) ∎

From now on, we will usually assume that R is a P.I.D. Most of the results, and their proofs, hold for general commutative rings (with identity), *mutatis mutandis.*

17.I.4 Lemma. *If the ideals I_k are pairwise comaximal, then*

$$I_1 + I_2 \cdot \ldots \cdot I_d = R$$

Proof: The case $d = 3$ is enough to illustrate the idea of the proof. By assumption

$$I_1 + I_2 = R$$

$$I_1 + I_3 = R$$

From this we infer

$$R = R^2 = (I_1 + I_2)(I_1 + I_3) = I_1^2 + I_1 I_2 + I_1 I_3 + I_2 I_3 \subset I_1 + I_2 I_3$$

The first equality follows because R has an indentity element by assumption. The third follows by mutual inclusion, rewriting an element of either memeber as an element of the other. And the last one follows because the first three terms are subideals of I_1

▮

The general case is proved by replacing 3 with d and inserting some dots.

In the case of a PID, the case $d = 3$ says that $(m_1, m_2) = 1, (m_1, m_3) = 1$ implies $(m_1, m_2 m_3) = 1$.

17.I.5 Theorem. *Same assumptions. Then*

$$I_1 \cap I_2 \cap \ldots \cap I_d = I_1 \cdot I_2 \cdot \ldots \cdot I_d$$

Proof: We start first with the case $d = 2$. We are assuming $I_1 + I_2 = R$. Therefore:

$$I_1 \cap I_2 = (I_1 \cap I_2) \cdot (I_1 + I_2) = (I_1 \cap I_2) \cdot I_1 + (I_1 \cap I_2) \cdot I_2 \subset I_2 \cdot I_1 + I_1 \cdot I_2 = I_1 \cdot I_2$$

The reverse inclusion has already been dealt with.

The general case proceeds by induction on the number of ideals. The induction hypothesis, and then the case $d = 2$, yield

$$\begin{aligned} I_1 \cap (I_2 \cap \ldots \cap I_d) &= I_1 \cap (I_2 \cdot \ldots \cdot I_d) \\ &= I_1 \cdot I_2 \cdot \ldots \cdot I_d \end{aligned}$$

where we also used that I_1 and $I_2 \cdots I_d$ are comaximal, by the lemma. ▮

17.I.6 Theorem. Chinese Remainder Theorem I. *Let $a_i, i = 1, 2, \ldots, d$, and $I_i, i = 1, 2, \ldots, d$ be given ideals of R, pairwise co-maximal. Then the system of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{I_1} \\ x &\equiv a_2 \pmod{I_2} \\ &\cdots \\ x &\equiv a_d \pmod{I_d} \end{aligned}$$

has a unique solution modulo $I_1 \cdot I_2 \cdots I_d$

Thus, in the PID case, $I_k = (m_k)$, the m_k pairwise relatively prime, the general solution is of the form

$$x = x_0 + r m_1 m_2 \cdots m_d; \ r \in R$$

Proof: *Existence:* It is enough to solve, for each fixed i, the system

$$x_i \equiv \delta_{ij} \pmod{I_j}, j = 1, 2, \ldots, d$$

($\delta_{ij} := 1$ if $i = j$, $\delta_{ij} = 0$ otherwise, "Kronecker delta")

The system of the statement above is then satisfied by $x = \sum_{i=1}^{d} a_i x_i$ (superposition, exercise).

For notational convenience we consider only $i = 1$:

$$\begin{aligned} x_1 &\equiv 1 \pmod{I_1} \\ x_1 &\equiv 0 \pmod{I_j}, \ j \neq 1 \end{aligned}$$

By lemma I.4. we have

$$I_1 + I_2 \cdot \ldots \cdot I_d = (1)$$

so there are elements $e_0 \in I_1$, $e_1 \in I_2 \cdot \ldots \cdot I_d$ satisfying

$$e_0 + e_1 = 1$$

Obviously, $x_1 = e_1$ does the trick!

