THE CHINESE REMAINDER THEOREM AND THE PHI FUNCTION

MATH 422, CSUSM. SPRING 2009. AITKEN

The goal of this handout is to present a proof of the Chinese Remainder Theorem, and to describe how to compute the associated inverse map. A version of the Chinese Remainder Theorem for units is also considered.

Theorem 1 (Chinese Remainder Theorem: two factors)**.** *Let m and n be relatively prime positive integers. Then the map*

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

defined by the rule $[x]_{mn} \mapsto \big([x]_m, [x]_n\big)$ is a bijection.

Exercise 1. Make a table describing the map for $m = 3$ and $n = 5$. Mentally check that it is indeed a bijection.

Exercise 2. Consider the example of the previous exercise. Mentally check that the units in the domain correspond to pairs of units in the codomain.

Exercise 3. Show that the assumption that m and n are relatively prime is necessary. Hint: give a counter-example for the case where this assumption is dropped.

The Chinese Remainder Theorem can be generalized to any number of relatively prime factors. The following gives the case of three factors.

Theorem 2 (Chinese Remainder Theorem: three factors)**.** *Let a, b, c be pairwise relatively prime positive integers. Then the map*

$$\mathbb{Z}_{abc} \to \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c.$$

defined by the rule $[x]_{abc} \mapsto \big([x]_a, [x]_b, [x]_c\big)$ is a bijection.

1. Some Lemmas

Recall the following (covered in Math 378).

Lemma 3. *Suppose $a, b, c \in \mathbb{Z}$ where $\gcd(a, b) = 1$. If $a \mid c$ and $b \mid c$ then $ab \mid c$.*

Exercise 4. Show that the assumption that $\gcd(a, b) = 1$ is necessary. Hint: give a counter-example for the case where this assumption is dropped.

Lemma 4. *Suppose $a, b, c \in \mathbb{Z}$ where $c \neq 0$. If a and c are relatively prime and if b and c are relatively prime then ab and c are relatively prime.*[1]

Proof. Suppose $d = \gcd(ab, c)$. We wish to show that $d = 1$. Suppose otherwise. Then d must have a prime divisor p. Thus $p \mid ab$. Hence $p \mid a$ or $p \mid b$. The first case contradicts the assumption that $\gcd(a, c) = 1$. The second contradicts $\gcd(b, c) = 1$. □

Date: February 25, 2009.

[1]The assumption that $c \neq 0$ is not really necessary since if $c = 0$ then $|a| = |b| = 1$ follows from the hypotheses, so $|ab| = 1$. Thus ab and c are relatively prime.

2. Well-Definedness

Before we can prove Theorem 1 we need to check that the map defined in the statement of the theorem is indeed a well-defined map. In particular, it should not depend on x but only on $[x]_{ab}$. To do so we must check that if $[x]_{mn} = [y]_{mn}$ then the proposed definition of the function yields the same result whether we use x or use y.

We start with a more basic map. Suppose $d \mid m$ where m is a positive integer. Then consider $\mathbb{Z}_m \to \mathbb{Z}_d$ defined by the rule $[x]_m \mapsto [x]_d$.

Lemma 5. *Suppose m and d are positive integers. If $d \mid m$ then the rule $[x]_m \mapsto [x]_d$ gives a well-defined function $\mathbb{Z}_m \to \mathbb{Z}_d$.*

Proof. To show it is well-defined we must show that if $[x]_m = [y]_m$, then the rule gives the same result whether we use x or y. In other words, we must show that $[x]_d = [y]_d$.

If $[x]_m = [y]_m$ then $x \equiv y \bmod m$. So $m \mid (x - y)$. But $d \mid m$, so by transitivity of divisibility, $d \mid (x - y)$. Thus $x \equiv y \bmod d$. So $[x]_d = [y]_d$. □

Exercise 5. Show that the rule $[x]_7 \mapsto [x]_5$ does not result in a well-defined map $\mathbb{Z}_7 \to \mathbb{Z}_5$.

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 $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ given by the rule $[x]_{mn} \mapsto ([x]_m, [x]_n)$ is well-defined.

Similarly, the function $\mathbb{Z}_{abc} \to \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$, from Theorem 2 is a well-defined function.

Remark. (For readers with abstract algebra experience). It is easily shown that $\mathbb{Z}_m \times \mathbb{Z}_n$ is a commutative ring. The definition of the function $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ implies that this function is actually a ring homomorphism. Theorem 1 implies that it is a ring isomorphism.

If $d \mid m$ then the map $\mathbb{Z}_m \to \mathbb{Z}_d$ is also a surjective homomorphism, but if $d < m$ it is not an isomorphism. The rule $x \mapsto [x]_m$ gives a surjective ring homomorphism $\mathbb{Z} \to \mathbb{Z}_m$ that is clearly not an isomorphism.

