Given an integer "$p \geq 2$" we say p is prime if the only positive divisors of p are 1 and p itself.
A composite number is a number that is not prime.

Ex: (primes)

$2, 3, 5, 7, 11, 13, 17, 19, \ldots$

(gaps: 1, 2, 2, 2)

$\gcd(a,b) = a \cdot p + b \cdot q$

$p \mid a$

$a = k \cdot p$

$a \mid b \Leftrightarrow b = a \cdot \ell$

Lemma: $a, b, c \in \mathbb{Z}$, p prime

(a) $p \nmid a$ then $\gcd(p,a) = 1$.

(b) $a \mid bc$ and $\gcd(a,b) = 1 \Rightarrow a \mid c$.

(c) $p \mid bc \Rightarrow p \mid b$ or $p \mid c$.

Proof: (a) Since $p \nmid a$, the only common divisors of "a" and "p" is 1. $\Rightarrow \gcd(a,p) = 1$

(b) $bc = a \cdot k$ (+) $1 = a \cdot \ell + b \cdot m$ hypothesis

$c = a \ell c + b m c$

$c = a \ell c + a k m$

$= a(\ell c + km)$ ($= p$)

$= a p$.

$c = a \cdot p$ thesis

(c) $bc = p \cdot \ell$

Cases

$p \mid b$ or $p \nmid b$

$\Downarrow$

$p \mid b$ or $p \mid c$

$\gcd(p,b) = 1$

Using letter "b"

$p \mid bc$ and $\gcd(p,b) = 1$

$p \mid c$. □

$\not{a}x = \not{a}by$

$\mathbb{Z}_m$

$\not{2} \cdot 3 = \not{2} \cdot \frac{6}{2}$

Proposition Let $a, b, k, m \in \mathbb{Z}$, $k \neq 0$

$\overline{ak} \equiv \overline{bk}$, $\gcd(k,m) = 1$

$\Downarrow$

$\overline{a} = \overline{b} \Leftrightarrow \overline{a-b} = \overline{0}$

$m \mid a-b$

$\overline{a} = \{a + p \cdot m ;\ p \in \mathbb{Z}\}$

$\overline{ak} - \overline{bk} \equiv 0$

$ak - bk = p \cdot m$

$(a-b) \cdot k = p \cdot m$

$\cdot\ \overline{a} - \overline{b} = \overline{a-b}$

$\cdot\ \overline{0} = \overline{m \cdot \ell}$

Since $m \mid pm$ then $m \mid (a-b) \cdot k \Rightarrow m \mid a-b$

$a - b = m \cdot p$

$\overline{a-b} = \overline{0}$

$\overline{a} = \overline{b}$.

□

Theorem: (Fermat's little theorem) If $a \in \mathbb{Z}$ and p is a prime $p \nmid a$ then

$a^{p-1} \equiv 1 \pmod{p}$

$(\overline{a^{p-1}} = \overline{1}$

$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$

Proof: $\{\overline{a}, \overline{2a}, \overline{3a}, \ldots, \overline{(p-1)a}\} = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$

$\overline{k\not{a}} = \overline{\ell \not{a}}$

$\overline{k} = \overline{\ell}$

$\overline{a} \cdot \overline{b} = \overline{ab}$

$\overline{a} \cdot \overline{\not{2}a} \cdot \overline{\not{3}a} \cdots \overline{(\not{p}-1)a} = \overline{1} \cdot \not{\overline{2}} \cdot \not{\overline{3}} \cdots \not{\overline{p-1}}$