Uniqueness: If x, x' are two solutions, then we have $x - x' \equiv a_j - a_j = 0 \pmod{I_j}$ $\forall j$, i.e., $x - x'$ belongs to the intersection of the I_j, hence to their product, by comaximality. (17.I.V) ∎

17.I.7 Example: At least for hand calculations there are two ways to solve a Chinese Congruence System.

Suppose we are to solve the system

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

with $3, 5, 7$ obviously relatively prime in pairs. We start by solving Bézout:

$$r_1 \cdot 3 + r_2 \cdot 5 = 1, \qquad 2 \cdot 3 - 1 \cdot 5 = 6 - 5 = 1$$

with

$$-5 \equiv 1 \pmod 3$$
$$-5 \equiv 0 \pmod 5$$

and

$$6 \equiv 0 \pmod 3$$
$$6 \equiv 1 \pmod 5$$

The solution to the first two congruences is then

$$x \equiv 1 \cdot (-5) + 2 \cdot 6 \equiv 7 \pmod{3 \cdot 5}$$

This is then combined with the third congruence, and the two together are treated exactly the same way as the first two:

$$\begin{aligned} x &\equiv 7 \pmod{15} \\ x &\equiv 3 \pmod 7 \end{aligned},$$

Solve Bézout again:

$$1 \cdot 15 - 2 \cdot 7 = 1, \qquad 15 - 14 = 1$$

and another superposition gives us:

$$x \equiv 7 \cdot (-14) + 3 \cdot 15 \equiv -53 \equiv 52 \pmod{15 \cdot 7}$$

that is,

$$x \equiv 52 \pmod{105}$$

We could also solve three Bézout identities. Let $m_1 = 3, m_2 = 5, m_3 = 7$ Putting $M = m_1 m_2 m_3, M_i = M/M_i$ we determine $r_i, s_i \quad i = 1, 2, 3$ such that

$$r_i M_i + s_i m_i = 1, \quad i = \quad 1, 2, 3$$

Putting $x_i = r_i M_i$ we see that $x_i \equiv 1 \pmod{m_i}$ and $x_i \equiv 0 \pmod{M_i}$, that is, $x_i \equiv 0 \pmod{m_j}$, $j \neq i$.

The solution is then

$$x \equiv a_1 x_1 + a_2 x_2 + a_3 x_3 \pmod{m_1 m_2 m_3}$$

with, in this case, $a_1 = 1, a_2 = 2, a_3 = 3$

In our numerical example we get:

$$12 \cdot 3 - 1 \cdot (5 \cdot 7) = 36 - 35 = 1$$
$$-4 \cdot 5 + 1 \cdot (3 \cdot 7) = -20 + 21 = 1$$
$$-2 \cdot 7 + 1 \cdot (3 \cdot 5) = -14 + 15 = 1$$

and

$$x \equiv 1 \cdot (-35) + 2 \cdot 21 + 3 \cdot 15 \equiv 52 \pmod{105}$$

This solution copies the proof of the Theorem.

∎

17.I.8 Example: Let $R = k[X]$, k a field, $m_i = (X - x_i), i = 1, 2, \ldots, d$ where the x_i are distinct elements of the field k. Let $y_i, i = 1, 2, \ldots, d$ be given elements of k. We have

$$p(X) \equiv y_i \pmod{(X - x_i)}$$

iff, for some $q(X) \in k[X]$, $p(X) = q(X)(X - x_i) + y_i$, i.e., iff $p(x_i) = y_i$. The solution to

$$\begin{aligned} p_1(X) &\equiv 1 \pmod{(X - x_1)} \\ p_1(X) &\equiv 0 \pmod{(X - x_j)}, j \neq 1 \end{aligned}$$

is easily found. By the second line above p_1 must be a constant multiple of $(X - x_2)(X - x_3)\cdots(X - x_n)$. By the first we must have $p_1(x_1) = 1$ which gives us the value of the constant. We find

$$p_1(X) = \frac{(X - x_2)\cdots(X - x_d)}{(x_1 - x_2)\cdots(x_1 - x_d)} = \frac{q_1(X)}{q_1(x_1)}$$

