

THE CHINESE REMAINDER THEOREM

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

The goal of this handout is to prove the Chinese Remainder Theorem.

1. PRELIMINARIES

One important concept associated to the finite ring \mathbb{Z}_m is the idea of *well-defined*.

Lemma 1. *Suppose m and d are positive integers. If $d \mid m$ then the rule $[a]_m \mapsto [a]_d$ is a well-defined function $\mathbb{Z}_m \rightarrow \mathbb{Z}_d$.*

Proof. To show it is well-defined we must show that if $[a]_m = [b]_m$, then the rule gives a consistent result when applied to $[a]_m$ or $[b]_m$. In other words, we must show that $[a]_d = [b]_d$.

So suppose $[a]_m = [b]_m$. Then $a \equiv b \pmod{m}$. So $m \mid (a - b)$. But $d \mid m$, so by transitivity of divisibility, $d \mid (a - b)$. Thus $a \equiv b \pmod{d}$. So $[a]_d = [b]_d$. \square

Remark. In the above proof, we used the very basic fact that $[x]_m = [y]_m$ if and only if $x \equiv y \pmod{m}$.

Remark. If $d \nmid m$ then the map is not well-defined. Consider the case where $m = 7$ and $d = 5$. Then the rule $[a]_7 \mapsto [a]_5$ is not well-defined because $[3]_7 \mapsto [3]_5$ but $[10]_7 \mapsto [10]_5 = [0]_5$. But $[3]_7 = [10]_7$. So equal elements map to non-equal elements, which is not allowed.

Remark. Let m and n be positive integers. Obviously, $m \mid mn$ and $n \mid mn$. So it follows from the above lemma that the function $\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ given by the rule $[a]_{mn} \mapsto ([a]_m, [a]_n)$ is well-defined. Recall from set theory that $\mathbb{Z}_m \times \mathbb{Z}_n$ is the set of ordered pairs whose first element is in \mathbb{Z}_m and whose second element is in \mathbb{Z}_n . By a basic counting argument, the set $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements. For example,

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \left\{ ([0]_2, [0]_3), ([1]_2, [0]_3), ([0]_2, [1]_3), ([1]_2, [1]_3), ([0]_2, [2]_3), ([1]_2, [2]_3) \right\}.$$

Finally, I should mention that $\mathbb{Z}_m \times \mathbb{Z}_n$ is a commutative ring.

Similarly, if $m = m_1 m_2 \cdots m_r$ where each m_i is a positive integer, then

$$\mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}, \quad [a]_m \mapsto ([a]_{m_1}, [a]_{m_2}, \dots, [a]_{m_r})$$

is a well-defined function. (Here, both the domain and codomain have m elements.)

Proposition 1. *Let m be a positive integer and let $a \in \mathbb{Z}$. Then $\bar{a} = [a]_m$ is a unit in $U_m \subset \mathbb{Z}_m$ if and only if $(a, m) = 1$.*

Proof. Suppose \bar{a} is a unit. Then there is a $b \in \mathbb{Z}$ such that $\bar{a}\bar{b} = \bar{1}$. In other words, $ab \equiv 1 \pmod{m}$. This implies that m divides $ab - 1$. So $ab - 1 = km$ for some $k \in \mathbb{Z}$. Write this equation as $ba + (-k)m = 1$. This shows that 1 is a linear combination of a and m . Since

there are no positive integers less than 1, this implies that 1 is the *least* linear combination of a and m . By Bezout's identity, $(a, m) = 1$.

Now suppose $(a, m) = 1$. By Bezout's identity again, 1 is a linear combination of a and m , so there is u and v with $ua + vm = 1$. So

$$1 \equiv ua + vm \equiv ua + v0 \equiv ua \pmod{m}.$$

This shows that $\bar{u} \cdot \bar{a} = \bar{1}$ in \mathbb{Z}_m . Thus \bar{a} is a unit. \square

Remark. The Euclidean Algorithm is a computational effective method for determining if \bar{a} is a unit, and for finding the multiplicative inverse of \bar{a} whenever it exists.

