The Chinese Remainder Theorem.
Topics in Algebra 5900
Spring 2011
Aaron Bertram

Let p and q be two (different) primes.

Definition. (i) The "mod pq" numbers are all the remainders:

$$\{0, 1, 2, \ldots, pq - 1\}$$

when a natural number is divided by pq.

(ii) Addition and multiplication are defined as for mod p numbers.

Example. The multiplication table for **mod 6** numbers is:

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

There are two important differences from arithmetic mod p:

(i) There are zero entries in the interior of the multiplication table.

(ii) Some numbers (e.g. p and q) have no reciprocals mod pq.

Example: The multiplication table for **mod 15** numbers is:

*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	4	11	3	10	2	9	1	8

which can be completed with negative numbers as we did mod p.

Notice: The numbers that are divisible by p or q are the *only* numbers that "divide zero" and fail to have a reciprocal.

Definition. The **Cartesian product** of the numbers mod p and q is the set of all *ordered pairs* (r, s) where $r \in \{0, 1, \ldots, p-1\}$ and $s \in \{0, 1, \ldots . q-1\}$. It is written $\{0, 1, 2, \ldots, p-1\} \times \{0, 1, 2, \ldots, q-1\}$.

Example. The Cartesian product $\{0,1\} \times \{0,1,2\}$ is:

$$\{(0,0),(1,0),(0,1),(1,1),(0,2),(1,2)\}$$

(which can be thought of as points in the plane).

The Chinese Remainder Theorem. The numbers mod pq map to the Cartesian product of the numbers mod p and mod q by taking their "further remainders" after dividing by p and q:

$$\{0,1,2,\ldots,pq-1\} \to \{0,1,2,\ldots,p-1\} \times \{0,1,2,\ldots,q-1\}$$

This map "preserves the arithmetic" and **it has an inverse.**

Example: The numbers mod 6 map to $\{0,1\} \times \{0,1,2\}$ as follows:

$$0 \mapsto (0,0)$$
$$1 \mapsto (1,1)$$
$$2 \mapsto (0,2)$$
$$3 \mapsto (1,0)$$
$$4 \mapsto (0,1)$$
$$5 \mapsto (1,2)$$

This map has an inverse simply because it is a bijection.

The Genius of the Chinese Remainder Theorem. There is a systematic way to construct the inverse map. It is done as follows:

Step 1. Find integers a and b so that:

$$ap + bq = 1$$

(this can always be done using the Euclidean algorithm).

Step 2. Given an ordered pair (r,s), take the remainder when:

$$rbq + sap \text{ is divided by } pq$$

This is the inverse image of (m,n) among the numbers mod pq.

Example. In the case of $pq = 6$, we easily find:

$$(-1)2 + (1)3 = 1$$

so we get the inverse by:

$$(0,0) \mapsto 0(3) + 0(-2) = 0$$
$$(1,0) \mapsto 1(3) + 0(-2) = 1$$
$$(0,1) \mapsto 0(3) + 1(-2) = -2 = 4 \text{ (mod 6)}$$
$$(1,1) \mapsto 1(3) + 1(-2) = 1$$
$$(0,2) \mapsto 0(3) + 2(-2) = -4 = 2 \text{ (mod 6)}$$
$$(1,2) \mapsto 1(3) + 2(-2) = -1 = 5 \text{ (mod 6)}$$

A Fancier Example: Consider the numbers mod 17 and mod 19 (and mod $323 = 17 \cdot 19$). From the fact that:

$$9 \cdot 17 + (-8) \cdot 19 = 153 - 152 = 1$$

we find that we can invert the map:

$$\{\text{numbers mod } 323\} \to \{\text{numbers mod } 17\} \times \{\text{numbers mod } 19\}$$

by sending:

$$(r, s) \mapsto r(-152) + s(153) \pmod{323}$$

Thus, for example,

$$20 \mapsto (3, 1) \text{ which are its remainders mod 17 and 19}$$

and

$$3(-152) + 1(153) = -303 = 20 \pmod{323}$$

is the inverse, which recovers 20 from the ordered pair $(3, 1)$.

More Chinese Remainders: Given three distinct primes o, p, q, the map from numbers mod opq to ordered **triples** of numbers mod o, mod p and mod q:

$$\{\text{numbers mod } opq\} \to$$
$$\{\text{numbers mod } o\} \times \{\text{numbers mod } p\} \times \text{ numbers mod } q\}$$

can be inverted as follows:

Step 1. Solve the following three equations with integers a, b, c, d, e, f:

$$ao + bpq = 1$$
$$cp + doq = 1$$
$$eq + fop = 1$$

Step 2. Given an ordered triple (r, s, t), take:

$$r(bpq) + s(doq) + t(fop) \text{ (mod opq)}$$

This is the inverse.

Example. Consider the numbers mod $105 (= 3 \cdot 5 \cdot 7)$.

Step 1. Solve the three magic equations:

$$(12)3 + (-1)35 = 1$$
$$(-4)5 + (1)21 = 1$$
$$(-2)7 + (1)15 = 1$$

Step 2. A number mod 105 can be recovered from its ordered triple (r, s, t) mod $3, 5, 7$ by taking:

$$r(-35) + s(21) + t(15) \pmod{105}$$

Impress your friends. Ask a friend to take his or her age and give you only the remainders when it is divided by $3, 5$ and 7. You will recover the age with Step 2 above in no time!