8/17

Review of UFT in $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

Def (Divisibility): Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that

a divides b / a is a divisor of b / b is divisible by a,

if there is $c \in \mathbb{Z}$ s.t. $b = ac$, namely, $\frac{b}{a} = c \in \mathbb{Z}$.

E.g. 1. $3 \mid 6$

2. $4 \mid -12$.

Properties:

1. Reflexivity: $a \mid a$ $(a \neq 0)$.

2. Anti-symmetry: $a \mid b$, $b \mid a \Rightarrow b = \pm a$.

3. Transitivity: $a \mid b$, $b \mid c \Rightarrow a \mid c$.

4. Linearity: $a \mid b$, $a \mid c \Rightarrow a \mid xb + yc$, $x, y \in \mathbb{Z}$.

5. Size: $a \mid b$ $(b \neq 0) \Rightarrow |a| \leq |b|$.

Defn (Unit). Let R be a comm ring (with 1). A unit in R is a nonzero element $r \in R$ s.t. $r^{-1} \in R$.

Q: Units in $\mathbb{Z}$?

A: ± 1.

Defn (Prime & Composite) $n > 1$ is called a prime number if it has only 1 and itself as positive divisors. Otherwise, n is called a composite number.

Lem 1.1. Every $n>1$ has a prime divisor.

Pf. ① $n=$ prime ✓.

② $n=$ composite: pick the smallest positive divisor $1<p<n$.

Claim: p is prime.

If $d \mid p$, then $d \mid n$. By minimality p and $d \leq p$, we see $d=1$ or $d=p$. So p is prime. $\square$

Thm (Fundamental Thm of Arithmetic) Every $n>1$ can be written as a product primes, uniquely up to the order of the prime factors.

E.g. $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 2 \cdot 5 = 5 \cdot 3 \cdot 2 \cdot 2 = \cdots$

Thm (Division Algorithm). Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$, s.t.

$$\underbrace{a}_{\text{dividend}} = \underbrace{q}_{\text{quotient}} \cdot \overbrace{b}^{\text{divisor}} + \underbrace{r}_{\text{remainder}}.$$