3. Proof

Proof of Theorem 1. Let f be the function $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ described in the statement of the theorem (which we now know is well-defined).

First we show that f is injective. Suppose $f\big([x]_{mn}\big) = f\big([y]_{mn}\big)$. In other words,

$$\big([x]_m, [x]_n\big) = \big([y]_m, [y]_n\big).$$

This means $[x]_m = [y]_m$ and $[x]_n = [y]_n$, so $x \equiv y \mod m$ and $x \equiv y \mod n$. Thus $m \mid (x - y)$ and $n \mid (x - y)$ by definition of congruence. In particular, $mn \mid (x - y)$ since m and n are relatively prime (Lemma 3). So $x \equiv y \mod mn$. Thus $[x]_{mn} = [y]_{mn}$.

The above argument shows that f is an injection. It can be shown to be a surjection by a simple counting argument. The domain is the ring $\mathbb{Z}_{mn}$ which has mn elements. The codomain also has mn elements since there are m possible first coordinates and n possible second coordinates. Since the domain and codomain are both finite with the same number of elements, any injection is automatically a surjection. □

Proof of Theorem 2. The map $\mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ is a bijection by Theorem 1. So the map $f : \mathbb{Z}_{ab} \times \mathbb{Z}_c \to \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$ defined by the rule $\big([x]_{ab}, [y]_c\big) \mapsto \big([x]_a, [x]_b, [y]_c\big)$ is easily seen to be a bijection.

Also by Theorem 1, the map $g : \mathbb{Z}_{abc} \to \mathbb{Z}_{ab} \times \mathbb{Z}_c$ is a bijection (see also Lemma 4).
Now consider the composition $f \circ g$ which is the composition of bijections. □

Exercise 6. Check the details of the proof. For example, verify that the map f in the above proof is actually a bijection. Show that $f \circ g$ is the same map that is described in the statement of Theorem 2.

Remark. A simple proof by induction using the ideas of the above proof extends the Chinese Remainder Theorem to any number of factors.

4. Finding the Inverse Map

We know that the functions described in Theorem 1 and Theorem 2 are bijections. Thus they have inverses. What is the inverse map?

Let us concentrate on trying to find the inverse in the case of the map into the triple Cartesian product: $\mathbb{Z}_{abc} \to \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$. The inverse for the double Cartesian product or the n-fold Cartesian product for $n \neq 3$ is similar.

Begin by defining e_1 to be an integer of the form kbc where k is chosen so that $e_1 \equiv 1 \mod a$. Such a k exists since $\gcd(bc, a) = 1$ (see Lemma 4), hence bc has an inverse k modulo a. For example, if $a = 7$, $b = 8$ and $c = 9$ then we look for $e_1 = k72$. However, $72 \equiv 2 \mod 7$. Thus we would choose $k = 4$ since 4 is the inverse of 2 modulo 7. So we want $e_1 = 288$.

Next define e_2 to be an integer of the form kac where k is chosen so that $e_2 \equiv 1 \mod b$. For example, if $a = 7$, $b = 8$ and $c = 9$ then we look for $e_2 = k63$. However, $63 \equiv -1 \mod 8$. Thus we would choose $k = -1$ since -1 is the inverse of -1 modulo 8. So we want $e_2 = -63$.

Finally define e_3 to be an integer of the form kbc where k is chosen so that $e_3 \equiv 1 \mod c$. For example, if $a = 7$, $b = 8$ and $c = 9$ then we look for $e_3 = k56$. However, $56 \equiv 2 \mod 9$. Thus we could choose $k = -4$ since -4 is the inverse of 2 modulo 9. So we want $e_3 = -224$ (but $e_3 = 280$ also works). Observe that, for this example, $e_1 + e_2 + e_3 = 1$ (see the Remark following the next theorem).

Observe that

$$[e_1]_{abc} \mapsto \big([1]_a, [0]_b, [0]_c\big)$$
$$[e_2]_{abc} \mapsto \big([0]_a, [1]_b, [0]_c\big)$$
$$[e_3]_{abc} \mapsto \big([0]_a, [0]_b, [1]_c\big)$$

This explains why we use the symbols e_1, e_2, e_3. We are inspired by linear algebra where these symbols are often used to indicate the standard basis.

Theorem 6. *Let $f : \mathbb{Z}_{abc} \to \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$ be the map described in Theorem 2. Then inverse is given by the formula*

$$f^{-1}\big([x]_a, [y]_b, [z]_c\big) = [xe_1 + ye_2 + ze_3]_{abc}$$

where e_1, e_2, e_3 are as described above.

