Mathematics, KTH
Bengt Ek
October 2015

Supplementary material for SF2736, Discrete mathematics:

The Chinese remainder theorem

We know that for all $m \in \mathbb{Z}_+$ and all $a \in \mathbb{Z}$, all integers x that satisfy

$$x \equiv a \pmod{m}$$

are given by $x = a + tm$, for $t \in \mathbb{Z}$. That is immediate from the definition of congruence mod m: $m \mid (x - a) \Leftrightarrow x - a = tm$ for some $t \in \mathbb{Z}$.

But suppose we have several such congruences and we want to find every x that satisfies all of them. That is, we want all solutions x of the following **system of congruences**:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \qquad (*)$$

where k, $m_1, \ldots, m_k \in \mathbb{Z}_+$ and $a_1, \ldots, a_k \in \mathbb{Z}$. In the simplest case, when the modules m_i are pairwise coprime, **the Chinese remainder theorem** (Sw. **Kinesiska restsatsen**) states that (for every $k \in \mathbb{Z}_+$ and) for every choice of integers a_1, $a_2, \ldots,$ a_k there are solutions to the system and also how different solutions are related to each other.

The natural mapping $\mathbb{Z} \to (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k})$

Let $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$ denote the set of all k-tuples $(b_1, b_2, \ldots, b_k)$, where $b_i \in \mathbb{Z}_{m_i}$, for $i = 1, \ldots, k$. We define the function

$$F : \mathbb{Z} \to (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k})$$

by

$$F(x) = ([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_k})$$

where $[x]_{m_i} = \{y \in \mathbb{Z} \mid y \equiv x \pmod{m_i}\}$, i.e. $[x]_{m_i}$ is "x considered as an element of $\mathbb{Z}_{m_i}$".

Example. Taking $x = 718$, $m_1 = 5$, $m_2 = 6$, $m_3 = 7$, we find

$$F(718) = ([718]_5, [718]_6, [718]_7) = ([3]_5, [4]_6, [4]_7), \text{ usually written } (3, 4, 4).$$

Recalling that $[x]_{m_i} = [a_i]_{m_i}$ iff $x \equiv a_i \pmod{m_i}$, we see that $x \in \mathbb{Z}$ satisfies $(*)$ iff

$$F(x) = ([a_1]_{m_1}, [a_2]_{m_2}, \ldots, [a_k]_{m_k}).$$

Furthermore

$$\begin{aligned} F(x) = F(y) &\Leftrightarrow [x]_{m_i} = [y]_{m_i} \text{ for } i = 1, \ldots, k \Leftrightarrow \\ &\Leftrightarrow x \equiv y \pmod{m_i} \text{ for } i = 1, \ldots, k \Leftrightarrow m_i \mid (x - y) \text{ for } i = 1, \ldots, k \Leftrightarrow \\ &\Leftrightarrow \operatorname{lcm}(m_1, \ldots, m_k) \mid (x - y), \end{aligned}$$

so if x satisfies $(*)$, y does so **iff $\boldsymbol{x \equiv y \pmod{\operatorname{lcm}(m_1, \ldots, m_k)}}$**.

Now we assume that the modules $\boldsymbol{m_i}$ **are pairwise coprime** and introduce $\boldsymbol{m = m_1 \cdot m_2 \cdot \ldots \cdot m_k}$. Then $\operatorname{lcm}(m_1, \ldots, m_k) = m$, so

$$F(x) = F(y) \Leftrightarrow m \mid (x - y) \Leftrightarrow [x]_m = [y]_m.$$

That means that F defines a function

$$f : \mathbb{Z}_m \to (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}) \text{ by } f([x]_m) = F(x).$$

$\Leftarrow$ above shows that different $y \in [x]_m$ have equal $F(y)$, so f is well-defined. $\Rightarrow$, on the other hand, shows that $f([x]_m) = f([y]_m) \Rightarrow [x]_m = [y]_m$, so f is one-to-one (an injection). Since $|\mathbb{Z}_m| = m = m_1 \cdot \ldots \cdot m_k = |\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}|$ and f takes different elements in $\mathbb{Z}_m$ to different elements in $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$, every element in $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$ is taken, so $\boldsymbol{f}$ **is one-to-one and onto** (a bijection).

