Rifa
Safeer
Shah

Homework 2: Primes, GCD, and Congruences 09/17/2019

1. Use the trial division algorithm to find the prime factorization for the following numbers:

a) 6300

$p = 2 \mid 6300$? Yes $6300 = 2 \times 3150$

$p = 2 \mid 3150$? Yes $3150 = 2 \times 1575$

$p = 2 \mid 1575$? No

$p = 3 \mid 1575$? Yes $1575 = 3 \times 525$

$p = 3 \mid 525$? Yes $525 = 3 \times 175$

$p = 3 \mid 175$? No

$p = 5 \mid 175$? Yes $175 = 5 \times 35$

$p = 5 \mid 35$? Yes $35 = 5 \times 7$

$p = 5 \mid 7$? No

$p = 7 \mid 7$? Yes $7 = 7 \times 1$

$6300 = 2 \times 2 \times 3 \times 3 \times 5 \times 5 \times 7 = 2^2 \times 3^2 \times 5^2 \times 7$

b) 2080

$p = 2 \mid 2080$? Yes $2080 = 2 \times 1040$

$p = 2 \mid 1040$? Yes $1040 = 2 \times 520$

$p = 2 \mid 520$? Yes $520 = 2 \times 260$

$p = 2 \mid 260$? Yes $260 = 2 \times 130$

$p = 2 \mid 130$? Yes $130 = 2 \times 65$

$p = 2 \mid 65$? No

$p = 3 \mid 65$? No

$p = 5 \mid 65$? Yes $65 = 5 \times 13$

$p = 5 \mid 13$? No

$p = 7 \mid 13$? No

$\sqrt{13} < 7 \therefore 13$ is prime number

2. Use the Euclidean Algorithm to find the GCD of the following:

a) gcd(900, 270)

$900 = 270 \times 3 + 90$

$270 = 90 \times 3 + 0$

Rifa
Safeer
Shah

Homework 2: Primes, GCD and Congruences 09/17/2019

$900 = (90 \times 3) \times 3 + 90$

$\gcd(900, 270) = 90$

b) $\gcd(154, 165)$

$165 = 154 \times 1 + 11$

$154 = 11 \times 14 + 0$

$165 = (11 \times 14) \times 1 + 11$

$\gcd(154, 165) = 11$

3 Prove Theorem 4.4.1: Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. If (i) $ac \equiv bc \pmod{m}$ and (ii) $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

$ac \equiv bc \pmod{m}$

$\therefore\ m \mid ac - bc$

$\therefore\ m \mid c(a-b)$

$\gcd(c, m) = 1$ by Lemma 4.4.1

$m \mid c(a-b) = c$

$m \mid \frac{\cancel{c}(a-b)}{\cancel{c}} = \frac{\cancel{c}}{\cancel{c}}$

$m \mid (a-b) = 1$

$\therefore\ a \equiv b \pmod{m}$

4. Prove the Chinese Remainder Theorem

Prove that a solution exists

Let $M_k = \frac{m}{M_k}$ for $k = 1, 2, \dots, n$.

M_k is the product of the moduli except for M_k as m_i and M_k do not have common factors greater than 1 when $i \neq k$, $\gcd(M_k, M_k) = 1$

By theorem 4.4.2 $M_k Y_k = 1 \pmod{k}$

$X = a_1 m_1 y_1 + a_2 m_2 y_2 + \dots + a_n m_n y_n$

$M_j = 0 \pmod{m_k}$ wherever $j \neq k$ except kth term in this sum is $\cong 0 \bmod m_k$

Because $M_k Y_k = 1 \pmod{m_k}$

$X = a_k M_k Y_k \equiv a_k \pmod{m_k}$ for $k = 1, 2, \dots, n$