Week 9 Summary

Lecture 17

Let n_1, n_2, ... , n_k be positive integers. The *direct sum* of $\mathbb{Z}_{n_1}$, $\mathbb{Z}_{n_2}$ ... , $\mathbb{Z}_{n_k}$ is defined to be the set of all k-tuples $(a_1, a_2, \ldots, a_k)$ such that $a_i \in \mathbb{Z}_{n_i}$ for each i. We use "$\oplus$" to denote direct sum. Thus,

$$\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 = \{\, (a, b, c) \mid a \in \mathbb{Z}_3,\ b \in \mathbb{Z}_5,\ c \in \mathbb{Z}_7 \,\}.$$

We can define addition and multiplication for k-tuples componentwise. Thus in $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$ we have

$$(2, 4, 3) + (2, 3, 6) = (4, 7, 9) = (1, 2, 2)$$

and

$$(2, 4, 3)(2, 3, 6) = (4, 12, 18) = (1, 2, 4).$$

Since 3, 5 and 7 are divisors of 105 there are homomorphisms from $\mathbb{Z}_{105}$ to $\mathbb{Z}_3$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$, as explained in Lecture 16. If we call these f, g and h (respectively) then we can combine them into a homomorphism from $\mathbb{Z}_{105}$ to $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$ given by the rule

$$a \mapsto (f(a), g(a), h(a))$$

for all $a \in \mathbb{Z}_{105}$. Thus, for example,

$$56 \mapsto (56, 56, 56) = (2, 1, 0)$$

(since $56 = 2$ in $\mathbb{Z}_3$, and so on). The Chinese Remainder Theorem tells us that this mapping is a one to one correspondence between between $\mathbb{Z}_{105}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$, since for each triples (a, b, c) in $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$ there is a unique $x \in \mathbb{Z}_{105}$ such that $x \equiv a \pmod 3$, $x \equiv b \pmod 5$ and $x \equiv c \pmod 7$. We can, for example, find the element of $\mathbb{Z}_{105}$ that maps to $(1, 4, 3)$ by solving the simultaneous congruences $x \equiv 1 \pmod 3$, $x \equiv 4 \pmod 5$ and $x \equiv 3 \pmod 7$ using the method given in Lecture 15. The solution is 94.

A homomorphism that is a one to one correspondence is called an *isomorphism.* The Chinese Remainder Theorem can be restated as follows: if m_1, m_2, ... , m_k are pairwise coprime then there is an isomorphism

$$\mathbb{Z}_{m_1 m_2 \cdots m_k} \longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k}$$

given by $a \mapsto (a_1, a_2, \ldots, a_k)$ (for all a), where $a \equiv a_i \pmod{m_i}$ for each i.
We say that $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ and $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ are *isomorphic.*

In the Chinese Remainder Theorem isomorphism, the element of the direct sum $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ corresponding to $1 \in \mathbb{Z}_{m_1 m_2 \cdots m_k}$ is the k-tuple $(1, 1, \ldots, 1)$. So if $a \in \mathbb{Z}_{m_1 m_2 \cdots m_k}$ corresponds to $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ then

a has an inverse in $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ if and only if a_i has an inverse in $\mathbb{Z}_{m_i}$ for each i. This yields the following Proposition.

***Proposition:** If m_1, m_2, $\ldots m_k$ are pairwise coprime positive integers then $\varphi(m_1 m_2 \cdots m_k) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)$.

The proof consists of recalling that the number of invertible elements of $\mathbb{Z}_m$ is $\varphi(m)$, and hence the number of k-tuples $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ such that each a_i is invertible is $\varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)$.

***Proposition:** If p is prime and $n \in \mathbb{Z}^+$ then $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$.

***Proposition:** If m is a positive integer then

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\cdots(1 - \frac{1}{p_k})$$

where p_1, p_2, $\ldots$, p_k are the distinct prime divisors of m.

For example, $\varphi(700) = 700(1 - (1/2))(1 - (1/5))(1 - (1/7)) = \frac{700\times4\times6}{2\times5\times7} = 240$.

Lecture 18

Example: Solve, in $\mathbb{Z}_{105}$, the equation $x^3 = 41$.

