Chapter 1

Day 15

Theorem 1.1 Prime Theorem of Divisibility

Let $m \in Integer, m \leq 1$. Then: m is prime $\leftrightarrow$ ($m|ab \rightarrow m|a$ or $m|b$)

Proof of Theorem above (already proved $\rightarrow$): (Other Direction):
If m is composite then:

$$(m|b \rightarrow m|a or m|b).$$

Now, Simplify the statement we want to show further:

$$\begin{aligned}(m|b \longrightarrow m|a \vee m|b) = \\ &= m|ab \wedge \ (m|a \wedge m|b) \\ &= m|ab \wedge (m|a \wedge m|b)\end{aligned}$$

Overall, we want to show that if m is composite them $(m|ab \wedge (m \nmid a \wedge m \nmid b))$

Assume m is composite.

Choose a = x and b = y. Then by D.L 4,

$$\begin{aligned}|x| < |m| \\ |y| < |n|.\end{aligned}$$

😀

Definition 1.1: Divisibility Property

$$\begin{aligned}a, b, q \in \mathbb{Z} \\ a > 0, b \geqslant 0 \\ r \in \mathbb{R} \\ \exists q > 0, q \in \mathbb{Z}, r \in \mathbb{N} \\ r < |b| st.a = bq + r.\end{aligned}$$

Definition 1.2: Modular Arithmetic

sad

Definition 1.3: Modular Arithmetic

Two integers a and b are **congruent modulo** m, written as $a \equiv b \pmod{m}$ if $b = a + km$ for some $k \in \mathbb{Z}$. (check camera roll for picture of worksheet related to this.)

Proof of Definition above: Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$
want to show $a \equiv c \pmod{m}$
we know from the definition of congruence mod m:

$$\begin{aligned} b &= a + km \\ c &= b + lm \\ c &= a + (l + k)m. \end{aligned}$$

Now, repack definition:

$$\begin{aligned} c &= a + (k + l)m \\ a &\equiv c(modm) \\ &. \end{aligned}$$

😄

Proof of 5 from worksheet: Try $n = 6$

$$(n - 1)! = 5! = 120 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$
$$.$$

😄