2. THE PROOF

For convenience we divide the proof up into lemmas. Throughout we assume that we are dealing with the function

$$\mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}, \quad [a]_m \mapsto \left([a]_{m_1}, [a]_{m_2}, \dots, [a]_{m_r} \right)$$

where $m = m_1 m_2 \cdots m_r$, each m_i is a positive integer, and $(m_i, m_j) = 1$ if $i \neq j$.

Lemma 2. *Consider the above function and assume that $(m_i, m_j) = 1$ for each $i \neq j$. Then for each i there exists an element $[e_i]$ which maps to*

$$\left([0]_{m_1}, \dots, [0]_{m_{i-1}}, [1]_{m_i}, [0]_{m_{i+1}}, \dots, [0]_{m_r} \right).$$

Proof. We prove this for $i = 1$. The proof for other i is similar. Let $c_1 = m/m_1 = m_2 \cdots m_r$. Since $(m_1, m_j) = 1$ if $j \neq 1$, it follows that $[m_j]_{m_1}$ is a unit. The product of units is a unit (by closure), so $[c_1]_{m_1}$ is also a unit, and it has a multiplicative inverse $[b_1]_{m_1}$. Let $e_1 = b_1 c_1$.

If $j > 1$ then $e_1 \equiv b_1 c_1 \equiv b_1 0 \equiv 0 \pmod{m_j}$ since $m_j \mid c_1$. Things are different modulo m_1 . In this case we have $e_1 \equiv b_1 c_1 \equiv 1 \pmod{m_1}$ since $[b_1]_{m_1}$ is the inverse of $[c_1]_{m_1}$. From these congruences, we conclude that

$$[e_1]_m \mapsto \left([1]_{m_1}, [0]_{m_2}, \dots, [0]_{m_r} \right).$$

\square

Example. In order to understand this lemma better, it helps to work through examples. Suppose, for instance, that $m_1 = 3, m_2 = 5, m_3 = 11$ and $m = 3 \cdot 5 \cdot 11 = 165$.

Here $c_1 = 5 \cdot 11 = 55$. In \mathbb{Z}_3 the inverse of $[55]_3$ is $[1]_3$ since $[55]_3 = [1]_3$. So $e_1 = 1 \cdot 55 = 55$. Observe that $[55]_{165} \mapsto ([1]_3, [0]_5, [0]_{11})$.

Next $c_2 = 3 \cdot 11 = 33$. Since $33 \equiv 3 \pmod{5}$, and since $3 \cdot 2 \equiv 1 \pmod{5}$, we can choose $b_2 = 2$. Thus $e_2 = 2 \cdot 33 = 66$. Observe that $[66]_{165} \mapsto ([0]_3, [1]_5, [0]_{11})$.

Finally, $c_3 = 3 \cdot 5 = 15$. The inverse of $[15]_{11}$ is $[3]_{11}$ since $15 \cdot 3 \equiv 1 \pmod{11}$. So $e_3 = 3 \cdot 15 = 45$. Observe that $[45]_{165} \mapsto ([0]_3, [0]_5, [1]_{11})$.

Lemma 3. *Consider the above function and assume that $(m_i, m_j) = 1$ for each $i \neq j$. Let e_i be as in the previous lemma. Let a_1, \dots, a_r be any given integers. Define $x = a_1 e_1 + \dots + a_r e_r$. Then*

$$[x]_m \mapsto \left([a_1]_{m_1}, [a_2]_{m_2}, \dots, [a_r]_{m_r} \right).$$

Proof. Since $[e_1]_m \mapsto ([1]_{m_1}, [0]_{m_2}, \dots, [0]_{m_r})$, it follows that $e_1 \equiv 1 \pmod{m_1}$ and also that $e_1 \equiv 0 \pmod{m_j}$ for $j > 1$. Thus

$$x \equiv a_1 e_1 + a_2 e_2 + \dots + a_r e_r \equiv a_1 1 + a_2 0 + \dots + a_r 0 \equiv a_1 \pmod{m_1}.$$

Thus $[x]_{m_1} = [a_1]_{m_1}$. A similar argument for other values of i give that $[x]_{m_i} = [a_i]_{m_i}$. The result follows. \square

The above shows us that each $([a_1]_{m_1}, [a_2]_{m_2}, \dots, [a_r]_{m_r})$ is in the image of the function. Thus we get the following.

