11th Lecture: 15/2

Theorem 11.1. (Chinese Remainder Theorem) *Let $n \in \mathbb{Z}_+$ with unique prime factorisation $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Then there is an isomphism of rings*

$$\mathbb{Z}_n \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}. \tag{11.1}$$

PROOF: There is a natural map

$$\phi : \mathbb{Z}_n \to \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$$
$$a \pmod{n} \mapsto (a \pmod{p_1^{\alpha_1}}, \dots, a \pmod{p_k^{\alpha_k}}).$$

Moreover, it is clear that ϕ is a ring homomorphism, i.e.: that it respects the operations of addition and multiplication in the respective rings. It thus remains to show that ϕ is a bijection.

Injectivity: Suppose $\phi(a \pmod{n}) = \phi(b \pmod{n})$. Now two elements of a direct product of rings are equal if and only if they are equal in every component. Hence $a \pmod{p_i^{\alpha_i}} = b \pmod{p_i^{\alpha_i}}$, for each $i = 1, \dots, k$. In other words, $a - b$ is divisible by $p_i^{\alpha_i}$ for each i. But then, by FTA, $a - b$ must be divisible by $\prod_{i=1}^{k} p_i^{\alpha}$, that is, $a - b$ is divisible by n and so $a \pmod{n} = b \pmod{n}$, v.s.v.

Surjectivity: We need to show that, for arbitrary integers $a_1, a_2, \dots, a_k$ there exists an integer x satisfying the system of congruences

$$x \equiv a_i \pmod{p_i^{\alpha_i}}, \quad i = 1, \dots, k.$$

More generally, we will show that, for arbitrary $a_1, \dots, a_k$ and arbitrary $n_1, \dots, n_k$ satisfying[1] $\mathrm{GCD}(n_i, n_j) = 1 \; \forall \, i \neq j$, there exists an integer x satisfying the system of congruences

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \dots, k. \tag{11.2}$$

Indeed, x can be given by an explicit formula, namely

$$x \equiv \sum_{i=1}^{k} a_i b_i N_i \pmod{N}, \tag{11.3}$$

where

$$N = \prod_{i=1}^{k} n_i, \quad N_i = \frac{N}{n_i} = \prod_{j \neq i} n_j, \quad b_i \equiv N_i^{-1} \pmod{n_i}. \tag{11.4}$$

To see that this formula is correct

- First note that, since the n_i are pairwise relatively prime, one also has $\mathrm{GCD}(N_i, n_i) = 1$ for each i and hence the numbers b_i are well-defined, by Proposition 10.11.

- Now substitute these into (11.3). For fixed i, each of the N_j, $j \neq i$, will contain n_i as a factor and hence be divisible by n_i. Hence each of the terms $a_j b_j N_j$, for $j \neq i$, will contribute zero modulo n_i. This leaves us with $x \equiv a_i b_i N_i \equiv a_i (N_i^{-1} N_i) \equiv a_i \pmod{n_i}$, v.s.v.

[1] The numbers n_i are said to be *pairwise relatively prime.*

Remark 11.2. The "hard part" of the above proof is surjectivity. For this reason, the term "Chinese Remainder Theorem" sometimes just refers to the statement that a system of congruences (11.2) has a unique solution modulo $\prod_i n_i$ given by (11.3).

Example 11.3. I did an example in class, but I'll be doing another one in Demo4, so look there instead.

Remark 11.4. If the n_i are not pairwise relatively prime, then the system (11.2) may or may not have a solution, depending on the values of the a_i. For example, take $n_1 = 4$, $n_2 = 6$. Then GCD$(n_1, n_2) = 2$, so any x satisfying (11.2) must in particular satisfy $x \equiv a_1 \equiv a_2 \pmod 2$. In other words, a necessary condition for a solution to exist is that $a_1 \equiv a_2 \pmod 2$. One can check (it follows from Theorem 11.1) that this condition is also sufficient. Similar remarks apply to arbitrary systems (11.2), but we hop over the technical details.

Corollary 11.5. *Let $n \in \mathbb{Z}_+$ with unique prime factorisation $n = \prod_{i=1}^k p_i^{\alpha_i}$. Then there is an isomphism of groups*

$$\mathbb{Z}_n^\times \cong \prod_{i=1}^k \mathbb{Z}_{p_i^{\alpha_i}}^\times . \tag{11.5}$$

PROOF: Follows immediately from Theorem 11.1 and eq. (10.1).

Definition 11.6. The *Euler-phi function* is the function $\phi : \mathbb{Z}_+ \to \mathbb{Z}_+$ given by

$$\phi(n) = |\mathbb{Z}_n^\times| = |\{a \in \mathbb{Z} : 0 \le a < n \text{ and } \mathrm{GCD}(a,\, n) = 1\}|.$$

Note that, for a prime power p^α one has GCD$(a,\, p^\alpha) > 1$ if and only if a is a multiple of p. Hence

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right). \tag{11.6}$$

From this and (11.5) it follows that for arbitrary $n \in \mathbb{Z}_+$,

$$\phi(n) = |\mathbb{Z}_n^\times| = \left| \prod_{i=1}^k \mathbb{Z}_{p_i^{\alpha_i}}^\times \right| = \prod_{i=1}^k |\mathbb{Z}_{p_i^{\alpha_i}}^\times|$$

$$= \prod_{i=1}^k \phi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \left[\prod_{i=1}^k p_i^{\alpha_i}\right] \left[\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)\right] = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

In other words,

$$\frac{\phi(n)}{n} = \prod_{p \,|\, n} \left(1 - \frac{1}{p}\right), \tag{11.7}$$

where the product is taken over the *distinct* primes which divide n.

