Note 6 Supplement: Chinese Remainder Theorem

Computer Science 70
University of California, Berkeley

Summer 2018

Prime numbers play a central role in the study of modular arithmetic. In particular, the finite field with p elements (denoted $\mathrm{GF}(p)$), where p is a prime, enjoys several nice properties:

1. Every non-zero element has a multiplicative inverse.
2. Fermat's Little Theorem: For non-zero $a \in \mathrm{GF}(p)$, $a^{p-1} \equiv 1 \pmod{p}$. In particular, Fermat's Little Theorem is the basis for the correctness of the RSA public-key cryptosystem.

The properties above do not hold modulo m, when the positive integer m is not prime. [1] Therefore, it is of interest to develop a systematic method for reducing problems modulo m to problems modulo p, where p is *prime*.

Here is the systematic method we seek.

Theorem 1 (Chinese Remainder Theorem)**.** *Let n be a positive integer and $y_1, \dots, y_n$ be given integers. For integers $m_1, \dots, m_n > 1$ which are pairwise coprime, the system of linear congruences*

$$\begin{aligned} x &\equiv y_1 \pmod{m_1}, \\ &\vdots \\ x &\equiv y_n \pmod{m_n}, \end{aligned}$$

[1] Fermat's Little Theorem, when suitably generalized with Euler's totient function, *does* have an analog modulo m.

has a unique solution $x \in \mathbb{Z}/m_1 \cdots m_n\mathbb{Z}$, and moreover, the solution can be explicitly computed.

See Note 6 for the proof of the theorem. The construction of the solution given in the proof is also interesting in its own right, and is very related to polynomial interpolation which we will see later in the course.

Example 1. Let p and q be primes, and let $m := pq$. Consider the equation $x^2 \equiv -1 \pmod{m}$, that is, we are interested in finding the square roots of -1 modulo m. Note that if $x^2 \equiv -1 \pmod{m}$, then $m \mid x^2 + 1$, and so $p \mid x^2 + 1$. Likewise, $q \mid x^2 + 1$. Thus, $x^2 + 1$ must satisfy the following system of linear congruences:

$$x^2 + 1 \equiv 0 \pmod{p} \tag{1}$$
$$x^2 + 1 \equiv 0 \pmod{q} \tag{2}$$

The CRT tells us that the solutions to $x^2 \equiv -1 \pmod{m}$ are precisely the x which solve the system of linear congruences

$$\begin{aligned} x &\equiv y_1 \pmod{p} \\ x &\equiv y_2 \pmod{q} \end{aligned}$$

where y_1 is a solution to (1) and y_2 is a solution to (2). Thus we see that a question posed modulo m is equivalent to first solving the equations (1) and (2) (which is done modulo primes), and then using the CRT to combine the solutions of (1) and (2) into solutions to the original question modulo m.

Remark: Example 1 is slightly misleading. In order to fully reduce a question modulo m into a question over the finite field $\mathrm{GF}(p)$, one needs more tools than the CRT alone. In general, one prime factorizes $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ for primes $p_1, \ldots, p_n$ and positive integer powers $\alpha_1, \ldots, \alpha_n$. Then, solving an equation modulo m is equivalent to first solving the equation modulo a prime power p^α. The technique of transferring solutions modulo p to solutions modulo p^α is known as "lifting" and will not be discussed further here.

We now give a deeper understanding of the CRT. Let $m_1, m_2 > 1$ be coprime integers, and consider the system of equations

$$x \equiv a \pmod{m_1} \tag{3}$$
$$x \equiv b \pmod{m_2} \tag{4}$$

where now we think of varying (a, b) in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$. Given any choice of (a, b), we can apply the CRT to find the unique solution x modulo m_1m_2. In fact, we can define a function

$$g : \mathbb{Z}/m_1m_2\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$$

$$\text{given by } g(x) := (x \bmod m_1,\ x \bmod m_2).$$

The CRT tells us that g is one-to-one and onto, that is, g is a bijection. The inverse function is

$$g^{-1} : (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \to \mathbb{Z}/m_1m_2\mathbb{Z}$$

$$\text{given by } g^{-1}(a, b) := x, \text{ where } x \text{ is the unique solution to (3) and (4).}$$

In fact, f is an *isomorphism*, a term from algebra which means that the two structures $\mathbb{Z}/m_1m_2\mathbb{Z}$ and $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ are *essentially the same* with respect to addition and multiplication. We already have an understanding of how to add and multiply elements in $\mathbb{Z}/m_1m_2\mathbb{Z}$, namely, we add and multiply them modulo m_1m_2. To pursue this idea further, we must define the operations of addition and multiplication on the set $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$.