Corollary 1. *If $(m_i, m_j) = 1$ for each $i \neq j$, then the given function is surjective (“onto”).*

Example. We illustrate the above lemma in the case where $m_1 = 3, m_2 = 5, m_3 = 11$ and $m = 3 \cdot 5 \cdot 11 = 165$. Let $e_1 = 55, e_2 = 66$, and $e_3 = 45$ as above.

Suppose someone wants an integer x such that

$$x \equiv 2 \pmod{3}, \quad x \equiv 1 \pmod{5}, \quad \text{and} \quad x \equiv 5 \pmod{11}.$$

So let $a_1 = 2, a_2 = 1$, and $a_3 = 5$. This gives $x = 2e_1 + 1e_2 + 5e_3 = 110 + 66 + 225 = 401$. Thus $x = 401$ works. Since x is considered modulo 165, we can replace 401 with $401 - 2 \cdot 165 = 71$. So $x = 71$ also works:

$$[71]_{165} \mapsto ([2]_3, [1]_5, [5]_{11}).$$

We are ready for the main theorem:

Theorem 1 (Chinese Remainder Theorem). *Let $m = m_1 m_2 \dots m_r$ where each m_i is a positive integer, and where $(m_i, m_j) = 1$ if $i \neq j$. Then the function*

$$\mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r}, \quad [a]_m \mapsto ([a]_{m_1}, [a]_{m_2}, \dots, [a]_{m_r})$$

is a bijection (in other words, it is one-to-one and onto).

Proof. We know from the previous corollary that it is surjective (onto). So we just need to show that it is injective (one-to-one). To do so, we observe that $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r}$ is a set of r -tuples, and by a basic counting principle the number of such r -tuples is $m_1 m_2 \dots m_r = m$. Thus the domain and codomain of the function are finite of the same cardinality. Since the function is surjective, it automatically means that it is a bijection. \square

Remark. In the above proof we used a basic theorem of Dirichlet that you should know from set theory. It states that if the domain and codomain are finite and of the same cardinality, then onto implies one-to-one. In other words, surjective implies bijective.

Remark. For those of you with some knowledge of abstract algebra: The above function is actually an isomorphism between rings.

The Chinese Remainder Theorem is a very useful result with many valuable consequences. Later we will show how it implies that $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$. When $r = 2$ the Chinese remainder theorem can be stated as follows: *if $(m, n) = 1$ then the function*

$$\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, \quad [a]_{mn} \mapsto ([a]_m, [a]_n)$$

is a bijection. One easy consequence is the following:

Corollary 2. *Suppose that m and n are positive relatively prime integers. Suppose that $m \mid a$ and $n \mid a$. Then $mn \mid a$.*

Proof. The hypotheses imply that, under the function $\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ described above, the element $[a]_{mn}$ maps to the ordered pair $([0]_m, [0]_n)$. But $[0]_{mn}$ also maps to that same ordered pair. Since the function is injective (one-to-one), we get that $[a]_{mn} = [0]_{mn}$. Thus $a \equiv 0 \pmod{mn}$. So $mn \mid a$. \square

Remark. The above generalizes easily to possibly negative m and n .

Remark. WARNING: the above fails if $(m, n) > 1$. For example $4 \mid 12$ and $6 \mid 12$, but we cannot conclude that $(4 \cdot 6) \mid 12$.

.
DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA
E-mail address: waitken@csusm.edu