In particular, this means one can easily compute $\phi(n)$ if one knows the factorisation of n. I believe it is still an open problem whether the converse is true in general[2]. See Homework 2, Exercise 7 for the case of $n = p_1 p_2$, a product of two distinct primes.

Theorem 11.7. (Euler's Theorem) *Let n be a positive integer and a any integer satisfying GCD$(a, n) = 1$. Then*

$$a^{\phi(n)} \equiv 1 \ (mod \ n). \tag{11.8}$$

PROOF: Follows immediately from Corollary 9.15 applied to the group $G = \mathbb{Z}_n^\times$.

Computing a^b (mod c). This is the core computation performed, for example, in the implementation of RSA cryptography (see Lecture 12). The positive integers a, b, c should be thought of as being *very large*, so large that the "stupid" way of doing the computation - first computing the integer a^b explicitly and then dividing by c and computing the remainder - is unfeasible. There are two basic options for a feasible computation:

Method 1: Use Euler's Theorem. The drawback with this is that it first requires one to compute $\phi(c)$ which, unless you're lucky, in turn requires you to factorise c. A second problem is that Euler's Theorem assumes that GCD$(a, c) = 1$ though, as we will show, one can get around this. Factorisation of c is thus the main sticking point in general, but if one somehow knows $\phi(c)$, this is the most efficient way of performing the computation.

Method 2: Repeated Squaring Algorithm. This is state-of-the-art for a method which *always* works. The main point about it is that it allows one to obtain the correct answer without ever having to work with numbers that are bigger than c^2.

I began (but did not finish) an example in class, but since I'll be doing one in Demo4 anyway, you can look there for a worked example. Note in particular how one gets around the situation where GCD$(a, c) > 1$.

Remark 11.8. One can use (11.5) to obtain the exact algebraic structure of the abelian group $\mathbb{Z}_n^\times$ as a direct sum of finite cyclic groups of prime power size, assuming one first can factorise n. To do so requires three additional facts, whose proofs I will skip over due to time constraints.

Fact 11.9. *Let p be an odd prime and n a positive integer. Then the group $\mathbb{Z}_{p^n}^\times$ is cyclic.*

Fact 11.10. $\mathbb{Z}_2^\times \cong C_1$, $\mathbb{Z}_4^\times \cong C_2$ *and, for* $n \geq 3$, $\mathbb{Z}_{2^n}^\times \cong C_2 \oplus C_{2^{n-2}}$.

Fact 11.11. *Let m, n be positive integers. Then $C_m \oplus C_n \cong C_{mn}$ if and only if GCD$(m, n) = 1$.*

[2] To state the converse problem precisely, one must define precisely what "easily" means. The usual definition is "in polynomial time", but I will leave it to you to find out what that means if you are interested.

Example 11.12. We determine the structure of $\mathbb{Z}_{624}^{\times}$. First we factorise:

$$624 = 2^4 \cdot 3 \cdot 13.$$

Hence, by (11.5),

$$\mathbb{Z}_{624}^{\times} \cong \mathbb{Z}_{16}^{\times} \times \mathbb{Z}_{3}^{\times} \times \mathbb{Z}_{13}^{\times}. \tag{11.9}$$

- Fact 11.10 implies that $\mathbb{Z}_3^{\times} \cong C_2$ and $\mathbb{Z}_{13}^{\times} \cong C_{12}$.
- Fact 11.11 implies that $\mathbb{Z}_{16}^{\times} \cong C_2 \oplus C_4$.
- Fact 11.12 implies in turn that $C_{12} \cong C_3 \oplus C_4$.

Substituting everything into (11.9) gives

$$\mathbb{Z}_{624}^{\times} \cong (C_2 \oplus C_4) \oplus C_2 \oplus (C_3 \oplus C_4) \cong (C_2 \oplus C_2) \oplus C_3 \oplus (C_4 \oplus C_4).$$

One can think of the RHS as being the "prime factorisation" of the abelian group $\mathbb{Z}_{624}^{\times}$. More generally, every finite abelian group has a "unique prime factorisation" in some sense - the theorem which makes this precise is called the *Fundamental Theorem of Finite Abelian Groups*. Look it up if you're interested !

Remark 11.13. By Fact 11.10, for each prime p the multiplicative group $\mathbb{Z}_p^{\times}$ of non-zero elements in the finite field $\mathbb{Z}_p$ is cyclic. A generator of this group is called a *primitive root modulo* p. Thus, $a \in \mathbb{Z}$ is a primitive root modulo p if and only if $a^k \not\equiv 1 \pmod{p}$ for any $1 \leq k < p-1$.

Note that, by Proposition 10.9, in a cyclic group of size t there are $\phi(t)$ generators. Hence, there are $\phi(p-1)$ primitive roots modulo p. Typically, this is quite a large fraction of the $p-1$ group elements (see (11.7)). However, when p is large, to actually *find* a primitive root, by anything other than an exhaustive search, is a non-trivial problem. See Homework 2, Exercise 5(f) for a worked example when p is small.

Indeed, some easy-to-state questions concerning primitive roots seem to have very deep "roots" (excuse the pun !). We mention the most famous problem:

Artin's Conjecture. *Let a be an integer which is not a perfect square. Then there are infinitely many primes p such that a is a primitive root modulo p.*

Note that the condition that a not be a perfect square is necessary. This is because, for any odd p, the group $\mathbb{Z}_p^{\times}$ has even size $p-1$. Hence, if $a = b^2$ then $a^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}$.

There is no single integer a for which Artin's Conjecture has been proven. It is, however, known that Artin's Conjecture would follow from a certain version of the *Generalized Riemann Hypothesis*. The Riemann Hypothesis, even in its classical formulation (which is not enough for Artin's Conjecture) for the zeta function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$, is probably the most significant open problem in all of mathematics.