Lecture 21

Enoch Cheung

November 11, 2013

1. **Lemma.** Let $m_1, m_2, \ldots, m_r \in \mathbb{N}$ be pairwise relatively prime. If $a \equiv b \pmod{m_i}$ for each $i \in [r]$ then $a \equiv b \pmod{m_1 m_2 \ldots m_r}$.

   Proof. We will induct on $r \in \mathbb{N}$.

   Base case: If $r = 1$, then $a \equiv b \pmod{m_1} \implies a \equiv b \pmod{m_1}$ so we are done.

   For convenience, we will prove it for $r = 2$ as well, because we will use it explicitly later. Consider $m_1, m_2 \in \mathbb{N}$ relatively prime, and $a \equiv b \pmod{m_i}$ for $i = 1, 2$, so $m_1|(b-a)$ and $m_2|(b-a)$.

   Suppose $m_1 m_2 \nmid (b-a)$, then $b - a = m_1 m_2 q + r$ for some $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ with $0 < r < m_1 m_2$. Then $r = (b-a) - m_1 m_2 q$, then since $m_1|(b-a)$, we have $m_1|r$. Similarly, $m_2|r$. This is a contradiction because $\gcd(m_1, m_2) = 1 \implies \operatorname{lcm}(m_1, m_2) = m_1 m_2$ (this uses the fact that $\gcd(m_1, m_2) \cdot \operatorname{lcm}(m_1, m_2) = m_1 \cdot m_2$), so r cannot be a common divisor of m_1, m_2. Therefore, $a \equiv b \pmod{m_1 m_2}$.

   Inductive case: Assume for some $r \in \mathbb{N}$, for any $m_1, \ldots, m_r \in \mathbb{N}$ pairwise relatively prime, $a \equiv b \pmod{m_i}$ for each $i \in [r]$ implies $a \equiv b \pmod{m_1 m_2 \cdots m_r}$.

   Now consider $m_1, \ldots, m_r, m_{r+1} \in \mathbb{N}$ pairwise relatively prime, then note that $m_1 \cdots m_r$ and m_{r+1} is relatively prime, because if they share a prime factor p, then by lemma proved in our last recitation $p|m_i$ for some $1 \le i \le r$ and $p|m_{r+1}$, which contradicts the fact that they are supposed to be pairwise relatively prime. By the inductive hypothesis, $a \equiv b \pmod{m_1 \cdots m_r}$ and $a \equiv b \pmod{m_{r+1}}$, so by the case for two relatively prime numbers, $a \equiv b \pmod{m_1 \cdots m_r m_{r+1}}$. $\square$

2. Let $\gcd(a, b) = d$ and suppose $d|c$. Further, let (x_0, y_0) be a solution to the diophantine equation $ax + by = c$.

   (a) $\forall k \in \mathbb{Z}$, $(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k)$ is also a solution.

   Note that the pair $(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k)$ is a pair of integers, due to our divisibility assumptions. Observe that

   $$a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = (ax_0 + by_0) + (\frac{ab}{d}k - \frac{ab}{d}k) = c$$

   (b) Suppose $(x, y) \in \mathbb{Z}$ is a solution to $ax + by = c$. Prove that $\exists k \in \mathbb{Z}$ such that $x = x_0 + \frac{b}{d}k$ and $y = y_0 - \frac{a}{d}k$ (i.e. every solution has this form).

   Since $ax + by = c$ and $ax_0 + by_0 = c$, and $\gcd(a, b) = d$,

   $$ax + by = ax_0 + by_0 \implies a(x - x_0) = b(y_0 - y) \implies \frac{d}{b}(x - x_0) = \frac{d}{a}(y_0 - y)$$

   so let $k = \frac{d}{b}(x - x_0) = \frac{d}{a}(y_0 - y) \in \mathbb{Q}$, then $x = x_0 + \frac{b}{d}k$ and $y = y_0 + \frac{b}{d}k$.

   Now we need to show that $k \in \mathbb{Z}$. In other words, we wish to show that $a|d(y_0 - y)$. Since $d = \gcd(a, b)$, by Tuesday's discussion, we can write $b = ed$ where e, a are relatively prime. Therefore, since $a(x - x_0) = b(y_0 - y)$,

   $$0 \equiv b(y_0 - y) \pmod{a} \implies 0 \equiv ed(y_0 - y) \pmod{a} \implies 0 \equiv d(y_0 - y) \pmod{a}$$

   since e is invertible mod a. Therefore, $k = \frac{d}{b}(x - x_0) = \frac{d}{a}(y_0 - y) \in \mathbb{Z}$ as desired.

3. Find all solution to

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{3} \end{aligned}$$

We wish to consider number of the form

$$\underbrace{5 \cdot 3 \cdot A}_{\text{vanishes mod 5 and mod 3}} + \underbrace{4 \cdot 3 \cdot B}_{\text{vanishes mod 4 and mod 3}} + \underbrace{4 \cdot 5 \cdot C}_{\text{vanishes mod 4 and mod 5}}$$

where $5 \cdot 3 \cdot A \equiv 3 \pmod 4$, $4 \cdot 3 \cdot B \equiv 1 \pmod 5$ and $4 \cdot 5 \cdot C \equiv 2 \pmod 3$. By multiplying with the corresponding inverses, we find $A \equiv 1 \pmod 4$, $B \equiv 3 \pmod 5$ and $C \equiv 1 \pmod 3$ to work.

By Chinese remainder theorem, the solution is unique modulo $4 \cdot 5 \cdot 3 = 60$. Therefore,

$$5 \cdot 3 \cdot 1 + 4 \cdot 3 \cdot 3 + 4 \cdot 5 \cdot 1 \equiv 15 + 36 + 20 \equiv 11 \pmod{60}$$

4. Show that if $\gcd(m_1, m_2) \nmid a_1 - a_2$ then there are no solutions to the system of linear congruences:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

Suppose there is such a solution x, then $m_1 | a_1 - x$ and $m_2 | a_2 - x$. Let $d = \gcd(m_1, m_2)$, then $d | m_1$ and $d | m_2$ so $d | a_1 - x$ and $d | a_2 - x$. Therefore, $d | (a_1 - x) - (a_2 - x)$ so $d | a_1 - a_2$. Thus, we have shown the contrapositive.