where $q_1(X) = q(X)/(X - x_1)$; $q(X) = (X - x_1)\cdots(X - x_d)$

Introducing

$$q_i(X) = \frac{q(X)}{(X - x_i)}, \quad i = 1, 2, \ldots, d$$

we similarly find (on replacing 1 by i) that the system

$$p_i(X) \equiv \delta_{ij} \pmod{(X - x_j)}, j = 1, 2, \ldots, d$$

is satisfied by

$$p_i(X) = \frac{q_i(X)}{q_i(x_i)}$$

so the general system

$$p(X) \equiv y_i \pmod{(X - x_i)}$$

has the solution

$$p(X) = \sum_{i=1}^{d} y_i \frac{q_i(X)}{q_i(x_i)}$$

Since the system is uniquely solvable modulo $q(X)$, by the theorem, and the degree of q is d, this is the unique polynomial of degree $\leq d - 1$, satisfying $p(x_i) = y_i, i = 1, 2, \ldots, d$.

This is Lagrange's Interpolation Formula.

The reader may wish to check that $q_i(x_i) = q'(x_i)$ (formal derivative) and that division of both members by $q(X)$ yields the well-known partial fractions decomposition of $p(X)/q(X)$.

17.I.9 Example: Another interpolation example. What does it mean to solve the system

$$f(X) \equiv pX + q \pmod{(X-a)^2}$$
$$f(X) \equiv rX + s \pmod{(X-b)^2}$$

where $a, b \in k, a \neq b$? Writing $pX + q = p(X-a) + (q + pa) =: p(X-a) + t$ we see that the first congruence reads

$$f(X) = t + p(X-a) + g(X)(X-a)^2$$

Substituting $X = a$ we get $t = f(a)$. Differentiating (a purely formal operation in an arbitrary field) and substituting $X = a$ again (details left to the reader) we get $f'(a) = p$ which should surprise no one. The system obviously satisifies the assumptions of the C.R.T. since $(X-a)^2$ and $(X-b)^2$ have no non-trivial factor in common. So it has a solution, proving the existence of a polynomial with given values and first derivatives at two given points.

By the uniqueness part of the C.R.T., $f(X)$ is uniquely determined modulo $(X-a)^2(X-b)^2$, so may be chosen of degree ≤ 3, since any solution may be reduced modulo $(X-a)^2(X-b)^2$ using polynomial division. ▮

More generally, given field elements $a_i, i = 1, 2, \dots k$, no two equal, and polynomials $g_i(X - a_i)$ of degrees $d_i - 1, \sum d_i = d + 1$, we can solve the system

$$f(X) \equiv g_i(X - a_i) \pmod{(X - a_i)^{d_i}} \;\; i = 1, 2, \dots, k$$

to find a polynomial f, of degreee $\leq d$, with prescribed Taylor expansions (of prescribed degrees) at the a_i, as long as the number of interpolation data (number of given values) sum up to the degreee of f plus 1 (note that f has $d+1$ coefficients).

An important use of the C.R.T. is fast polynomial and integer arithmetic. Everything is reduced modulo a suitably large integer (or polynomial) and further reduced modulo its various primary factors (powers of irreducible factors). We add or multiply the given numbers (or polynomials) modulo these factors. Using the C.R.T. we then reconstruct the solution from the residues found. See, e.g., Lidl-Pilz, Applied Abstract Algebra. (Springer Undergraduate Texts in Mathematics).

17.I.10 Example: Secret Sharing

A staff of 17 secretaries is assigned to the task of guarding my social security number $N < 5 \cdot 10^9$. The head of the Math Department chooses a prime number $P > 5 \cdot 10^9$, e.g., $P = 5789134517$.

He then chooses at random 16 different numbers $0 < f_0, f_1, \dots f_{15} < P$, and another sequence $0 < x_1, x_2, x_3, \dots, x_{17} < P$ and puts $f_{16} = N$, the number to be kept secret. (This random procedure is similar to that for deciding the salaries of the lecturers in the Department.)

