Lecture 12: The Chinese remainder theorem

In this lecture, we shall prove a theorem that comes from Ancient Chinese mathematics rather than Ancient Greek. We shall, however, prove it in modern dress.

Let M_1 and M_2 be two monoids with binary operations $\circ_1$ and $\circ_2$, respectively and identities e_1 and e_2, respectively. Then the set of ordered pairs $M_1 \times M_2$ can be made into a monoid as follows. We define a binary operation $\circ$ by putting

$$(a_1, a_2) \circ (b_1, b_2) = (a_1 \circ_1 b_1, a_2 \circ_2 b_2).$$

This is clearly a binary operation on the set $M_1 \times M_2$ and it is left as an exercise to prove that it is associative and that (e_1, e_2) is the identity. We call this monoid the *direct product* of the monoids M_1 and M_2. It is a technique that enables us to make new monoids from old.

What we have done for two monoids we can do for any finite number of monoids. Let $M_1, \ldots, M_k$ be k monoids with multiplication in every case denoted by concatenation to keep the notation simple. The identity of M_i is denoted by e_i. Then $M = M_1 \times \ldots \times M_k$ is a monoid when we define

$$(a_1, \ldots, a_i, \ldots, a_k)(b_1, \ldots, b_i, \ldots, b_k) = (a_1 b_1, \ldots, a_i b_i, \ldots, a_k b_k);$$

observe that the multiplication is defined *componentwise*. The identity is $(e_1, \ldots, e_i, \ldots, e_k)$.

We shall need to work out the group of units of M in terms of the groups of units of the monoids M_i. The following result delivers the goods.

Lemma 0.1. *If $M = M_1 \times \ldots \times M_k$ as above, then $U(M) = U(M_1) \times \ldots \times U(M_k)$.*

Proof. Observe that $(a_1, \ldots, a_i, \ldots a_k)$ is invertible if and only if there is an element $(b_1, \ldots, b_i, \ldots b_k)$ such that

$$(a_1, \ldots, a_i, \ldots a_k)(b_1, \ldots, b_i, \ldots b_k) = (e_1, \ldots, e_i, \ldots, e_k).$$

This holds if and only if $a_i b_i = e_i = b_i a_i$ for each i which means it holds if and only if each a_i is invertible in M_i. □

The proof of the following is now imemdiate.

Corollary 0.2. *If the monoids M_i are finite then, with the notation above,*

$$|U(M)| = |U(M_1)| \ldots |U(M_k)|.$$

We shall now work in the multiplicative monoid $\mathbb{Z}_n$.

Theorem 0.3 (Chinese Remainder Theorem)**.** *Let* $n = n_1 \dots n_k$ *where* $\gcd(n_i, n_j) = 1$ *when* $i \neq j$*. Then the function*

$$\theta\colon \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$$

defined by

$$\theta([a]) = ([a_1], \dots, [a_k])$$

where $a_i \equiv a \pmod{n_i}$ *is an isomorphism of monoids.*

Proof. It is easy to see that $\theta(ab) = \theta(a)\theta(b)$. It remains to show that θ is bijective. We show first that it is surjective. Let $(a_1, \dots, a_k)$ be an element of $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$. We need to find $x \in \mathbb{Z}_n$ such that $\theta(x) = (a_1, \dots, a_k)$. This is equivalent to solving the following system of equations

$$x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_k \pmod{n_k}.$$

The solution is by means of explicit construction.

For each i put $c_i = \frac{n}{n_i}$. By its very definition

$$\gcd(c_i, n_i) = 1.$$

This implies that $[c_i]$ is an invertible element in $\mathbb{Z}_{n_i}$. Let the inverse be $[d_i]$. Thus $[c_i][d_i] = [1]$. Define

$$x_0 = \sum_{i=1}^{k} a_i c_i d_i.$$

Let's examine this element modulo n_i. For $j \neq i$ we have that $n_i \mid n_j$. Thus all other terms are zero except for $a_i c_i d_i$. But modulo n_i we have that $c_i d_i \equiv 1$. It follows that x_0 modulo n_i is equal to a_i.

We have therefore shown that θ is surjective.

To show that it is injective suppose that x_0 and x_1 are both solutions. Then $x_0 - x_1$ are divisible by $n_1, \dots, n_k$ in turn which are pairwise coprime. It follows that $x_0 - x_1$ is divisible by n, as required. □

The following is an important deduction.

Corollary 0.4. *Let* $n = p_1^{e_1} \dots p_k^{e_k}$ *be the prime factorization of* n*. Then the group* $\mathbb{U}_n$ *is isomorphic to the direct product group*

$$\mathbb{U}_{p_1^{e_1}} \times \dots \times \mathbb{U}_{p_k^{e_k}}.$$

We now observe that if two monoids are isomorphic then there groups of units will be isomorphic. This gives us a nice conceptual proof of the fact that the Euler ϕ-function is multiplicative.

Corollary 0.5. *Let* $\gcd(a, b) = 1$*. Then* $\phi(ab) = \phi(a)\phi(b)$*.*

We finish off with an example. Let

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

We need to find a number modulo $105 = 3 \times 5 \times 7$ that satisfies all of the equations. We calculate the numbers $35 = \frac{105}{3}, 21 = \frac{105}{5}, 15 = \frac{105}{7}$. We now calculate

$$35^{-1} \equiv 2 \pmod 3, \quad 21^{-1} \equiv 1 \pmod 5, \quad 15^{-1} \equiv 1 \pmod 7.$$

Put

$$x_0 = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233$$

which is congruent to 23 modulo 105. You can now check that 23 satisfies all three equations.