Summer High School 2009
Aaron Bertram

5. The Chinese Remainder Theorem.

Notation. Let R_n be the set of *remainders* mod n.

We can write:

$$R_n = \{0, 1, 2, 3, \ldots, n-1\}$$

and think of it as points on the number line:

$$\begin{array}{cccccccc} * & * & * & * & \ldots & * & * \\ 0 & 1 & 2 & 3 & \cdots & n-2 & n-1 \end{array}$$

We can think of "mod_n" as a remainder *function* from $\mathbb{Z}$ to R_n:

$$\mathrm{mod}_n(0) = 0, \mathrm{mod}_n(1) = 1, \cdots, \mathrm{mod}_n(n-1) = n-1$$

$$\mathrm{mod}_n(n) = 0, \mathrm{mod}_n(n+1) = 1, \cdots$$

that wraps around as integers are increased by multiples of n.

Next, consider the *Cartesian product* of two of these sets:

$$R_m \times R_n = \{(k, l) \mid 0 \leq k < m, 0 \leq l < n\}$$

which is a set of ordered pairs, or, visually, a rectangle of points:

$$\begin{array}{cccccccc} n-1 & * & * & * & * & \ldots & * & * \\ n-2 & * & * & * & * & \ldots & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 3 & * & * & * & * & \ldots & * & * \\ 2 & * & * & * & * & \ldots & * & * \\ 1 & * & * & * & * & \ldots & * & * \\ 0 & * & * & * & * & \ldots & * & * \\ & 0 & 1 & 2 & 3 & \cdots & m-2 & m-1 \end{array}$$

Definition 5.1. The *remainders mod m and n* function:

$$\mathrm{mod}_{m,n} : R_{mn} \to R_m \times R_n$$

takes a single remainder (r mod mn) to the ordered pair of remainders (r mod m, r mod n). It is well-defined because m and n divide mn.

Examples: The two sets R_{mn} and $R_m \times R_n$ have the same number of elements, namely, mn, so there is a chance that taking remainders mod m and n might be a *bijection* of the two sets:

(a) The remainders function $\mathrm{mod}_{2,3}$ **is** a bijection.

$$\mathrm{mod}_{2,3}(0) = (0,0), \quad \mathrm{mod}_{2,3}(1) = (1,1), \quad \mathrm{mod}_{2,3}(2) = (0,2),$$
$$\mathrm{mod}_{2,3}(3) = (1,0), \quad \mathrm{mod}_{2,3}(4) = (0,1), \quad \mathrm{mod}_{2,3}(5) = (1,2)$$

(b) The remainders function $\text{mod}_{2,2}$ is **not** a bijection.

$\text{mod}_{2,2}(0) = (0,0), \text{mod}_{2,2}(1) = (1,1),$
$\text{mod}_{2,2}(2) = (0,0), \text{mod}_{2,2}(3) = (1,1)$

We can visualize the remainders function by wrapping the numbers from 0 to $mn-1$ around the $m \times n$ rectangle. The function will be a bijection if they wrap without overlapping:

Visual Examples:

(c) Remainders $\text{mod}_{3,4}$ "wrap without overlap":

$$\begin{array}{ccc} 3 & 7 & 11 \\ 6 & 10 & 2 \\ 9 & 1 & 5 \\ 0 & 4 & 8 \end{array}$$

(d) Remainders mod $_{2,4}$ "overlap when they wrap":

$$\begin{array}{cc} * & 3,7 \\ 2,6 & * \\ * & 1,5 \\ 0,4 & * \end{array}$$

Chinese Remainder Theorem:
When $\text{GCD}(m,n) = 1$, $\text{mod}_{m,n}$ is a bijection.

Proof: The best way to prove that a function is a bijection is to find the *inverse function*. We can do this using the equation:

$$am + bn = 1 \text{ when } m \text{ and } n \text{ are relatively prime}$$

for integers a and b (that we can compute using Euclid's algorithm!). So suppose (s,t) is a pair of remainders mod m and mod n. Then:

$$amt + bns \mod mn$$

will give us what we want, namely, a remainder r mod mn with the property that $\text{mod}_{m,n}(r) = (s,t)$. That's because:

$$bns = s - ams \quad \text{and} \quad amt = t - bnt$$

by the equation above, so:

$$(\text{Mod } m) \quad r \equiv amt + bns \equiv bns \equiv s - bms \equiv s$$

and

$$(\text{Mod } n) \quad r \equiv amt + bns \equiv amt \equiv t - bnt \equiv t$$

□

Corollary 1: From the previous section,

$$\phi(mn) = \phi(m)\phi(n)$$

whenever m and n are relatively prime.

Proof: A remainder mod mn is relatively prime to mn if it has no prime factors in common with mn. But this is the case if and only if it has no prime factors in common with m and with n. So the bijection of the Chinese Remainder Theorem must take relatively prime remainders to pairs of relatively prime remainders. Thus these sets must also be in bijection, so they have the same numbers of elements. □

The next Corollary is really useful in practice.

