

Chapter 1

Introduction and Philosophy

The story about the Chinese Remainder Theorem, CRT, can be told in many ways. In a highly abstracted mathematical exposition, one would start with a Dedekind ring and the decomposition of the principal ideal into a product of prime ideals and then proceed to the so-called Theorem on the Independence of Exponents which can be viewed as a possibility for an abstract formulation of CRT. Such an approach would forget the original landscape of CRT: integers and remainders under division. The opposite extreme of telling the story would consist of various numerical examples in the original landscape, with little general theory, or none whatsoever.

Our approach in this book lies between the two extreme approaches mentioned. Indeed it can be labeled as applications-oriented. During its long history, CRT has appeared in many disguises, never failing to find new aspects of application. An aspect inherent in the very core of CRT is *computing*: algorithms for taking calculations via a detour where much smaller numbers can be used. Such a detour can be partitioned in a fashion where redundancy is added to the data, or data can be recovered only with the cooperation of sufficiently many parties sharing them partially. Then aspects of (error-correcting) *codes* and *cryptography* become relevant. This book tells the story of CRT in the landscape of three C's: computing, codes and cryptography. We feel that our approach in some sense reflects the change visible in mathematical research in general. There is greater interest in constructive algorithmic results, also in their efficiency, and less interest in only existential studies with little or no computational significance.

1.1 A Historical Overview

The Chinese Remainder Theorem, CRT, appeared in the mathematical classic of Sun Zi, a mathematician in ancient China. The book is known by the name

Sun Zi Suanjing, Sun's Arithmetical Manual. The exact date is unknown, but it is reasonable to take it to be during the first century A. D. Although we do not plan to dwell on the history of mathematics, it is useful to try to get some time-perspective.

Every human culture exhibits mathematics, at least in some primitive forms. "Western" mathematics, as a systematic pursuit, originated in Egypt and Mesopotamia, achieved an early culmination in Greece and spread to the Graeco-Roman world. After the fall of Rome, there was a stillstand in mathematical creativity in Europe, lasting half a millennium. On the other hand, the Islamic branch was born, to become combined with the European branches. Thus, we arrive at the following rough timetable for the periods of development of western mathematics:

Egyptian	3000 B.C.—1500 B.C.
Babylonian	1700 B.C.—300 B.C.
Greek	600 B.C.—200 B.C.
Graeco-Roman	A.D. 100—A.D. 500
Islamic	A.D. 750—A.D. 1450
Medieval-Renaissance	A.D. 1100—A.D. 1600
Modern	A.D. 1600—

Early *oriental* and western mathematics were quite isolated from one another. Details of possible interactions are not clear and are still a subject of further investigations. It can be seen from the above timetable that the book of CRT, *Sun Zi Suanjing*, falls timewise to the beginning of the Graeco-Roman period in western mathematics. Let us now briefly look into the history of early Chinese mathematics, before and during the time of *Sun Zi Suanjing*, to get a comparison of the above western timetable.

The oldest Chinese mathematical classic is *Chou Pei Suanjing*, a record of mathematics for astronomical calculations from about 1000 B.C. The Pythagorean Theorem was already used in the astronomical calculations of this book.

The most influential of all ancient Chinese mathematical books was *Jiuzhang Suanshu*, Nine Chapters on the Mathematical Art. It was composed about A.D. 50-100, somewhat earlier than *Sun Zi Suanjing*. It includes 246 problems and solutions coming from practice. The calculation of square and cubic roots can be found in some of the solutions. A systematic method for solving some systems of linear equations, involving also negative numbers, is presented in the book. The last chapter includes results on rectangular triangles, some of which were rediscovered later in India and Europe. In this book the approximation for π equals 3. Later a Chinese geometer Liu Hui, an important commentator on this book, improved the value of π to 3.14 by considering a regular polygon of

96 sides, and further to 3.14159 by considering a polygon of 3072 sides. The Chinese mathematician Tsu Chung-Chih (430-501) knew the approximation $\pi \approx 22/7$ and called it “inexact”, and presented also the more accurate value $\pi \approx 355/113 \approx 3.1415929$. Basically, the main topics in *Sun Zi Suanjing* are the same as those in the Nine Chapters, *Jiuzhang Suanshu*, except that one topic appears for the first time in Sun’s Manual: The Chinese Remainder Theorem.