Example. Taking $m_1 = 3$, $m_2 = 5$ (which are coprime), making $m = 15$, we find for $f : \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$ (omitting the $[.]_{15}$, $[.]_3$, $[.]_5$):

$$\begin{array}{lll} f(0) = (0,0), & f(5) = (2,0), & f(10) = (1,0) \\ f(1) = (1,1), & f(6) = (0,1), & f(11) = (2,1) \\ f(2) = (2,2), & f(7) = (1,2), & f(12) = (0,2) \\ f(3) = (0,3), & f(8) = (2,3), & f(13) = (1,3) \\ f(4) = (1,4), & f(9) = (0,4), & f(14) = (2,4) \end{array}$$

and we can verify that every element in $\mathbb{Z}_3 \times \mathbb{Z}_5$ appears exactly once as a value.

An isomorphism $(\mathbb{Z}_{\boldsymbol{m}}, +, \cdot) \approx (\mathbb{Z}_{\boldsymbol{m_1}} \times \ldots \times \mathbb{Z}_{\boldsymbol{m_k}}, +, \cdot)$

Defining addition and multiplication componentwise in $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$, i.e.

$$([x]_{m_1}, \ldots, [x]_{m_k}) + ([y]_{m_1}, \ldots, [y]_{m_k}) = ([x]_{m_1} + [y]_{m_1}, \ldots, [x]_{m_k} + [y]_{m_k}),$$

$$([x]_{m_1}, \ldots, [x]_{m_k}) \cdot ([y]_{m_1}, \ldots, [y]_{m_k}) = ([x]_{m_1} \cdot [y]_{m_1}, \ldots, [x]_{m_k} \cdot [y]_{m_k}),$$

(note that $+$ and $\cdot$ on the left hand sides are defined here, whereas $+$ and $\cdot$ on the right hand sides are in the different $\mathbb{Z}_{m_i}$) and recalling that $[x]_n + [y]_n = [x + y]_n$, $[x]_n \cdot [y]_n = [x \cdot y]_n$ (by the definition of $+$ and $\cdot$ in $\mathbb{Z}_n$), we find for $x, y \in \mathbb{Z}_m$:

$$\boldsymbol{f(x) + f(y) = f(x + y)} \quad \text{and} \quad \boldsymbol{f(x) \cdot f(y) = f(x \cdot y).}$$

($+$ and $\cdot$ on the left are as defined above and $+$ and $\cdot$ on the right are in $\mathbb{Z}_m$.)

This means that f is an **isomorphism** (Sw. **isomorfi**) (a structure-preserving bijection) between $(\mathbb{Z}_m, +, \cdot)$ and $(\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}, +, \cdot)$, denoted

$$\boldsymbol{(\mathbb{Z}_m, +, \cdot) \approx (\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}, +, \cdot).}$$

We have shown the

Theorem:
If k, $m_1, \ldots, m_k \in \mathbb{Z}_+$, $\gcd(m_i, m_j) = 1$ if $i \neq j$, and $m = m_1 \cdot \ldots \cdot m_k$, then the natural mapping $f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$ defines an isomorphism

$$(\mathbb{Z}_m, +, \cdot) \approx (\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}, +, \cdot)$$

This isomorphism can be used to simplify calculations in $\mathbb{Z}_m$.
For example, to calculate $x \cdot y$ one can find $f(x)$ and $f(y)$, calculate $f(x) \cdot f(y) = f(x \cdot y)$ (using simpler calculation in the $\mathbb{Z}_{m_i}$, possibly in parallel) and then "go back" (since f is one-to-one) to find $x \cdot y$ in $\mathbb{Z}_m$.
Since f is one-to-one and $f(1) = ([1]_{m_1}, \ldots, [1]_{m_k})$ we also see that

$x \in \mathbb{Z}_m$ is invertible $\Leftrightarrow$ there is a $y \in \mathbb{Z}_m$ with $x \cdot y = 1 \Leftrightarrow$
$\Leftrightarrow$ there is a $y \in \mathbb{Z}_m$ with $f(x) \cdot f(y) = f(1) \Leftrightarrow$
$\Leftrightarrow$ there is a $y \in \mathbb{Z}_m$ with $[x]_{m_i} \cdot [y]_{m_i} = [1]_{m_i}$ for $i = 1, \ldots, k \Leftrightarrow$
$\Leftrightarrow [x]_{m_i}$ is invertible for $i = 1, \ldots, k$,

so $x \in \mathbb{Z}_m$ is invertible (in $\mathbb{Z}_m$) iff $[x]_{m_i}$ is invertible (in $\mathbb{Z}_{m_i}$) for $i = 1, \ldots, k$ and then $f(x^{-1}) = ([x]_{m_1}^{-1}, \ldots, [x]_{m_k}^{-1})$.

