Lecture 35, Nov. 14

35.1 Theorem (Linear Congruence Theorem)**.** *Let $n \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}$, let $d = gcd(a, n)$. Consider the equation*

$$ax = b \mod n$$

1. *The equation $ax = b \mod n$ has a solution $x \in \mathbb{Z}$ if and only if $d \mid b$*
2. *If $x = u$ is a solution (so that $au = b \mod n$), then the general solution is*

$$x = u + k\frac{n}{d} \text{ for } k \in \mathbb{Z}.$$

35.2 Theorem (Chinese Remainder Theorem)**.** *Let $n, m \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$. Then the pair of congruences*

$$x = a \mod n$$

$$x = b \mod m$$

has a solution $x \in \mathbb{Z}$ if and only if $d \mid (b - a)$ where $d = gcd(m, n)$, and if $x = u$ is one solution to the pair of congruences then the general solution is $x = u \mod l$ where $l = lcm(n, m)$.

Proof. Suppose the pair of congruences has a solution. Choose a solution $x \in \mathbb{Z}$ (so we have $x = a \mod n$ and $x = b \mod m$). Since $x = a \mod n$, we can choose s so that $x = a + ns$, and since $x = b \mod m$, we can choose t so that $x = b + mt$. Then $a + ns = b + mt$, so $ns - mt = b - a$. By the Linear Diophantine Equation Theorem, for $d = gcd(m, n)$, we have $d \mid (b - a)$.

Conversely, suppose that $d \mid (b - a)$. By the Linear Diophantine Equation Theorem we can choose $s, t \in \mathbb{Z}$ so that $ns - mt = b - a$. Then $a + ns = b + mt$. Let $x = a + ns$ (so $x = b + mt$). Then since $x = a + ns$ we have $x = a \mod n$. Since $x = b + mt$ we have $x = b \mod m$.

Suppose that $x = u$ is a solution to the pair of congruences. So we have $u = a \mod n$ and $u = b \mod m$. Let $k \in \mathbb{Z}$. Let $x = u + kl$ where $l = lcm(m, n)$. Since $l = lcm(m, n)$, choose $s, t \in \mathbb{Z}$ so that $l = ns = mt$. Since $x = u + kl = u + kns$, we have $x = u \mod n$ so $x = a \mod n$. Similarly we have $x = b \mod m$. Thus $x = u + kl$ is a solution to the pair of congruences.

Conversely, let x be any solution to the pair of congruences. So we have $x = a \mod n$ and $x = b \mod m$. Since $x = a \mod n$ and $u = a \mod n$, we have $x - u = 0 \mod n$, thus $n \mid x - u$. Since $x = b \mod m$ and $u = b \mod m$, we have $x = u = 0 \mod m$, so $m \mid x - u$. Since $n \mid (x - u)$ and $m \mid (x - u)$, it follows from the following lemma that $l \mid (x - u)$ since $l = lcm(m, n)$. Since $l \mid (x - u)$ we have $x = u \mod l$ as required. $\square$

35.3 Lemma. *Let $n, m \in \mathbb{Z}^+$ and let $l = lcm(m, n)$. For every $k \in \mathbb{Z}$, if $n \mid k$ and $m \mid k$ then $l \mid k$.*

Proof. Let $k \in \mathbb{Z}^+$ with $n \mid k$ and $m \mid k$. Write $k = \prod_{i=1}^{q} p_i^{m_i}$ where $q \in \mathbb{Z}^+$, the p_i are distinct primes and each $m_i \in \mathbb{Z}^+$. Since $n \mid k$, every prime factor p of n is also a factor of k, so we can write $n = \prod_{i=1}^{q} p_i^{j_i}$ with each $j_i \in \mathbb{N}$. Similarly, we can write $m = \prod_{i=1}^{q} p_i^{k_i}$ with each $k_i \in \mathbb{N}$.

Since $n \mid k$ we have $j_i \leq m_i$ for all indices i. Since $m \mid k$, we have $k_i \leq m_i$ for all indices i. Since $m_i \geq j_i$ and $m_i \geq k_i$, we have $m_i \geq max(j_i, k_i)$. Thus

$$\prod_{i=1}^{q} p_i^{max(j_i,k_i)} \mid \prod_{i=1}^{q} p_i^{m_i}$$

that is

$$lcm(m, n) \mid k$$

□

35.4 Theorem. *For*

$$n = \prod_{i=1}^{q} p_i^{k_i}$$

where $q \in \mathbb{Z}^+$, the p_i are distinct primes, and each $k_i \in \mathbb{Z}^+$, we have

$$\varphi(n) = \prod_{i=1}^{q} \varphi(p_i^{k_i}) = \prod_{i=1}^{q} p_i^{k_i} - p_i^{k_i - 1}$$

Proof. By induction, it suffices to show that for all $l, m \in \mathbb{Z}^+$ with $gcd(l, m) = 1$, we have $\varphi(lm) = \varphi(l)\varphi(m)$. We shall prove that $|U_{lm}| = |U_l \cdot U_m|$.

Define $F \colon \mathbb{Z}_{lm} \to \mathbb{Z}_l \times \mathbb{Z}_m$ by $F(x) = (x, x)$ for $x \in \mathbb{Z}$ (that is $F(x \mod lm) = (x \mod l, x \mod m)$). Note that F is well-defined, which means that for all $x, y \in \mathbb{Z}$ if $x = y \mod lm$ then $x = y \mod k$ and $x = y \mod m$ (if $x = y \mod lm$, say $x = y + tlm$ then $x = y + (tl)m$ so $x = ymodm$)
Note that F is bijective by the (RT indeed F is surjective (onto) because given $a, b \in \mathbb{Z}$ we can solve $x = a \mod l$ and $x = b \mod m$ and then $F(x) = (x \mod l, x \mod m) = (a, b)$ and F is injective by the Chinese Remainder Theorem.

Finally, it remains to show that F restricts to a bijective map

$$F \colon U_{lm} \to U_l \times U_m$$

that is for all $x \in \mathbb{Z}$, if $gcd(x, lm) = 1$ then $gcd(x, l) = 1$ and $gcd(x, m) = 1$, and if $gcd(x, l) = 1$ and $gcd(x, m) = 1$, then $gcd(x, lm) = 1$. □