Finally, it should be emphasized that the relative isolation of early Chinese and western mathematics began to decrease later on. Nowadays mathematicians form a worldwide community whose unification will become even stronger during the times of the Internet.

1.2 Pars pro toto

The Chinese Remainder Theorem can be viewed as a manifestation of the general principle “pars pro toto”—a part goes for the whole thing. Aspects of this principle can be found in most different environments. We now try to illustrate the principle *pars pro toto* by some examples, converging towards our ultimate goal, the Chinese Remainder Theorem. The crucial question in this connection will be: can the whole thing be replaced or represented by its part, or to what extent or in what sense can it be so replaced or represented?

An area where the principle *pars pro toto* appears in a fascinating form in *genetics*. The whole individual is in a very definite sense present in a single cell or in some DNA strips. Under favorable circumstances, these DNA strips can still much later be recovered in fossils remaining after the individual.

Another example of the principle *pars pro toto*, lying in quite a different direction, is decision-making through *parliamentary democracy*. Instead of direct decision-making, a population elects representatives, members of a parliament, who are going to make the decisions. Thus, the whole population is represented or replaced by a part, the parliament, for the process of decision-making. This book is not an appropriate place to discuss the virtues or disadvantages of such a representation, for instance, as regards the various minorities in the population. Instead, we proceed to an example coming closer to our actual topic of CRT: how well can *information* or *data* be represented by its suitably chosen parts?

There are many instances of situations, where a thing is or should be found out by some of its properties. Thus, in such a case the properties in question contain enough information to identify the whole thing—the whole thing is represented or can be replaced by those properties. Having a property can be understood as belonging to the class of objects with this property. As regards each specific class S and object X , the matter is settled by a “yes” or “no”

answer to the question “Is X in S ?” In a popular game of questions and answers, one has to find the identity of an object X by such questions whose number should not exceed a pregiven bound, say twenty.

Let us take one step forward and become more specific. By a suitable encoding, all information can be represented as numbers. So let us assume that our object X , the piece of information we are interested in, is a positive integer. We are allowed to ask questions of the form

(n) Is X greater than n ?

In this way we get a sequence of answers of the form (n, Z) , where $Z = \text{yes}$ or $Z = \text{no}$. (For instance, (1000, yes) says that X is greater than 1000.) It is obvious that any X is determined by a sequence of answers

$$(n_1, Z_1)(n_2, Z_2) \cdots (n_t, Z_t).$$

A trivial way to do this is to consider the sequence

$$(n, \text{no})(n-1, \text{yes}),$$

which identifies X as n . However, if X is completely unknown, we cannot possibly expect to be so lucky that we would immediately guess the questions (n) and $(n-1)$!

A general strategy would be the following. First one has to aim at a “no” answer. After an answer (n, no) , roughly $\log_2 n$ questions are needed to determine X . This matter will be discussed further from an information-theoretic point of view in Section 4.1. For instance, the sequence of answers

$$(128, \text{no})(64, \text{yes})(96, \text{no})(80, \text{yes})(88, \text{yes})(92, \text{yes})(94, \text{yes})(95, \text{yes})$$

determines the value $X = 96$, the number of questions after the first “no”-answer being $\log_2 128 = 7$. For convenience we have only used powers of 2. The first questions, before the first “no”-answer, can be only guesses.

In the above example, the properties we used for characterizing the number X were formulated by question (n) and, thus, were very simple indeed. They are simple also in the characterization due to the Chinese Remainder Theorem, CRT. An unknown number X is characterized by its remainders under divisions by different integers n . Thus, the questions asked will be of the form

(n) What is the smallest nonnegative remainder of X modulo n ?

Here it is more convenient to formulate the questions in this way but, if so preferred, each question (n) can obviously be replaced by n questions with only “yes” or “no” answers.