Corollary 2: Arithmetic mod mn can be done mod m and mod n by first taking remainders, then doing the arithmetic, then using the inverse function of the Chinese Remainder Theorem.

Example. Calculate $17 \cdot 23 \bmod 35 = 5 \cdot 7$.

First use Euclid's algorithm:

$$\begin{array}{rcrcr} 7 & = & 1 \cdot 5 & + & 2 \\ 5 & = & 2 \cdot 2 & + & 1 \end{array}$$

and the matrices/vectors:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ -2 \end{pmatrix}$$

to get:

$$3 \cdot 5 + (-2) \cdot 7 = 1, \quad \text{so} \quad a = 3 \text{ and } \ b = -2$$

Now take remainders and multiply:

$$17 \equiv 2 \bmod 5 \text{ and } 23 \equiv 3 \bmod 5, \text{ so } 17 \cdot 23 \equiv 2 \cdot 3 \equiv 1 \bmod 5$$

$$17 \equiv 3 \bmod 7 \text{ and } 23 \equiv 2 \bmod 7, \text{ so } 17 \cdot 23 \equiv 3 \cdot 2 \equiv 6 \bmod 7$$

That is, we get $(2,3) \cdot (3,2) \equiv (1,6) \bmod (m,n)$. Next, follow the prescription of the Chinese Remainder Theorem to take:

$$amt + bns = (3)(5)(6) + (-2)(7)(1) = 90 - 14 = 76 \equiv 6 \bmod 35$$

The answer is 6. We can check this:

$$17 \cdot 23 = 391 \equiv 41 \equiv 6 \bmod 35$$

Check!

Example. This one appeared in this year's IB mathematics exam.

Problem: Prove that the ones digit of any natural number n is always equal to the ones digit of n^5.

Proof: The ones digit of n is its remainder mod 10. It suffices to check this problem with mod 10 arithmetic. Here's the long answer:

$0^5 = 0 \equiv 0 \bmod 10$, $1^5 = 1 \equiv 1 \bmod 10$

$2^5 = 32 \equiv 2 \bmod 10$, $3^5 = 243 \equiv 3 \bmod 10$

$4^5 = 1024 \equiv 4 \bmod 10$, $5^5 = 3125 \equiv 5 \bmod 10$

$6^5 = (-4)^5 \equiv (-1)^5(4^5) \equiv (-1)(4) \equiv 6 \bmod 10$

etc. (the minus sign trick eliminates a lot of arithmetic!)

Or, you can reason as follows. By the Chinese Remainder Theorem, arithmetic mod 10 is the same as arithmetic of pairs (s,t) mod $(2,5)$, so it suffices to show that each:

$$s^5 \equiv s \bmod 2 \text{ and } t^5 \equiv t \bmod 5$$

$0^5 = 0$ and $1^5 = 1$ takes care of mod 2 and

$0^5 = 0, 1^5 = 1, 2^5 = 32 \equiv 2, 3^5 \equiv (-2)^5 \equiv 3, 4^5 \equiv (-1)^5 \equiv 4$

takes care of mod 5, so $2^5 = 32$ was the only calculation we needed!

Higher Dimensional Version of the CRT:

Suppose $n = m_1 m_2 m_3 \cdots m_k$ such that each $\text{GCD}(m_i, m_j) = 1$. Then there is an inverse function to the multi-dimensional remainder:

$$\text{mod}_{m_1,m_2,\ldots,m_k} : R_n \to R_{m_1} \times \cdots R_{m_k}$$

given as follows. Since each m_i is relatively prime to the product of all the other m's, namely n/m_i, Euclid's algorithm gives integers a_i, b_i such that:

$$a_1 m_1 + b_1(n/m_1) = 1, \quad a_2 m_2 + b_2(n/m_2) = 1, \text{ etc}$$

The inverse of $\text{mod}_{m_1,m_2,\cdots m_k}$ is given by sending a multi-dimensional remainder $(s_1, s_2, \cdots, s_k)$ to:

$$b_1(n/m_1)s_1 + b_2(n/m_2)s_2 + \cdots + b_k(n/m_k)s_k \bmod n$$

This version is extensively used in computer science!

Example: (Stupid Party Trick) Ask a friend to choose a number between 0 and 100 (actually, 104 will do). Now ask her to give you the remainders when her number is divided by $3, 5$ and 7. You quickly scribble something down and come up with her number(!)

Here's what you scribble. In advance, you've calculated:

$$b_1 = -1, \quad b_2 = 1, \quad b_3 = 1$$

so when you're given the three remainders (s_1, s_2, s_3), all you do is find:

$$-35s_1 + 21s_2 + 15s_3 \bmod 105$$

For example, if she says $(2, 3, 4)$, you scribble out $-70 + 63 + 60 = 53$ and impress her and the rest of your friends!