Let (a_1, b_1), (a_2, b_2) be two elements of $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$. We define addition and multiplication componentwise:

$$\begin{aligned} (a_1, b_1) + (a_2, b_2) &= (a_1 + a_2,\ b_1 + b_2), \\ (a_1, b_1)(a_2, b_2) &= (a_1a_2,\ b_1b_2). \end{aligned}$$

The special property of the function g defined above is that it preserves the operations of addition and multiplication, that is:

$$g(x + y) = g(x) + g(y), \tag{5}$$

$$g(xy) = g(x)g(y), \tag{6}$$

for all $x, y \in \mathbb{Z}/m_1m_2\mathbb{Z}$. Notice that on the left, the expression $x + y$ is the operation of addition in the set $\mathbb{Z}/m_1m_2\mathbb{Z}$, while on the right, the expression $g(x) + g(y)$ is the operation of addition in the set $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$.

To understand the meaning of the statements above, notice that $x + y$ is the addition of two elements in $\mathbb{Z}/m_1m_2\mathbb{Z}$, and then when we "convert" to $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ via the bijection g, then we get $g(x + y)$. On the other hand, if we convert x and y to $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ individually, we get $g(x)$ and $g(y)$ respectively, and then if we add $g(x)$ and $g(y)$ as tuples in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$, we get $g(x) + g(y)$. So, $g(x + y) = g(x) + g(y)$ says that it does not matter whether we perform the addition in $\mathbb{Z}/m_1m_2\mathbb{Z}$, or in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$, because the result is the same in either case. Similarly, it does not matter in which structure we perform multiplication.

To understand why g is an isomorphism, note that for all $x, y \in \mathbb{Z}/m_1m_2\mathbb{Z}$,

$$\begin{aligned} g(x+y) &= (x + y \bmod m_1,\ x + y \bmod m_2) \\ &= (x \bmod m_1,\ x \bmod m_2) + (y \bmod m_1,\ y \bmod m_2) \\ &= g(x) + g(y), \\ g(xy) &= (xy \bmod m_1,\ xy \bmod m_2) \\ &= (x \bmod m_1,\ x \bmod m_2)(y \bmod m_1,\ y \bmod m_2) \\ &= g(x)g(y). \end{aligned}$$

The isomorphism is denoted by $\mathbb{Z}/m_1m_2\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$.

To give a concrete example, we will now build a table for the isomorphism between $\mathbb{Z}/45\mathbb{Z}$ and $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$.

	0	1	2	3	4	5	6	7	8
0	0	10	20	30	40	5	15	25	35
1	36	**1**	**11**	21	**31**	**41**	6	**16**	**26**
2	27	**37**	**2**	12	**22**	**32**	42	**7**	**17**
3	18	**28**	**38**	3	**13**	**23**	33	**43**	**8**
4	9	**19**	**29**	39	**4**	**14**	24	**34**	**44**

Additional insights can be gleaned from the table.

- The table can be constructed by writing 0 in the upper left corner, and then writing successive numbers diagonally to the right, wrapping around the rows and columns on the table when necessary.

- The bolded numbers are the numbers which are relatively prime to 45. Note that the bolded numbers appear precisely in the rows which are relatively prime to 5 and the columns which are relatively prime to 9. This is the statement that if $g(x) = (a, b)$, then x has an inverse modulo m_1m_2 if and only if a has an inverse modulo m_1 and b has an inverse modulo m_2.

The structures $\mathbb{Z}/m_1m_2\mathbb{Z}$ (with addition and multiplication taken modulo m_1m_2) and $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ (with the operations of addition and multiplication defined above) are examples of structures called *rings*. A simple way to describe a ring is a structure on which you can perform addition and multiplication. In this language, g is known as a *ring isomorphism*. The existence of a ring isomorphism means that any fact about the structure $\mathbb{Z}/m_1m_2\mathbb{Z}$ which is phrased solely in terms of addition and multiplication (e.g., x has a multiplicative inverse in $\mathbb{Z}/m_1m_2\mathbb{Z}$) can be transferred over to a corresponding fact in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ (e.g., $g(x)$ has a multiplicative inverse in $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$). If you are interested in learning more, consider taking Mathematics 113.

Finally, we restate the CRT with the more nuanced view:

Theorem 2 (Chinese Remainder Theorem). *Let n be a positive integer and $m_1, \dots, m_n > 1$ be coprime integers. Then,*

$$\mathbb{Z}/m_1 \cdots m_n\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}).$$

In other words, there exists a function

$$g : \mathbb{Z}/m_1 \cdots m_n\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$$

such that g is a bijection and for all $x, y \in \mathbb{Z}/m_1 \cdots m_n\mathbb{Z}$,

$$\begin{aligned} g(x+y) &= g(x) + g(y), \\ g(xy) &= g(x)g(y). \end{aligned}$$

The isomorphism is explicitly given by $g(x) := (x \bmod m_1,\ \dots,\ x \bmod m_n)$.