

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 13.

Last Time: We investigated the solutions of one congruence equation

$$ax \equiv b \pmod{m}.$$

(We failed to remark then that if m is prime, then every a which is not congruent to zero modulo m has an inverse modulo m .)

This time we introduced the (generalized) Chinese Remainder Theorem which tells us when we can solve the system of equations

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ (*) \quad x &\equiv b_r \pmod{m_r}. \end{aligned}$$

We did Examples 3.3.1 and 3.3.2 (with different numbers). We proved the Chinese Remainder Theorem, which says that if the numbers m_1, \dots, m_r are pairwise coprime, then (*) has a unique solution modulo $m_1 \cdots m_r$.

We also stated the generalized Chinese Remainder Theorem 3.3.4 which says that in general (*) has a solution if and only if $b_i \equiv b_j \pmod{(m_i, m_j)}$ for every i and j . We gave examples like those in Example 3.3.5.