By the Chinese Remainder Theorem, each $x \in \mathbb{Z}_{105}$ corresponds to a triple (x_1, x_2, x_3) in $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$. Consequently the problem can be restated as follows: solve $(x_1^3, x_2^3, x_3^3) = (41, 41, 41) = (2, 1, 6)$ in $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$. Now the cubes of the elements 0, 1 and 2 in $\mathbb{Z}_3$ are (respectively) 0, 1 and $8 = 2$; so $x_1^3 = 2$ gives $x_1 = 2$. In $\mathbb{Z}_5$ the cubes of 0, 1, 2, $3 = -2$ and $4 = -1$ are 0, 1, $8 = 3$, $-8 = 2$ and $-1 = 4$. So $x_2^3 = 1$ gives $x_2 = 1$. In $\mathbb{Z}_7$ the cubes of 0, 1, 2, 3, -3, -2 and -1 are 0, 1, $8 = 1$, $27 = -1$, $-27 = 1$, $-8 = -1$ and -1. So $x_3^3 = 6 = -1$ gives $x_3 = 3$, 5 or 6. So there are three solutions:

$$(x_1, x_2, x_3) = (2, 1, 3),\ (2, 1, 5) \text{ or } (2, 1, 6).$$

The corresponding elements of $\mathbb{Z}_{105}$ are found by using the same method as used in the example given in Lecture 16. For example, the element $x \in \mathbb{Z}_{105}$ such that $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 5$ and $x \equiv 5 \pmod 7$ is 26. The other two solutions of $x^3 = 41$ are 94 (corresponding to (2,1,3)) and 41 (corresponding to (2,1,6)).

Let $f(x) = x^k + a_1 x^{k-1} + \cdots + a_{k-1}x + a_k$ be a polynomial over $\mathbb{Z}_p$, where p is some fixed prime number. That is, the coefficients a_i are integers modulo p, and we shall cosider values of x in $\mathbb{Z}_p$. If $t \in \mathbb{Z}_p$ then by division of polynomials one can find a polynomial $q(x)$ over $\mathbb{Z}_p$ and an element $r \in \mathbb{Z}_p$ with $f(x) = (x - t)q(x) + r$. Putting $x = t$ gives $r = f(t)$: this result is known as the *Remainder Theorem*. It follows that $x - t$ is a factor of $f(x)$ if and only if $f(t) = 0$ (since clearly $x - t$ is a factor of $f(x)$ if and only if the remainder r is zero). It follows that a polynomial equation of degree k over $\mathbb{Z}_p$ can have at most k roots. This is proved by induction on k. In the case $k = 1$ the equation has the form $ax + b = 0$ for some nonzero

$a \in \mathbb{Z}_p$, and the unique solution is $x = -ba^{-1}$. (Note that the argument fails at this point if p is not prime: for example $2x = 4$ has two solutions in $\mathbb{Z}_6$.) Now assuming that a polynomial equation of degree $k-1$ has at most $k-1$ solutions, and let $f(x) = 0$ be an equation of degree k and that $x = t$ is one solution. Then $f(x) = (x-t)g(x)$ where $g(x)$ has degree $k-1$, and if $u \neq t$ is another solution of $f(x) = 0$ then u must be a solution of $g(x) = 0$. (Note that this step also fails when p is not prime.) Since $g(x) = 0$ has at most $k-1$ solutions, $f(x) = 0$ has at most k solutions.

***Proposition:** In $\mathbb{Z}_p$, where p is prime, $x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$.

Note that looking at the constant term is this we recover Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$ when p is prime.

Our next objective is to establish the existence of primitive roots modulo p whenever p is prime. The first step is as follows.

***Proposition:** Let p be prime and q any prime divisor of $p-1$. Let $p-1 = q^n K$ where K is not divisible by q. Then there is some integer t whose order modulo p is q^n.

The proof goes as follows. By the Euler-Fermat Theorem, since $\varphi(p) = p-1$, for all integers t not divisible by p we have $(t^K)^{q^n} = t^{Kq^n} = t^{p-1} \equiv 1 \pmod{p}$. It follows that $\mathrm{ord}_p(t^K)$ is a divisor of q^n. Note that the divisors of q^n are precisely the powers q^i of q, from $i = 0$ to $i = n$. Apart from q^n itself these are all divisors of q^{n-1}. So if $\mathrm{ord}_p(t^K) \neq q^n$ then $(t^K)^{q^{n-1}} \equiv 1 \pmod{p}$. So if there is no t such that $\mathrm{ord}_p(t^K) = q^n$ then every nonzero $t \in \mathbb{Z}_p$ satisfies $t^{Kq^{n-1}} = 1$. But this means that every nonzero $t \in \mathbb{Z}_p$ is a root of the polynomial equation $x^k - 1 = 0$, where $k = Kq^{n-1}$. So this equation has $p-1$ roots. But its degree k is less than $p-1$, since $k = Kq^{n-1} < Kq^n = p-1$, and so it cannot have as many as $p-1$ roots. So for some t the order of t^K is q^n, and this proves the result.