3.7 Applications of Number Theory

Thm 1 If $a, b \in \mathbb{Z}^+$, then $\exists\ s, t \in \mathbb{Z} \ni \gcd(a,b) = sa + tb$

(i.e. $\gcd(a,b)$ can be written as a linear combo of a & b w/ integer coefficients)

Lemma 1 If $a, b, c \in \mathbb{Z}^+ \ni \gcd(a,b) = 1$ and $a \mid bc$, then $a \mid c$.

Lemma 2 If p is prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Proof of uniqueness of prime factorization of $n \in \mathbb{Z}^+$.

(By contradiction) Suppose $n \in \mathbb{Z}^+$ can be written as prime factorization in two different ways, $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ where each $p_i \neq q_j$ are prime numbers, and $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$.

Assume there are some common prime factors that we can divide out from each factorization.

This leaves $p_{i_1} p_{i_2} \cdots p_{i_m} = q_{j_1} q_{j_2} \cdots q_{j_k}$ $m, k \in \mathbb{Z}^+$,

By Lemma 1, since $\gcd(p_{i_1}, q_{j_k}) = 1$ for some $k = 1, 2, \ldots, k$, then $p_{i_1} \mid q_{j_k}$ for at least one k. But this is a contradiction because no prime divides another prime. $\Rightarrow$ there is only one unique prime factorization for n //

3.7 (cont)

Ex 1 Express the gcd as a linear combo of the two integers.

(a) 21 and 44

(b) 117 and 213

(c) 36 and 48

3.7 (cont)

Thm 2 Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$.
If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then
$a \equiv b \pmod{m}$

Linear Congruence $ax \equiv b \pmod{m}$ $m \in \mathbb{Z}^+$

we want to solve for x

$\Rightarrow$ we need some sort of inverse to get x alone.

notation: $\bar{a}\, a \equiv 1 \pmod{m}$; integer $\bar{a}$ is inverse of a modulo m

---

Thm 3 If a & m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists, and this inverse is unique modulo m.
(i.e. $\exists$ a unique $\bar{a} \in \mathbb{Z}^+ \ni \bar{a} < m$ where $\bar{a}$ is an inverse of a modulo m & every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Ex 2 Find inverse of 7 modulo 26

3.7 (cont)

Ex 3 Solve $7x \equiv 10 \pmod{26}$

Ex 4 Solve $19x \equiv 5 \pmod{141}$

3.7 (cont)

Sun-Tsu's question: Find the #. when divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2.

Can be translated into:

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}\right\} \text{a system of congruences}$$

Thm 4 (Chinese Remainder Thm)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_n$ an arbitrary integers. Then

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

has unique soln modulo $M = m_1 m_2 \cdots m_n$

i.e. $\exists$ soln x $\ni$ $0 \le x < m$ + all other solns are $\equiv$ to x modulo m)

☆ read proof pg 236 (examples will use technique outlined there)

3.7 (cont)

Ex 5 To solve Sun-Tsu's question:

$a_1 = 2$
$a_2 = 3$
$a_3 = 2$

Let $m = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{m}{3} = 35$

$M_2 = \frac{m}{5} = 21$

$M_3 = \frac{m}{7} = 15$

universe of 35 modulo 3? y_1

universe of 21 modulo 5? y_2

universe of 15 modulo 7? y_3

$\Rightarrow$ solns to system are $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

3.7 (cont)

If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime integers, $m_i \geq 2$, and $m = m_1 m_2 \cdots m_n$ (product), then each integer a $0 \leq a < m$ can be uniquely represented by n-tuple,

$$(a \bmod m_1,\ a \bmod m_2, \ldots, a \bmod m_n)$$

Ex 6 Express each nonnegative integer a less than 15 using the pair $(a \bmod 3,\ a \bmod 5)$.

Ex 7 Which integers leave a remainder of 2 when divided by 3 and a remainder of 5 when divided by 7?