Does such a *pars pro toto* representation, with suitably chosen moduli, always determine a unique X , that is, can a number X always be characterized in this way by remainders? Obviously, this is not possible because, no matter how the moduli n_1, \dots, n_t are chosen, each of the infinitely many numbers

$$X + in_1 \cdots n_t, \quad \text{for } i = 0, 1, 2, \dots,$$

possesses the same smallest nonnegative remainders with respect to each of the moduli. As we will see in the exact formulation of the Chinese Remainder Theorem, this method of representation by remainders determines a unique X only among numbers having a well-specified size.

1.3 Chinese Remainder Theorem: A First Formulation

A magician wants to impress the audience with the following “mind-reading” trick. A randomly chosen helper is asked to think of a number less than 60. Then he/she is asked to tell the remainders when the number is divided by 3, 4, and 5, in succession. Upon hearing the remainders, the magician tells the number. For instance, the number will be 37 in case of the remainders 1, 1 and 2, obtained in divisions by 3, 4, and 5, respectively.

This illustration is taken from an old guide-book for magicians. The book tells the magician to divide the number $40a + 45b + 36c$, where a , b and c are the three remainders, by 60 and announce the remainder as the result of the mind-reading! In the example case the division of 157 by 60 leaves indeed the remainder 37. Although this example is correctly treated, the book is not very successful in its generalization to arbitrary moduli.

Let us now do it properly and prove the Chinese Remainder Theorem in its basic version. We assume here that the reader is familiar with the fact that the greatest common divisor of two integers a and b , denoted by $\gcd(a, b)$, can be represented as the sum

$$\gcd(a, b) = ua + vb,$$

for some integers u and v , following the so called Euclidean algorithm. We also want to point out that the discussion of the basic version of CRT will be resumed in Chapter 2 from a slightly different angle. In this way we hope to give the reader a solid background before moving into the more advanced chapters.

We say that the integers m_1, m_2, \dots, m_t are *relatively prime in pairs* if $\gcd(m_i, m_j) = 1$ for any distinct i and j where $1 \leq i, j \leq t$.

Chinese Remainder Theorem Let a_1, a_2, \dots, a_t be any t integers and m_1, m_2, \dots, m_t be relatively prime in pairs. Then there is a number x with

the property

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \dots, t. \quad (1.1)$$

Moreover, x is unique in the following sense. Let M be the product $m_1 m_2 \cdots m_t$ and let y satisfy the system of congruences (1.1). Then $y \equiv x \pmod{M}$.

Proof: We apply induction on t . For $t = 1$, it suffices to take $x = a_1$. The uniqueness as asserted is also obvious.

Assumingly that the result holds for $t = k$, we demonstrate its validity for $t = k + 1$. Consider the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ &\dots\dots\dots \\ x &\equiv a_k \pmod{m_k}, \\ x &\equiv a_{k+1} \pmod{m_{k+1}}, \end{aligned}$$

where the moduli are relatively prime in pairs. By the inductive hypothesis, there is a number x' satisfying the first k of these congruences.

Observe that the product $m_1 \cdots m_k$ and the integer m_{k+1} are relatively prime, that is, their greatest common divisor equals 1. Otherwise, they would have a common prime factor p . Since p divides the product $m_1 \cdots m_k$, it must divide one of the factors, say m_j , $1 \leq j \leq k$. But then

$$\gcd(m_j, m_{k+1}) \geq p > 1,$$

which contradicts the assumption of the moduli being relatively prime in pairs.

Since $m_1 \cdots m_k$ and m_{k+1} are relatively prime, there are integers u and v (possibly negative) such that

$$um_1 \cdots m_k + vm_{k+1} = 1.$$

Multiplying both sides by $(a_{k+1} - x')$, we obtain

$$u(a_{k+1} - x')m_1 \cdots m_k + v(a_{k+1} - x')m_{k+1} = a_{k+1} - x'$$

and, further,

$$x' + u''m_1 \cdots m_k = a_{k+1} + v''m_{k+1},$$

where we have abbreviated

$$u'' = u(a_{k+1} - x') \text{ and } v'' = -v(a_{k+1} - x').$$

Denoting $x'' = x' + u''m_1 \cdots m_k$, this tells us that

$$x'' \equiv a_{k+1} \pmod{m_{k+1}}.$$

On the other hand,

$$x'' \equiv x' \equiv a_i \pmod{m_i}, \quad i = 1, \dots, k,$$

where the first congruence follows by the definition of x'' , and the second congruence is due to the choice of x' . Thus, x'' satisfies all of our original $k + 1$ congruences, and we have completed the induction step.