Example. Again taking $m_1 = 3$, $m_2 = 5$ and $m = 15$, we can calculate $9 \cdot 13$ in $\mathbb{Z}_{15}$ like this:
By the table above, $f(9) = (0, 4)$, $f(13) = (1, 3)$, so $f(9 \cdot 13) = f(9) \cdot f(13) = (0 \cdot 1, 4 \cdot 3) = (0, 2) = f(12)$ (the last '=' by the table). Since f is one-to-one this implies that $9 \cdot 13 = 12$ in $\mathbb{Z}_{15}$.
In the same way we find $f(9+13) = (0, 4)+(1, 3) = (1, 2) = f(7)$, so $9+13 = 7$ in $\mathbb{Z}_{15}$.
Also $f(12) = (0, 2)$ shows that 12 is not invertible in $\mathbb{Z}_{15}$ (since 0 is not invertible in $\mathbb{Z}_3$) and $f(13) = (1, 3)$ shows that 13 is invertible in $\mathbb{Z}_{15}$ (since $[1]_3$ and $[3]_5$ are invertible) and $f(13^{-1}) = (1^{-1}, 3^{-1}) = (1, 2) = f(7)$ gives $13^{-1} = 7$.

When calculating with very large numbers (in $\mathbb{Z}$), especially when many additions and multiplications must be carried out after each other, the method described here can be used to speed up the calculations (**fast arithmetic**). Then one would use m_i of a reasonable size and a fairly large k to give a very big m. The calculations can then be carried out in parallel in each $\mathbb{Z}_{m_i}$ and if we can estimate that the result is in some interval of length m, the value in $\mathbb{Z}$ is determined by the result (which is in $\mathbb{Z}_m$).
For this to be useful in practice, we must be able to compute values of f and f^{-1} (i.e. find a value of x with given $([x]_{m_1}, \ldots, [x]_{m_k})$) reasonably fast. In the example we looked up the values in the table, but that is of course not possible when m is huge. f is found by division with (the not very big) m_i, which is fast, and for f^{-1} we shall find an efficient method in the next section.

Back to the Chinese remainder theorem

The existence of the bijection $f : \mathbb{Z}_m \to (\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k})$ expressed in terms of solutions to the system of congruences $(*)$ we started out with gives

The Chinese remainder theorem:
If $k, m_1, \ldots, m_k \in \mathbb{Z}_+$, $\gcd(m_i, m_j) = 1$ if $i \neq j$, $m = m_1 \cdot \ldots \cdot m_k$, and $a_1, \ldots, a_k \in \mathbb{Z}$, then the system of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \qquad (*)$$

has a solution, which is unique modulo $m = m_1 \cdot \ldots \cdot m_k$
(i.e. if x is a solution, all solutions are the $x + t \cdot m,\ t \in \mathbb{Z}$).

It remains to find a simple way to obtain one solution $x \in \mathbb{Z}$ of $(*)$, given the m_i and the a_i, i.e. to find x with $F(x) = (a_1, \ldots, a_k)$.

We present two methods:

1. Using the linearity of F:
Suppose we have integers y_i, $i = 1, \ldots, k$ satisfying
$F(y_i) = (\overset{1}{0}, \ldots, 0, \overset{i}{1}, 0, \ldots, \overset{k}{0})$, with the only 1 in position i. Then

$$F(a_1 y_1 + \ldots + a_k y_k) = F(a_1 y_1) + \ldots + F(a_k y_k) = ([a_1]_{m_1}, \ldots, [a_k]_{m_k}),$$

so $\boldsymbol{x = a_1 y_1 + \ldots + a_k y_k}$ **is a solution to** $\boldsymbol{(*)}$ (and all solutions are the integers $y \equiv x \pmod{m}$).

So, if we have such y_i, we can find the solutions of $(*)$ very efficiently. In particular, if we want to solve many systems $(*)$ with different a_i, it is enough to compute the y_i once (since they don't depend on the a_i). They can then be stored once and for all, to be used whenever we need them.

To find the y_i, remember that they satisfy $(*)$ with $a_i = 1$, $a_j = 0$ for $j \neq i$. If we let $M_i = \frac{m}{m_i} = m_1 \cdot \ldots \cdot \cancel{m_i} \cdot \ldots \cdot m_k$, then $M_i \cdot b_i$ will be an acceptable y_i if $M_i \cdot b_i \equiv 1 \pmod{m_i}$ and since $\gcd(M_i, m_i) = 1$ there are such b_i for $i = 1, \ldots, k$.