From this he constructs the polynomial

$$f(X) = f_0 X^{16} + f_1 X^{15} + \cdots f_{15} X + f_{16} \in K[X]$$

where $K = \mathbf{Z}_P$ and computes

$$u_i = f(x_i) \quad 1 = 1, 2, \ldots 17$$

He distributes the values u_i among the secretaries and keeps a record of the x_i

When he needs my number, e.g., to make important decisions regarding my pension, he brings together the 17 secretaries. Using the Lagrange Interpolation Formula they reconstruct the polynomial $f(X)$, whence also its constant term $f_{16} = N$.

If only 16 secretaries, say those guarding the vaules $u_1, \ldots u_{16}$, come together they can do no better than finding a polynomial

$$p_0(X) + k \cdot (X - x_1) \cdots (X - x_{16}), \quad k \in K$$

with p_0 of degree ≤ 15, satisfying the 16 interpolation data, and an undetermined k.

However, knowing k is equivalent to knowing the constant term. We need more secretaries.

17.II . The Chinese Remainder Theorem, II.

First we define a recipe for forming big rings from smaller ones.

17.II.1 Definition: Let $R_1, R_2, \ldots, R_d$ be rings. We define their **direct sum**

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_d = \oplus_{i=1}^{d} R_i$$

to be the set of d-tuples $(r_1, r_2, \ldots, r_d)$, with componentwise addition and multiplication, i.e.,

$$(r_1, \ldots, r_d) + (s_1, \ldots, s_d) = (r_1 + s_1, \ldots, r_d + s_d)$$

$$(r_1, \ldots, r_d) \cdot (s_1, \ldots, s_d) = (r_1 s_1, \ldots, r_d s_d)$$

It is easy to check that this definition turns R into a ring with zero element $(0, 0, \ldots, 0)$ and identity element $1 = (1, 1, \ldots, 1)$. Obviously, the elements $(0, 0, \ldots, r_j, \ldots, 0)$, with zeros in all positions except the jth, form a subring isomorphic to R_j, with identity element $e_j = (0, 0, \ldots, 1, \ldots, 0)$. We will use the notation R_j for this subring, too.

The e_j:s satisfy $e_j^2 = e_j$, i.e., they are *idempotent*. Furthermore $i \neq j \Rightarrow e_i e_j = 0$ and $1 = e_1 + e_2 + \cdots + e_d$. We say that the e_j form a complete system of *orthogonal idempotents* for R.

Each subring R_j is not only a subring but an ideal, as well, since it is obviously closed under multiplication by elements of R:

$$(r_1, \ldots, r_j, \ldots, r_d)(0, \ldots, 0, s_j, 0, \ldots, 0) = (0, \ldots, 0, r_j s_j, 0, \ldots, 0)$$

It is generated, over R, by e_j; $R_j = Re_j$.

The ideal sum of all R_i's but one, R_j say, consists of all elements with a zero in the j:th position.:

$$(r_1, \ldots r_{j-1}, 0, r_{j+1}, \ldots, r_d)$$

We denote this ideal by I_j. It is easy to see that

$$R/I_j \simeq R_j$$

Simply define a surjective homomorphism $R \to R_j$ by $(r_1, \ldots, r_d) \to r_j$ and note that the kernel equals I_j.

So the R_j enter our construction simultaneously as subrings, ideals, and quotient rings.

17.II.2 Theorem. Chinese Remainder Theorem, version II. *R still a P.I.D. Let the ideals $I_j = (m_j), j = 1, 2, \ldots, d$ be pairwise comaximal. Then we have an isomorphism*

$$R/(I_1 \cap \ldots \cap I_d) = R/(I_1 \cdots I_d) \simeq \oplus_{j=1}^{d} R/I_j$$

Proof: Define

$$\varphi : R \to \oplus_{j=1}^{d} R/I_j$$

by

$$\varphi(r) = (r + I_1, r + I_2, \ldots, r + I_d)$$

φ is trivially a homomorphism. Its kernel is, equally trivially, $I := I_1 \cap \ldots \cap I_d$, so φ induces an *injection*

$$R/I \to \oplus_{j=1}^{d} R/I_j =: S$$

So we still have to prove surjectivity. Pick any

$$s = (r_1 + I_1, r_2 + I_2, \ldots, r_d + I_d) \in S$$

We wish to find an $r \in R$ mapping to s under φ. We want

$$\varphi(r) = (r + I_1, r + I_2, \ldots, r + I_d) = (r_1 + I_1, r_2 + I_2, \ldots, r_d + I_d)$$