Proof. Fix $\big([x]_a, [y]_b, [z]_c\big) \in \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$. Observe that

$$xe_1 + ye_2 + ze_3 \equiv x \cdot 1 + y \cdot 0 + z \cdot 0 \equiv x \mod a$$
$$xe_1 + ye_2 + ze_3 \equiv x \cdot 0 + y \cdot 1 + z \cdot 0 \equiv y \mod b$$

$$xe_1 + ye_2 + ze_3 \equiv x \cdot 0 + y \cdot 0 + z \cdot 1 \equiv z \mod c.$$

Thus

$$f\big([xe_1 + ye_2 + ze_3]_{abc}\big) = \big([x]_a, [y]_b, [z]_c\big)$$

Now apply f^{-1} to both sides of the above equation. □

Remark. There is a short cut for finding e_1, e_2, e_3. Since $[e_1 + e_2 + e_3]$ and $[1]$ both map to $\big([1], [1], [1]\big)$ we have that they are equal (injectivity). So

$$e_1 + e_2 + e_3 \equiv 1 \mod abc.$$

This means that we can choose e_3 to be $1 - e_1 - e_2$. In other words, if we know two of the three, the third can be obtained by subtracting the others from 1.

Exercise 7. Choose a, b, c pairwise relatively prime, and determine the inverse map for your choice of a, b, c.

Exercise 8. Describe the procedure for finding the inverse in the case of Theorem 1. Give an example (such as $m = 4$ and $n = 3$).

Exercise 9. Describe the procedure for finding the inverse in the case

$$\mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \mathbb{Z}_{m_4}$$

where $m = m_1 m_2 m_3 m_4$ and where m_1, m_2, m_3, m_4 are pairwise relatively prime.

5. Units

Proposition 7. *Suppose that $d \mid m$ where m is a positive integer. If $[x]_m$ is a unit in $\mathbb{Z}_m$, then its image $[x]_d$ is a unit in $\mathbb{Z}_d$.*

Proof. If $[x]_m$ is a unit in $\mathbb{Z}_m$ then x and m have greatest common divisor 1. Since the common divisors of x and d form a subset of the common divisors of x and m, we have that 1 is the greatest common divisor of x and d. Thus $[x]_d$ is a unit. □

Another Proof. Suppose that $[x]_m$ has inverse $[y]_m$. Then $xy \equiv 1 \bmod m$. Thus m divides $xy - 1$. This means d divides $xy - 1$. Hence $xy \equiv 1 \bmod d$. So $[x]_d$ has inverse $[y]_d$. □

Exercise 10. Make a list of units in $\mathbb{Z}_{20}$ and verify that they all map to units in $\mathbb{Z}_4$. Show that there is a non-unit of $\mathbb{Z}_{20}$ that maps to a unit in $\mathbb{Z}_4$.

Corollary 8. *Let m and n be relatively prime positive integers. Then the map*

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

defined by the rule $[x]_{mn} \mapsto \big([x]_m, [x]_n\big)$ sends units to ordered pairs of units. In other words, it restricts to a map

$$\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times.$$

Theorem 9. *Let m and n be relatively prime positive integers. Then the map*

$$\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times.$$

defined by the rule $[x]_{mn} \mapsto \big([x]_m, [x]_n\big)$ is a bijection.

Proof. The associated function $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ on the larger domain is injective, so the restriction $\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ is injective. We just need to show it is surjective.

To show it is bijective, let $\big([s]_m, [t]_n\big) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ be an arbitrary element of the codomain. We must find an element of the domain that maps to it. By the Chinese Remainder Theorem there is an element $[x]_{mn} \in \mathbb{Z}_{mn}$ that maps to it under the function describe in Theorem 1, but is it a unit? If so then we would have that $\big([s]_m, [t]_n\big)$ is in the image of $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$.

Since $[x]_{mn} \mapsto \big([x]_m, [x]_n\big)$ we have $\big([x]_m, [x]_n\big) = \big([s]_m, [t]_n\big)$. Comparing first coordinates, we get $[x]_m = [s]_m$, which means that $[x]_m$ is a unit in $\mathbb{Z}_m$. Thus $\gcd(x, m) = 1$. Likewise, $\gcd(x, n) = 1$ (by comparing second coordinates). By Lemma 4 we have $\gcd(x, mn) = 1$. Thus $[x]_{mn}$ is in fact a unit. This shows that our function is surjective. □

Remark. (For readers with abstract algebra experience). The function described in the above theorem is an isomorphism between groups.

6. Euler's phi function and units

An element $\overline{a} \in \mathbb{Z}_m$ is a unit if and only if a and m are relatively prime. Thus the size of $\mathbb{Z}_m^\times$ is equal to the number of elements in $\{1, \ldots, m\}$ that are relatively prime to m. This number, called $\phi(m)$, arises in many places in number theory.

Definition 1. Let $m \geq 1$ be an integer. Then $\phi(m)$ is defined to be the number of integers in $\{1, \ldots, m\}$ that are relatively prime to m. The function $m \mapsto \phi(m)$ is called *Euler's phi function* or the *totient function*.