For the assertion about uniqueness, consider two numbers x_1 and x_2 satisfying (1.1). Thus, also

$$x_1 \equiv x_2 \pmod{m_i}, \quad i = 1, 2, \dots, t,$$

from which the relation $x_1 \equiv x_2 \pmod{M}$ immediately follows, by the definition of a congruence and by our assumption about these m_i being relatively prime in pairs. \square

Although the computational aspect is not emphasized in the above proof, the proof still contains the ingredients of both the iterative and direct Chinese Remainder Algorithm, as will become clear from the discussion in Chapter 2.

As a first indication of the power of the Chinese Remainder Theorem, we prove a corollary showing how any finite sequence of integers can be represented in terms of two integers. The corollary is important in various considerations dealing with logic and mathematics, but it will not be needed as such in this book. We will use here and later on in this book the short notation $(a \bmod n)$, with or without parentheses, for the smallest nonnegative remainder of a modulo n .

Corollary Let a_i , $0 \leq i \leq t$, be a finite sequence of nonnegative integers. Then there are integers u and v such that

$$(u \bmod (1 + (i + 1)v)) = a_i, \quad \text{for every } i = 0, 1, \dots, t.$$

Proof: Let a be the largest among the integers a_i , $0 \leq i \leq t$, and define $v = 2a \cdot t!$ and $m_i = 1 + v(i + 1)$, $0 \leq i \leq t$. We claim that the integers m_i , $0 \leq i \leq t$, are relatively prime in pairs. Assume the contrary: a prime p divides both m_i and m_j , for some $i > j$. Then p divides also the difference

$$(i + 1)m_j - (j + 1)m_i = i - j \leq t.$$

Since $p \leq t$ divides m_i and v is divisible by all integers $\leq t$, we obtain the contradiction $p = 1$. This proves our claim.

Thus, the integers m_i qualify as moduli for the Chinese Remainder Theorem. Hence, there is a number u such that

$$u \equiv a_i \pmod{m_i}, \quad i = 0, 1, \dots, t.$$

Hence, $(u \bmod m_i) = (a_i \bmod m_i)$, for all $0 \leq i \leq t$. But because $a_i < v < m_i$, we conclude that

$$(a_i \bmod m_i) = a_i, \quad \text{for } 0 \leq i \leq t.$$

Hence,

$$(u \bmod m_i) = a_i, \quad \text{for } 0 \leq i \leq t,$$

as asserted in our corollary. □

1.4 CRT in the Hands of Old Mathematicians

The view that mathematics is a cumulative science in the sense that earlier results are needed in building up later theories is only partially true. Some entire theories become obsolete and unpopular, and pass into oblivion. The advent of computers has very much changed the map of mathematics in making the *discrete modeling* of the world a very feasible and most applications-oriented approach. As a result, for instance, *graph theory* has gained tremendously in prestige and has become a huge science with numerous big branches, from an earlier slum area of topology.

With an estimated one million (more or less) new mathematical theorems being established every year, one cannot expect that even most of them will be useful in later developments. Very often an area of mathematics becomes saturated, after which research stubbornly pursued in this area is bound to remain on small side tracks. When remnants of such research are later discovered in some connection, this does not usually happen with enthusiasm. Doors of the mathematical past being rusted does not mean that there lies a treasure inside.

However, there are many marvelous exceptions. Some research areas and individual results seem to thrive in most diverse mathematical cultures. Such areas are repeatedly used as a basis of new fields of research, and such results customarily pop up in various disguises during the course of history. Basic number theory is certainly such a research area, and CRT such an individual result.