so we must solve the system of congruences

$$r \equiv r_i \pmod{m_i}, \ i = 1, 2, \ldots, d$$

This is possible by the first version of the C.R.T. ∎

We saw above that S possesses a full set of orthogonal idempotents $e'_j, j = 1, 2, \ldots, d$, $1 = e'_1 + \cdots + e'_d$. By the isomorphism just proved, this must hold for R/I too. Let e_j denote the pre-images of the e'_j under φ. Then $1 = e_1 + \cdots + e_d$ and we can view R/I as the direct sum of the subrings (or ideals) $(R/I)e_i$.

The inverse isomorphism

$$\varphi^{-1} : \quad \oplus_j R/I_j \to R/I$$

is given by

$$\varphi^{-1}(r_1, \ldots, r_d) = \sum_j r_j e_j,$$

check this. It is instructive, although not necessary, to check the homomorphism properties of the inverse, just to get the right feeling for the role of idempotents.

17.II.3 Example: let k be field, and $x_i, i = 1, 2, \ldots, d$ distinct elements of k. Let $q(X) = (X - x_1) \cdots (X - x_d)$, and $q_i(X) = q(X)/(X - x_i)$. Then the C.R.T., version II, shows that

$$k[X] \simeq \oplus_{i=1}^{d} k[X]/(X - x_i)$$

by an isomorphism sending a polynomial to its residue classes modulo $(X - x_i)$. By Example I.7., of the previous section, this mapping is essentially an evaluation mapping sending each polynomial to its values at the x_i.

We checked above that the system of congruences (for fixed i):

$$p_i(X) \equiv \delta_{ij} \pmod{(X - x_j)}, \quad j = 1, 2, \ldots, d$$

is satisified by

$$p_i(X) = \frac{q_i(X)}{q_i(x_i)}, \quad i = 1, 2, \ldots d$$

By the proof

$$\varphi(p_i) = (0, 0, \ldots 1, \ldots 0) = e_i'$$

with the "1" in the i:th position. Being preimages of the idempotents e_i', they are a full set of orthogonal idempotents for the ring $k[X]/(q(X))$. I leave it as an exercise to check, directly, that

$$p_1(X) + \cdots + p_d(X) \equiv 1 \pmod{q(X)}$$

$$p_i(X)p_j(X) \equiv \delta_{ij} p_i(X) \pmod{q(X)}$$

You need only check equality of both members at the zeros of $q(X)$ (why?).

The reader is invited to investigate the last example of the previous section in a similar manner.

17.II.4 Example: Let us illustrate the statement

$$\mathbf{Z}/(15) \simeq \mathbf{Z}/(3) \oplus \mathbf{Z}/(5)$$

By the proof of the C.R.T., the isomorphism is given by the mapping

$$\varphi(n + (15)) = (n + (3), n + (5))$$

sending a class modulo 15 to the pair of the corresponding classes modulo 3 and 5. The kernel consists of all classes $n + (15)$ where n belongs to both (3) and (5), hence is divisible by 3 and 5, hence is divisible by 15, i.e., the kernel consists of the zero class, whence φ is injective.

Surjectivity follows directly from this fact, and the fact that both members have 15 elements.

The general theory provides us with a complete orthogonal set of idempotents $e_i, i = 1, 2; 1 = e_1 + e_2$, mapping to the idempotents $(1, 0), (0, 1)$. They are found, on solving the systems

$$x \equiv 1 \pmod 3$$

$$x \equiv 0 \pmod 5$$

and

$$y \equiv 0 \pmod 3$$

$$y \equiv 1 \pmod 5$$

to be

$$e_1 = \overline{10}, e_2 = \overline{6}$$

(classes modulo 15). Check that

$$10^2 \equiv 10 \pmod{15};\ 6^2 \equiv 6 \pmod{15};\ 10 \cdot 6 \equiv 0 \pmod{15}$$

Each element in

$$\mathbf{Z}/(3) \oplus \mathbf{Z}/(5)$$

may be written

$$(m + (3), n + (5))$$

where m and n are uniquely determined modulo 3 and 5, respectively, so we may assume $m = 0, 1, 2$, $n = 0, 1, 2, 3, 4$.

