

§2.3 Chinese remainder theorem

Quiz: No definitions

Theorem 1 (2.18 The Chinese Remainder Theorem). *Let m_1, m_2, \dots, m_r denote r positive integers such that $(m_i, m_j) = 1 \forall i, j$. Then the congruences*

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\&\vdots \\x &\equiv a_r \pmod{m_r}\end{aligned}$$

have common solutions. If x_0 is one such solution, then x is also a solution $\Leftrightarrow x = x_0 + km_1m_2 \dots m_r$.

Proof: Let $m = m_1 \dots m_r$. Then $\frac{m}{m_i}$ is an integer, and $(\frac{m}{m_i}, m_j) = 1$. Now, $\forall j \exists b_j$ such that $\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$. Note that $\frac{m}{m_j} b_i \equiv 0 \pmod{m_i}$ if $i \neq j$. Now,

$$x_0 := \sum_{j=1}^r \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_j} b_j a_j \equiv a_j \pmod{m_j}.$$

Thus, x_0 is a solution. The last part follows from Theorem 2.3. ■

NOTE THE HYPOTHESIS THAT THE MODULI ARE RELATIVELY PRIME IN PAIRS!!

Examples:

1. Find the least positive integer such x such that $x \equiv 4 \pmod{5}$, $x \equiv 3 \pmod{7}$, and $x \equiv 2 \pmod{13}$.
2. Show that $x \equiv 7 \pmod{12}$ and $x \equiv 3 \pmod{24}$ are inconsistent.
3. In groups: Determine whether the systems $x \equiv j \pmod{8}$ (j varies per group), $x \equiv 7j \pmod{10}$ and $x \equiv 3j \pmod{14}$ have solutions, and find all the

solutions for those j where there are any.

Theorem 2. *If m_1 and m_2 denote 2 positive, relatively prime integers, then $\phi(m_1m_2) = \phi(m_1)\phi(m_2)$. If $m = \prod_{p_i|m} p_i^{r_i}$, then*

$$\phi(m) = m \prod_{p_i|m} \left(1 - \frac{1}{p}\right).$$

We say that ϕ is a multiplicative function because of the first property.

Algebraic proof: Recall that $\phi(m)$ is the order of $\mathbb{Z}/m\mathbb{Z}$. If m_1 and m_2 are relatively prime then $\mathbb{Z}/m_1m_2\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$. But the order of this direct product is m_1m_2 . Thus $\phi(m_1m_2) = \phi(m_1)\phi(m_2)$. ■

Theorem 3 (2.20). *Let $f(x)$ be a fixed polynomial with integer coefficients, and for any positive integer m let $N(m)$ denote the number of solutions of $f(x) \equiv 0 \pmod{m}$. If $m = ab$ and $(a, b) = 1$, then $N(m) = N(a)N(b)$.*

Examples:

Find all solutions to the congruence $x^2 + x + 7 \equiv 0 \pmod{15}$.

Find all roots of $x^2 + x + 7 \equiv 0 \pmod{21}$.