Example. In a previous example we used $m_1 = 5$, $m_2 = 6$, $m_3 = 7$ (pairwise coprime), so $m = 5 \cdot 6 \cdot 7 = 210$, and found $F(718) = (3, 4, 4)$. That means for $719 = 89 \in \mathbb{Z}_{210}$ that $f(89) = (4, 5, 5)$ and we see that $f(89^{-1}) = (4^{-1}, 5^{-1}, 5^{-1}) = (4, 5, 3) \in \mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7$. (718 is not invertible in $\mathbb{Z}_{210}$ since 4 is not invertible in $\mathbb{Z}_6$).

To find 89^{-1}, we calculate (one possible choice of) y_1, y_2, y_3 in this case:

$y_1 = 6 \cdot 7 \cdot b_1 = 42 b_1 \equiv_5 1 \Leftrightarrow 2 b_1 \equiv_5 1$ and we can take $b_1 = 3$, so $y_1 = 126$.
(Here we found b_1 "by inspection", but in a realistic case one would use the Euclidean algorithm to find $b_1 = M_1^{-1} \in \mathbb{Z}_{m_1}$.)

$y_2 = 5 \cdot 7 \cdot b_2 = 35 b_2 \equiv_6 1 \Leftrightarrow -b_2 \equiv_6 1$, we take $b_2 = -1$, so $y_2 = -35$.

$y_3 = 5 \cdot 6 \cdot b_3 = 30 b_3 \equiv_7 1 \Leftrightarrow 2 b_3 \equiv_7 1$, we take $b_3 = 4$, so $y_3 = 30 \cdot 4 = 120$.

Since $f(89^{-1}) = (4, 5, 3)$ we find
$89^{-1} = 4y_1 + 5y_2 + 3y_3 = 4 \cdot 126 + 5(-35) + 3 \cdot 120 = 689 \equiv_{210} 59$ (in $\mathbb{Z}_{210}$).

The method used in the example to compute $89^{-1} \in \mathbb{Z}_{210}$ is probably slower than the direct method using the Euclidean algorithm, but it illustrates the method to compute f^{-1}. For a single example it is often faster to use a direct method:

2. Solving the congruences one by one:
We take the same example as above and want to solve

$$\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 6 \\ x \equiv 3 \pmod 7. \end{cases} \qquad (*)$$

The first equation is satisfied iff $x = 4 + 5s$ for some $s \in \mathbb{Z}$.
These x also satisfy the second equation iff

$$4 + 5s \equiv_6 5 \Leftrightarrow -s \equiv_6 1 \Leftrightarrow s = -1 + 6t \text{ for some } t \in \mathbb{Z},$$

i.e. iff $x = 4 + 5(-1 + 6t) = -1 + 30t$ for some $t \in \mathbb{Z}$.
x satisfies all three equations iff

$$-1 + 30t \equiv_7 3 \Leftrightarrow 2t \equiv_7 4 \Leftrightarrow t \equiv_7 2 \Leftrightarrow t = 2 + 7n \text{ for some } n \in \mathbb{Z}$$

(using $\gcd(2, 7) = 1$ in the next to last step).
So, all three congruences are satisfied iff $x = -1 + 30t = -1 + 30(2 + 7n) = 59 + 210n$ for some $n \in \mathbb{Z}$.
This means that $[89]_{210}^{-1} = [59]_{210}$, as with method 1.

Exercises

1. Find all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7). \end{cases}$$

Use both the methods presented in the text.
Also find all $y \in \mathbb{Z}$ such that for all solutions x, $x \cdot y \equiv 1 \pmod 3$, $\pmod 5$ and $\pmod 7$.

2. Find all integers x with $0 \leq x \leq 3000$ such that

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{13}). \end{cases}$$

3. Let $f : \mathbb{Z}_{315} \to (\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_9)$ be as in the text.

a. Find $f(3)$ and $f(43)$.
b. Find $f^{-1}((1, 0, 0))$, $f^{-1}((0, 1, 0))$ and $f^{-1}((0, 0, 1))$.
c. Use f and f^{-1} to calculate $(186 + 212) \cdot 88^{-1} + 167$ in $\mathbb{Z}_{315}$.

4. Find all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 6). \end{cases}$$

Answers

1. $x = 68 + 105m,\ m \in \mathbb{Z}$ and $y = 17 + 105n,\ n \in \mathbb{Z}$.

2. $x = 811,\ 2527$.

3a. $(3, 3, 3)$ and $(3, 1, 7)$, **b.** 126, 225 and 280, **c.** 193.

4. There are no such x.