By the C.R.T.- isomorphism the corresponding statement holds in $\mathbf{Z}/(15)$: each element may be written, in a unique manner, as

$$\overline{m}e_1 + \overline{n}e_2 = \overline{m}\overline{10} + \overline{n}\overline{6}$$

with $m = 0, 1, 2$, $n = 0, 1, 2, 3, 4$. In particular, $e_1 + e_2 = \overline{10} + \overline{6} = \overline{16} = \overline{1}$

Note, for instance, that

$$(\overline{m}e_1 + \overline{n}e_2)(\overline{p}e_1 + \overline{q}e_2) =$$

$$\overline{mp}e_1 + \overline{nq}e_2$$

This has an amusing representation in a 3×5-matrix. If we number the rows and columns from 0 to 2, and 0 to 4, respectively, we can represent the class of $m \cdot 10 + n \cdot 6$ as the element in position (m, n).

We immediately find the elements $\overline{k} = k \cdot \overline{1} = k \cdot (e_1 + e_2) = \overline{k \cdot 10 + k \cdot 6}$, $k = 0, 1, 2$, in positions $(0, 0), (1, 1), (2, 2)$:

$$\begin{pmatrix} 0 & ? & ? & ? & ? \\ ? & 1 & ? & ? & ? \\ ? & ? & 2 & ? & ? \end{pmatrix}$$

Next in line is $\overline{3} = \overline{3}(e_1 + e_2) = \overline{0}e_1 + \overline{3}e_2$ in position $(0, 3)$:

$$\begin{pmatrix} 0 & ? & ? & 3 & ? \\ ? & 1 & ? & ? & ? \\ ? & ? & 2 & ? & ? \end{pmatrix}$$

You have guessed the pattern: we proceed along the diagonal until we hit the bottom of a column. We then move to the top of the next column and move along a new diagonal:

$$\begin{pmatrix} 0 & ? & ? & 3 & ? \\ ? & 1 & ? & ? & 4 \\ ? & ? & 2 & ? & ? \end{pmatrix}$$

Similarly, on hitting the right wall of the matrix, we move on to the beginning of the next row obtaining

$$\begin{pmatrix} 0 & ? & ? & 3 & ? \\ ? & 1 & ? & ? & 4 \\ 5 & ? & 2 & ? & ? \end{pmatrix}$$

Once again we hit the bottom of a column and move to the top of the next one. And so on.

We finally wind up with

$$\begin{pmatrix} 0 & \underline{6} & 12 & 3 & 9 \\ \underline{10} & 1 & 7 & 13 & 4 \\ 5 & 11 & 2 & 8 & 14 \end{pmatrix}$$

Reading off the (1,0) and (0,1) elements we find our idempotents!

The first row consists of multiples of 6, modulo 15, the first column of multiples of 10, modulo 15.

Each element in the matrix is the sum of the first element in the same column and the first element in the same row, which is exactly what our direct sum decomposition states, quite concretely.

This representation or interpretation of the C.R.T. is at the basis of the so-called Good-Thomas algorithm for Finite Fourier Transforms.

17.II.5 Example: Let us work through a polynomial example. We work over the field $k = \mathbf{Z}/(2)$ and study the ring $k[X]/I$ where I is generated by the polynomial $X^3+1 = (X+1)(X^2+X+1)$ the factors of which are irreducible, hence relatively prime.

So we have an isomorphism

$$\overline{R} = k[X]/(X^3+1) \simeq k[X]/(X+1) \oplus k[X]/(X^2+X+1)$$

by a mapping sending the class of $f(X)$ to its classes modulo $X+1$ and X^2+X+1.

Again, if $f(X)+(X^3+1)$ is sent to the zero classes, $f(X)$ is divisible by $X+1$ and X^2+X+1, hence by their product, hence $f(X)$ belongs to the zero class modulo X^3+1, so our mapping is injective.

