NUMBER THEORY HOMEWORK 1

WILL CHUANG

3.4–18

Proof:

Suppose $d = \gcd(a,b)$, i.e. $d \neq 0$, and $\exists$ some $l, m \in \mathbb{Z}$ s.t. $a = dl, b = dm$.

- Claim: $lcm(a,b) \leq \frac{ab}{d}$.

$$\Rightarrow ab = d^2lm = a(dm) = b(dl).$$

It follows that:

$$\frac{ab}{d} = am \Rightarrow a \mid \frac{ab}{d}$$

and

$$\frac{ab}{d} = bl \Rightarrow b \mid \frac{ab}{d}.$$

Since $lcm(a,b)$ means the *least* common multiple, thus if

$$a \mid \frac{ab}{d} \text{ and } b \mid \frac{ab}{d}$$

then

$$lcm(a,b) \mid \frac{ab}{d}$$

and this implies

$$lcm(a,b) \leq \frac{ab}{d}. \tag{1}$$

- Claim: $lcm(a,b) \geq \frac{ab}{d}$.

By the definition of the least common multiple, $a \mid lcm(a,b)$. Hence, we multiply b on the both sides

$$ab \mid lcm(a,b)b$$
$$\Rightarrow ab \mid lcm(a,b)dm$$
$$\Rightarrow \frac{ab}{d} \mid lcm(a,b)m$$

Thus,

$$\frac{ab}{d} \mid lcm(a,b)$$

which implies

$$lcm(a,b) \geq \frac{ab}{d}. \tag{2}$$

- By equations (1) and (2), we complete the proof.

3.1–28 Since $a \mid b \Rightarrow \exists k \in \mathbb{N}\, s.t. b = ka.$

- **Base case.** For $k = 1 \Rightarrow a = b \Rightarrow a \mid b \Rightarrow F_a \mid F_b$. Thus, the statement holds.
- **Inductive Case.**
  Suppose when $k = k', k' \in \mathbb{N}$ the statement is true.
  That is assume $a \mid ka \Rightarrow F_a \mid F_{ka} \Rightarrow \exists l \in \mathbb{Z}$ s.t. $F_{ka} = lF_a$.
  Proof:
  For $k = k' + 1$

$$\Rightarrow F_{(k'+1)a} = F_{k'a+a}$$
$$\Rightarrow= F_{k'a}F_{a+1} + F_{k'a-1}F_a$$
$$\Rightarrow= F_a(lF_{a+1} + F_{k'a-1})$$
$$\Rightarrow F_a \mid F_a(lF_{a+1} + F_{k'a-1})$$

Therefore, by induction $F_a \mid F_b$, and this completes the proof.

Theorem 1. *2.2.2 The Well-Ordering Principle*
Every nonempty set of positive integers has a smallest element.

Theorem 2. *2.2.3 Corollary*
Let S be a nonempty set of integers, and suppose there exists an integer m s.t for every $s \in S$, $s \geq m$. Then S has a smallest element.

Definition 3. *The Fibonacci sequence $F_1, F_2, ...$ is defined by $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}, n \leq 3$.*

Lemma 1. *For any natural number n, $\phi^n < F_{n+2} < \phi^{n+1}$.*

Definition 4. *3.1.1 Let $a, d \in \mathbb{Z}$. We say that d divides a if $\exists q \in \mathbb{Z}$ s.t. $a = qd$. We express this in symbols as $d \mid a$ (which is read d divides a).*

Lemma 2. *Let d, a be natural numbers. If $d \mid a$, then $1 \leq d \leq a$.*

Lemma 3. *Let $d, m, x, y \in \mathbb{Z}$ If $d \mid x$ and $d \mid y$, then $d \mid mx + ny$.*

Theorem 5. *Given any rational numbers r, there exists two relatively prime integers p and q, with $q \neq 0$, s.t. $r = \frac{p}{q}$.*

Definition 6. *gcd*

Definition 7. *lcm*

Theorem 8 (The Division Theorem)**.** *Let $a \in \mathbb{Z}$, and $b \in \mathbb{N}$. Then $\exists$ unique integers q and r s.t. $a = qb + r$.*

Lemma 4. *Let a, b, x be integers s.t. a, b are nonzero. If $a \mid x, b \mid x$, then $lcm(a, b) \mid x$.*