$\overline{a}^{p-1} = \overline{1}$

Proposition $x, y \in \mathbb{Z}_+$

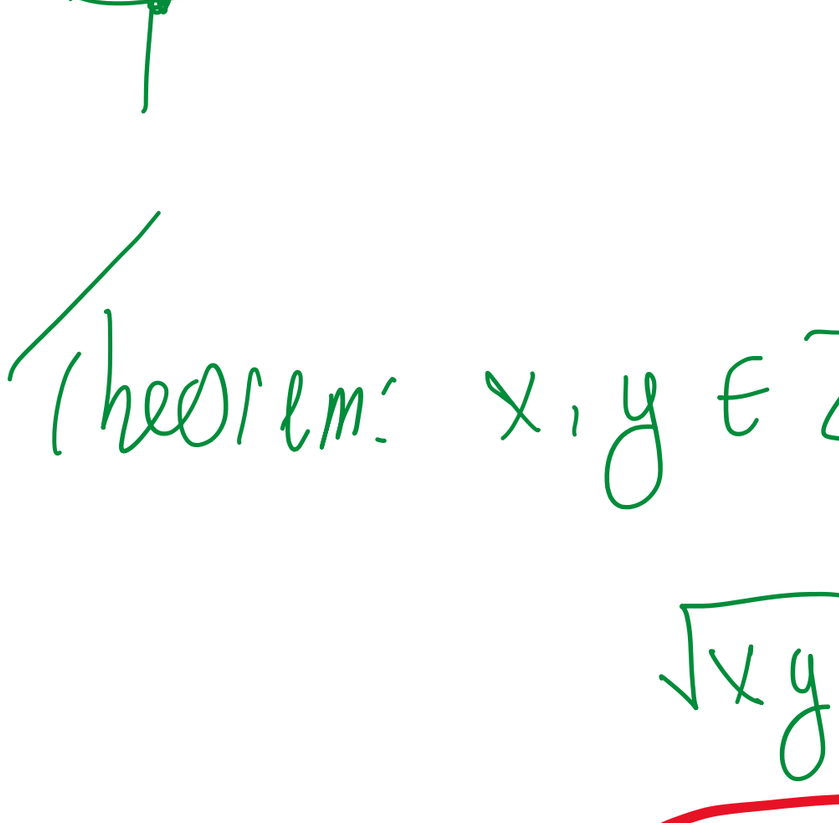
$x \geq y \Rightarrow \sqrt{x} \geq \sqrt{y}$

$x = (\sqrt{x})^2$

$(a^2 - b^2) = (a-b)(a+b)$

Proof: $x \geq y \Rightarrow x - y \geq 0$

$(\sqrt{x})^2 - (\sqrt{y})^2 \geq 0$



$(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \geq 0$

$\sqrt{x} - \sqrt{y} \geq 0$

$\sqrt{x} \geq \sqrt{y}$

Theorem: $x, y \in \mathbb{Z}_+$

$\sqrt{xy} \leq \frac{x+y}{2} \Leftrightarrow 2\sqrt{xy} \leq x + y$

Proof: $(\sqrt{x} - \sqrt{y})^2 \geq 0$

$+4\sqrt{xy}$ $\quad x - 2\sqrt{xy} + y \geq 0 \quad + 4\sqrt{xy}$

$x + 2\sqrt{xy} + y \geq 4\sqrt{xy}$

$x + y \geq 2\sqrt{xy}$

$\sqrt{xy} \leq \frac{x+y}{2}$

~ ✩ ~

2.3 $2k + 2p + 1 = 2(k+p) + 1$

$= 2q + 1$ odd

2.4

(a) $n = 2k$, $-n = -2k = 2 \cdot (-k)$

(c) $n = 2k$, $(-1)^n = (-1)^{2k} = ((-1)^2)^k = 1^k = 1$

2.8 (c) $n \in \mathbb{Z}$, $n^2 + 3n - 6$ is even

$n = 2k$

$(2k)^2 + 3 \cdot 2k - 6$

$4k^2 + 6k - 6 = 2 \cdot (\overbrace{2k^2 + 3k - 3}^{p}) = 2p$.

$n = 2k + 1$

$(2k+1)^2 + 3(2k+1) - 6$

$4k^2 + 4k + 1 + 6k + 3 - 6$

$4k^2 + 10k - 2$

$2(2k^2 + 5k - 1)$

$2p$

2.16 15 by 4

$15 = 4 \cdot 3 + 3$ (quotient 3, remainder 3)

65 by 11

$65 = 11 \cdot 5 + 10$

2.25. $\forall n \in \mathbb{Z}$ $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

$\overline{n^2} = \overline{0}$ or $\overline{n^2} = 1$

$n = 2k$

$\overline{n^2} = \overline{(2k)^2} = \overline{4k^2} = \overline{0}$

$n = 2k + 1$

$\overline{(2k+1)^2} = \overline{\not{4k^2} + \not{4k} + 1} = \overline{1}$

2.24. $a, b, c \in \mathbb{Z}$

$a^2 \mid b$ and $b^3 \mid c \Rightarrow a^6 \mid c$

$b = k \cdot a^2$, $c = \ell \cdot b^3$

$c = a^6 \cdot p$

$c = \underbrace{\ell \cdot k^3}_{p} \cdot a^6 = a^6 \cdot p$