Example. The integers less than or equal to 12 that are relatively prime to 12 are $1, 5, 7, 11$. Thus $\phi(12) = 4$.

Thus we have the following:

Theorem 10. *Let $m \geq 1$ be an integer. Then $\mathbb{Z}_m$ has $\phi(m)$ units. Thus $\mathbb{Z}_m^\times$ is a group with $\phi(m)$ elements.*

Combining this with Theorem 9 yields the following:

Theorem 11. *Suppose that m and n are relatively prime positive integers. Then*

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

Proof. This follows from Theorem 9 together with the fact that the cardinality of $A \times B$ is ab where a is the cardinality of A and b is the cardinality of B. □

Corollary 12. *If $m_1, \ldots, m_r$ are pairwise relatively prime positive integers, then*

$$\phi(m_1 \cdots m_r) = \phi(m_1) \cdots \phi(m_r).$$

Proof. This follows from iterating the previous result. To prove this formally, use induction on r. □

7. Other formulas for ϕ

Let p be a prime. It is easy to see that $\phi(p) = p - 1$ since every positive integer less than p is relatively prime to p. This generalizes from p^1 to p^k as follows.

Proposition 13. *Let k be a positive integer. If p is a prime, then*

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Proof. Clearly $\gcd(a, p^k) > 1$ if and only if a is a multiple of p since all common divisors of a and p^k must be powers of p. The multiples of p less than or equal to p^k are $p, 2p, 3p, \ldots, p^{k-1}p$. Observe that there are p^{k-1} such multiples. If we remove them from $1, 2, 3, \ldots, p^k$, we are left with $p^k - p^{k-1}$ integers. □

Remark. Once we have a prime power factorization of m, we can use the proceeding corollary and proposition to compute $\phi(m)$ as follows:

Proposition 14. *If $m > 1$ is an integer, and $m = p_1^{e_1} \cdots p_r^{e_r}$ where each p_i is a prime and each e_i is positive, then*

$$\phi(m) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})$$

Example. Since $150 = 2^1 \cdot 3^1 \cdot 5^2$, we have $\phi(150) = (2-1)(3-1)(25-5) = 40$. So $\mathbb{Z}_{150}^\times$ is a group with 40 elements.

Here is another version of the above formula:

Corollary 15. *If $m > 1$ is an integer then*

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

where the product is over all primes p dividing m.

Proof. Write $m = \prod p^{e_p}$ where $e_p = \mathrm{ord}_p(m)$. From the above proposition:

$$\phi(m) = \prod (p_1^{e_p} - p_1^{e_p-1}) = \prod p^{e_p} \left(1 - p^{-1}\right) = \prod p^{e_p} \cdot \prod \left(1 - p^{-1}\right) = m \prod \left(1 - p^{-1}\right).$$

□

Exercise 11. Calculate $\phi(m)$ for $m = 10, 15, 17, 21, 125, 250, 500, 1000$.

Remark. Let $m > 1$ be an integer. Then all primes p, except for those dividing m, are relatively prime to m. So there are $\phi(m)$ cases for such primes. Dirichlet revolutionized number theory in 1837 by proving that there are an infinite number of primes in each of these $\phi(m)$ equivalence classes, and that statistically they are evenly distributed between the classes.

For example ($m = 4$), all primes except 2 are of the form $4n+1$ or $4n+3$. In other words, they are in the classes $\overline{1}$ or $\overline{3}$ in $\mathbb{Z}_4$. Can you give examples of primes in each of these classes? Dirichlet proved that, in the limit, half the primes are of the form $4n+1$ and half are of the form $4n+3$. The number one half is just $1/\phi(4)$ since $\phi(4) = 2$.

Another example ($m = 10$). Observe that $\phi(10) = 4$, and that the units in $\mathbb{Z}_{10}$ are $\overline{1}, \overline{3}, \overline{7}, \overline{9}$. Every prime number, except 2 and 5, is in one of these equivalence classes. In other words, every such prime has final digit $1, 3, 7, 9$. Can you find a couple examples of each type? Dirichlet's theorem states that there are an infinite number of primes in each of these four equivalence classes, and that the density of primes in each class is $1/4$. This means, in the limit, one fourth of the primes have final digit 7, say, and one fourth have final digit 9.

What is even more surprising about this result is the method used to prove it. Dirichlet used analysis and functions defined by infinite products and series. This is the beginning

of *analytic* number theory. In particular, he studied the zeta function $\zeta(s)$ and related functions. The famous *Riemann conjecture* concerns this zeta function. Analytic number theory is a facinating subject since it uses the resources of $\mathbb{R}$ and $\mathbb{C}$ to study the subset $\mathbb{Z}$.

Prof. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA
E-mail address: waitken@csusm.edu