We have already spoken about the origins of CRT. The Chinese background will be discussed in Chapter 2. We now give glimpses about how CRT is treated by two old mathematicians, Fibonacci and Euler. Fibonacci, Filius Bonacci, the

son of Bonaccus, also known as Leonardo Pisano, wrote in his *Liber Abbaci* from 1202 roughly as follows.

“Let a contrived number be divided by 3, also by 5, also by 7; and ask each time what remains from each division. For each unity that remains from the division by 3, retain 70; for each unity that remains from the division by 5, retain 21; and for each unity that remains from the division by 7, retain 15. And as much as the number surpasses 105, subtract from it 105; and what remains to you is the contrived number. Example: suppose from the division by 3 the remainder is 2; for this you retain twice 70, or 140; from which you subtract 105, and 35 remains. From the division by 5, the remainder is 3; for which you retain three times 21, or 63, which you add to the above 35; you get 98. From the division by 7, the remainder is 4, for which you retain four times 15, or 60; which you add to the above 98, and you get 158, from which you subtract 105, and the remainder is 53, which is the contrived number. From this rule comes a pleasant game, namely if someone has learned this rule with you; if somebody else should say some number privately to him, then your companion, not interrogated, should silently divide the number for himself by 3, by 5, and by 7 according to the above-mentioned rule; the remainders from each of these divisions he says to you in order; and in this way you can know the number said to him in private.”

Sun’s original approach will be described in Chapter 2. In general mathematical terms, Fibonacci’s presentation is very similar. Both of them have their presentation based on a specific numerical example, however, an implicit feeling is conveyed about the method being general. Neither one worries about the uniqueness of the solution. Observe the very pleasant leisurely writing style of Fibonacci. His approach is also very algorithmic and directly implementable. Rather surprising is the cryptographic touch in his description of the “pleasant game”. Remember that cryptography is one of the C’s in the landscape of this book.

From the point of view of mathematical terms and notation, the approach becomes very different in the writing of Leonhard Euler. The integers in the specific example are replaced by variables, and modern algebraic notation is followed. There is also no doubt that the method is intended to be general: instead of five numbers, there can be arbitrarily many. The text by Euler is from the publication of St. Petersburg Academy of Sciences in 1734:

“A number is to be found that, when divided by a, b, c, d, e , which numbers I suppose to be relatively prime, leaves respectively the remainders p, q, r, s, t . For this problem the following numbers satisfy:

$$Ap + Bq + Cr + Ds + Et + m \times abcde$$

in which A is the number that divided by $bcd e$ has no remainder, by a , however,

has the remainder 1; B is the number that divided by $acde$ has no remainder, by b , however, has the remainder 1, ..., which numbers can consequently be found by the rule given for two divisors."

Here the last remark refers to a result earlier in the text, needed in the computing of the numbers A, B, C, D, E .

We conclude this section with the following formulation of the Chinese Remainder Theorem in a ring-theoretic setting:

Let A be a commutative ring with identity and let $\{m_i | 1 \leq i \leq t\}$ be a finite collection of ideals in A such that $m_i + m_j = A$ for all $i \neq j$. Then, for any set of elements $\{x_i \in A | 1 \leq i \leq t\}$, there exists an $x \in A$ such that

$$x \equiv x_i \pmod{m_i}, \quad 1 \leq i \leq t.$$

The reader should be able to figure out, eventually after consulting the Tutorial in Algebra given in Appendix B, how the basic numerical version of the Chinese Remainder Theorem results from the ring-theoretic formulation. Instead of explaining this matter in detail, we conclude this section with a story about Oscar Zariski, a foremost figure in the field of algebraic geometry, told in [28].

Oscar Zariski gave a course in projective geometry on a highly abstract level. One of the students, afterwards a well-known mathematician, felt the need of some clarification and examples. "What would you get", he asked the professor, "if you specialized the field F to the complex numbers?" Zariski answered: "Yes, just take F as the complex numbers."

1.5 CRT in Applications: the Three C's

We have already pointed out that we will not pursue in this book the abstract mathematical formulation when telling about CRT. Indeed, at a sufficiently high level of abstraction, CRT becomes an axiom for the structure you are investigating—and so there is very little you can say about it, but you have to proceed to other matters instead. This means that, instead of the title "CRT", the book should have a title such as "CRT-Based Structures".