Both members may be viewed as vector spaces over k. Since each element in $k[X]/(X^3+1)$ has a unique representative of degree < 3 (requiring 3 coefficients) this ring has dimension 3 as a vector space over k. Similarly the two factors in the right member have dimensions 1 and 2, respectively, so the direct sum has dimension 3. By the Dimension Theorem, "injective" (nullspace dimension $= 0$) implies "surjective" (dimension of range $= 3$).

Of course, with a finite ground field we could count elements as well. Both members have $2^3 = 8$ elements.

From the proof of the theorem it is clear that we find our idempotents by solving Bézout's Identity:

$$1 = p(X)(X+1) + q(X)(X^2+X+1) = e_1 + e_2$$

(The *classes* of e_1, e_2, modulo X^3+1, are the idempotents).

We could use Euclid's Algorithm for that kind of computation but a partial fractions decomposition may often be more convenient. Decomposing $1/(X^3+1)$ we get

$$\frac{1}{X^3+1} = \frac{1}{X+1} + \frac{X}{X^2+X+1}$$

Multiplying by X^3+1 we get, omitting the bars signifying residue classes

$$1 = (X^2+X+1) + (X^2+X)$$

The classes of X^2+X+1 and X^2+X modulo X^3+1 are our idempotents, since they satisfy the systems of congruences of the proof. The reader should check this.

Of course, any element in $\overline{R}$ may be expressed in the idempotents. The coefficients will be uniquely determined modulo $X+1$, and X^2+X+1, respectively, so their representatives may be chosen of degrees < 1 and < 2. We find

$$\begin{aligned} 1 &= (X^2+X+1) + (X^2+X) \\ X &= (X^2+X+1) + X(X^2+X) \\ X^2 &= (X^2+X+1) + (X+1)(X^2+X) \end{aligned}$$

The remaining 5 elements are suitable $k-$linear combinations of these elements. I invite the reader to ponder over the following matrix

$$\begin{pmatrix} 0 & 0 & 1 & X & 1+X \\ 0 & 0 & \underline{X^2+X} & X^2+1 & 1+X \\ 1 & \underline{X^2+X+1} & 1 & X & X^2 \end{pmatrix}$$

The underlined elements are the idempotents. The first row and first column are the coefficients (replacing row and column indices). All computations are performed modulo X^3+1.

Of course, such a matrix scheme does not exist in the case of an infinite field k.

17.II.6 RSA Ciphers

In cryptology it is common practice to represent words as numbers or classes modulo some large integer. The RSA cipher is a very simple encryption-decryption scheme (at least empirically) with very good properties. It rests on the following simple theorem:

17.II.7 Theorem. . *Let $n = pq$ be a product of two distinct primes p and q. Let e and d be two numbers, relatively prime to $(p-1)(q-1)$. Assume $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then, for every integer w,*

$$w^{ed} \equiv w \pmod{n}$$

Proof: By the C.R.T, we have an isomorphism

$$\mathbf{Z}/(pq) \simeq \mathbf{Z}/(p) \oplus \mathbf{Z}/(q)$$

so, letting w denote the class of w modulo n as well, we may write

$$w = (u, v)$$

where u, v are classes modulo p and q, respectively. Since

$$w^k = (u^k, v^k)$$

it is enough to prove the corresponding result for u and v, say u, i.e., that

$$u^{ed} = u$$

This is obvious if $u = 0$, so assume $u \neq 0$. By Fermat's Little Theorem

$$u^{p-1} = 1$$

As

$$ed = j(p-1)(q-1) + 1$$

for some j, we get

$$u^{ed} = u \cdot (u^{p-1})^{j(q-1)} = u \cdot 1 = u$$

∎

The RSA scheme is the following. Let n be a product of two very large primes (which are kept secret, of course). Transmit the word $c = w^e$ (reduced modulo n) for some e, relatively prime to $(p-1)(q-1)$. The receiver, who knows d, computes $c^d = w^{ed}$ (modulo n), thereby retrieving the word w. The cipher is safe as long as no one is able to factor the integer n. But no one has really proved that factoring is necessary, or equivalent to breaking the cipher.

The letters R,S,A are the initials of Rivest, Shamir, and Adleman.