Unit 1:Divide & Conquer

Paul Ycay
MATH 409- Athabasca University

December 13, 2019

The following theorems are ones to be marked. There is a seperate file of handwritten notes for the rest of the theorems in this chapter

Theorem 1.1. Let a, b, c be integers. If $a|b$ and $a|c$, then $a|(b+c)$

Proof. Suppose $a|b$ and $a|c$. Then we want to find $r, s \in \mathbb{Z}$ such that $b = ar$ and $c = as$. Taking their sum, we have

$$\begin{aligned} c + b &= as + ar \\ c + b &= a(s + r) \\ c + b &= aq && (q \in \mathbb{Z}) \end{aligned}$$

Thus, $a|(b+c)$ ☐

Theorem 1.6. Let a, b, and c be integers. If $a|b$, then $a|bc$

Proof. Suppose $a, b, c \in \mathbb{Z}$. Then there exists $t \in \mathbb{Z}$ such that $at = b$

$$\begin{aligned} (at)c &= (b)c && \text{(by post multiplying by c)} \\ (at)c &= (at)c \\ &= a(tc) \\ &= aq && \text{(where } q = tc \text{ is an integer)} \end{aligned}$$

Thus, $a|bc$ ☐

Theorem 1.12. Let $a, b, c, d, \& n \in \mathbb{Z}$ with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$

Proof. Suppose $n|(a-b)$ & $n|(c-d)$.In other words, $\exists\ r, s \in \mathbb{Z}$ such that

$$\begin{aligned} sn &= c - d \\ sn + d &= c \\ 1)\, c &= sn + d \end{aligned}$$

Similarly,

$$\begin{aligned} rn &= a - b \\ rn + b &= a \\ 2)\, a &= rn + b \end{aligned}$$

Subtracting 2) by 1), we have,

$$\begin{aligned} a - c &= rn + b - (sn + d) \\ &= rn - sn + b - d \\ &= n(r - s) + b - d \\ &= nq + b - d && \text{(where } q = r - s \text{ is an integer)} \end{aligned}$$

Thus $a - c \equiv b - d \pmod{n}$ □

Theorem 1.14. Let $a, b, c, d, \& n \in \mathbb{Z}$ with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$

Proof. We want to show that $n|ac - bd$.
Suppose that $n|a - b$ and $n|c - d$. In other words, $\exists\ k, l \in \mathbb{Z}$ such that $nk = a - b$ and $nl = c - d$. Thus, $a = nk + b$ and $c = nl + d$. Taking their products, we have

$$\begin{aligned} ac &= (nk + b)(nl + d) \\ &= n^2kl - nkd + bnl + bd \\ &= n(nkl - kd + bn) + bd \\ &= nq + bd && \text{(where } q = nkl - kd + bn \text{ is an integer)} \end{aligned}$$

i.e. $ac - bd = nq$

Thus, $n|ac - bd$. □

Theorem 1.18. Let $a, b, k, \& n \in \mathbb{Z}\, with\, n > 0\, and\, k > 0.\, If\, a \equiv b \pmod{n},\, then\, a^k \equiv b^k \pmod{n}$.

Proof. By induction.
Base case: k=1
$a^1 \equiv b^1 \pmod{n}$
$a \equiv b \pmod{n}$
Thus, statement is true for k=1.
Induction step: Let statement be true for k=t
$a^t \equiv b^t \pmod{n}$
Now, consider $k = t + 1$
$a^{t+1} \equiv b^{t+1} \pmod{n}$
$a^t a \equiv b^t b \pmod{n}$ (by properties of exponents)
But by Theorem 1.14, we know that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$. Taking c to be a^t and d to be b^t, this completes the proof.
As statement is true for $k = t + 1$, the statement is true for all $k \in \mathbb{Z}$. □

Theorem 1.28. *Let $a, b,$ & n be integers with $n > 0$.*
Then $a \equiv b \pmod{n}$ if and only if a & b have the same remainder when divided by n.

Proof. If $a \equiv b \pmod{n}$, then $\exists\, q_1, q_2 \in \mathbb{Z}$ such that $a = q_1 n + r$ & $b = q_2 n + r$. Suppose $n | a - b \implies nx = a - b, x \in \mathbb{Z}$. In other words, $a = nx + b$.
Assume r is the remainder when dividing b by n, then we must show that r is the same remainder when dividing a by n. Assume that $b \equiv r \pmod{n} \implies b - r = nt, t \in \mathbb{Z}$
Thus $b = nt + r$. But

$$\begin{aligned} a &= nx + b \\ &= nx + nt + r && \because b = nt + r \\ &= n(x + t) + r \end{aligned}$$

Thus, $a \equiv b \pmod{n} \Leftrightarrow a$ and b have the same remainder when divided by n □

Theorem 1.43. *Let a , b, and , n be integers. If $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) =$ 1.*

Proof. Suppose $ax + ny = 1$ and $bt + ns = 1$, for some $x, y, t, s \in \mathbb{Z}$. In other words, ① $ax = 1 - ny$ and ② $bt = 1 - ns$. Multiplying ① by ②, we have

$$\begin{aligned} axbt &= (1 - ny)(1 - ns) \\ axbt &= 1 - ns - ny - n^2 sy \\ axbt &= 1 - n(s + y + nsy) \\ abxt &= 1 - nf && \because (f = s + y + nsy) \in \mathbb{Z} \\ abg &= 1 - nf && \because (g = xt) \in \mathbb{Z} \\ abg + nf &= 1 \end{aligned}$$

Thus, $(ab, n) = 1$. $\square$