But there is much to say about the *use* of CRT in various contexts. This is what our book is about. Specifically, we will tell about the applications of CRT in the landscape of three C's: computing, codes, cryptography.

We want to emphasize that the list of applications of CRT considered in this book is by no means exhaustive. Indeed, applications of CRT occur in almost every area of mathematics. We just mention the following modern applications to the theory of finite automata by Yu, Zhuang and Salomaa [105]. Let m and n be relatively prime. By a CRT-based argument concerning the largest

integer not representable in the form $cm + dn$, for some positive or nonnegative c, d (three possible cases), it is shown in [105] that the representation of the catenation L_1L_2 in a finite deterministic automaton may require mn states, if the representation of L_1 (resp. L_2) requires m (resp. n) states. Moreover, the number of states which is necessary and sufficient in the worst case for a finite deterministic automaton to accept the star of an n -state language, $n > 1$, over a one-letter alphabet is $(n - 1)^2 + 1$. We neither explain nor use these notions in this book, so this illustration is meant to a reader knowledgeable in automata theory.

The Chinese Remainder Problem arose originally from the computation of calendars, as will be seen below in Chapter 2, where also many other ancient problems, related to modular computations, are discussed. The C of *computing*, in the landscape of three C's we are describing, is undoubtedly the oldest and most diversified. It will be the subject matter of Chapters 3-5 below. The Chinese Remainder Algorithm, CRA, is basically a divide-and-conquer technique. The originally given problem is divided into subproblems. The latter can be solved independently of each other, so parallel processing is possible. Finally, the results for the subproblems are combined by CRT to get a solution of the original problem. This procedure is depicted in Fig. 3.1 in Section 3.1 below.

We will not describe here the contents of the individual chapters, as this will be done at the beginning of the chapters themselves. Modular computations based on CRA are dealt with in Chapter 3, the Schönhage algorithm for multiplication being one of the topics. Chapter 4 develops CRA-based ideas in more extended contexts: polynomial interpolation, shift-register synthesis, cyclic convolution and fast Fourier transform, to name a few. Chapter 5 addresses the problem of carrying CRA-type arguments over to structures, where they would not be valid as such, that is, building a bridge from the "CRA-territory" to some parts outside of it.

Codes, the second of the C's in our landscape, form the subject matter of Chapter 6. The basic technique in coding theory is to add redundancy to data sent via a noisy channel or stored in a computer, this being done because of error detection and correction. In general, for modular algorithms based on CRT, the product of the moduli should be large enough with respect to the data. But it should not be too large, since this would be harmful to the efficiency of the modular algorithm. In applications to coding theory, however, matters look quite different, since making the product larger increases the possibilities of adding redundancy.

The third C, *cryptography*, is the topic of our final Chapter 7. The Chinese Remainder Theorem is in itself a *secret-sharing scheme*. Different parties are each in possession of a number. When they combine their knowledge, they find out a secret number, using CRT. This line of argument was clearly present

already in the writing of Fibonacci quoted above, as well as in the actions of the ancient Chinese general who arranged his troops in rows of 9, 10, and 11 soldiers, by turns, and found out their exact number, without having to disclose it to anybody not knowing the CRT-technique.

The interdependence of the chapters can be roughly described by the following chart.

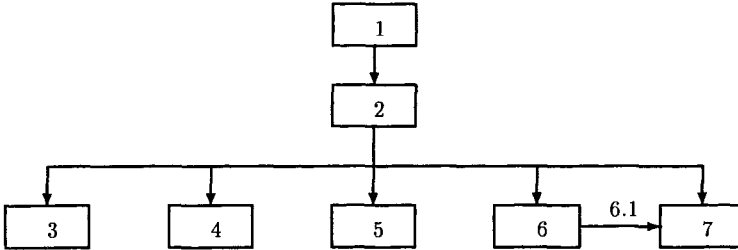


Figure 1.1: A flowchart of the interdependence of the chapters.