

# Selected Definitions and Theorems for Math 322

**Def 2.1.1.**  $a|b \iff \exists c$  such that  $ac = b$

**Lem 2.1.3.**

- (a)  $a|b$  and  $x|y \implies ax|by$
- (b)  $a|b$  and  $b|c \implies a|c$
- (c)  $a|b$  and  $b \neq 0 \implies |a| \neq |b|$
- (d)  $a|b$  and  $a|c \implies a|bx + cy$

**The Division Thm**  $\forall a, b$  with  $b \neq 0$ ,  $\exists$  unique  $q$  and  $r$  such that  $a = bq + r$ ,  $0 \leq r < |b|$

**Lem 2.1.11.** Let  $n, d > 0$ . The number of positive multiples of  $d$  that are less than or equal to  $n$  is the floor of  $n/d$ .

**Prop 2.2.3. (Primality Test)**  $p$  is prime iff it is not divisible by any prime  $q$ ,  $1 < q \leq \sqrt{p}$ .

**FTA** Every positive integer greater than 1 can be factored uniquely into a product of primes.

**Lem 2.3.1.** Let  $a = \pm p_1^{d_1} \cdots p_k^{d_k}$  be the prime factorization. Then  $b|a$  and  $b > 0$  iff  $b = p_1^{e_1} \cdots p_k^{e_k}$  with  $0 \leq d_i \leq e_i$ ,  $i = 1, \dots, k$

**Prop 2.3.2** Let  $n = p_1^{e_1} \cdots p_k^{e_k}$ . The number of positive divisors  $\nu(n)$  of  $n$  is

$$\nu(n) = (e_1 + 1) \cdots (e_k + 1)$$

**Prop 2.3.4.**  $p$  is prime and  $p|ab$ , then  $p|a$  or  $p|b$ .

**Def 2.5.1.** The **greatest common divisor** of  $a$  and  $b$ , not both zero, is the largest integer dividing both  $a$  and  $b$ . It will be denoted by  $(a, b)$ .

**Def 2.5.3.** Two integers  $a$  and  $b$  are said to be **relatively prime**, or **coprime** if  $(a, b) = 1$ .

**Lem 2.5.4.**

- (a)  $(a, b) = (-a, b)$
- (b)  $(a, b) = (a - b, b)$
- (c)  $(a, b) = d$  implies  $(\frac{a}{d}, \frac{b}{d}) = 1$

**Thm 2.5.6.**  $\forall a, b, \exists m, n$  s.t.  $ma + nb = (a, b)$ .

**Def 2.5.8.** The **least common multiple** (denoted by  $[a, b]$ ) of  $a$  and  $b$  is the smallest positive integer divisible by both  $a$  and  $b$ .

**Prop 2.5.10.** Let  $a = p_1^{d_1} \cdots p_k^{d_k}$  and  $b = p_1^{e_1} \cdots p_k^{e_k}$  with  $d_i, e_i \geq 0$ . Then

$$(a, b) = p_1^{\min(d_1, e_1)} \cdots p_k^{\min(d_k, e_k)}$$

$$[a, b] = p_1^{\max(d_1, e_1)} \cdots p_k^{\max(d_k, e_k)}$$

**Cor 2.5.12.**  $(a, b)[a, b] = |ab|$

**Cor 2.5.13.**  $a|bc$  and  $(a, c) = 1 \implies a|b$ .

**Prop 2.5.15.** Let  $a = bq + r$  and  $0 \leq r < b$  then  $(a, b) = (b, r)$ .

**Thm 2.6.1.**  $ax + by = m$  is solvable iff  $(a, b)|m$ . If  $(x_0, y_0)$  is a solution, then all solutions are

$$x = x_0 + \frac{b}{(a, b)}k, \quad y = y_0 - \frac{a}{(a, b)}k, \quad \forall k$$

**Def 3.1.1.**  $a \equiv b \pmod{m}$  iff  $m|a - b$

**Prop 3.1.3.**

- (a)  $a \equiv a \pmod{m}$ ,  $\forall a$
- (b)  $a \equiv b \pmod{m}$  iff  $b \equiv a \pmod{m}$
- (c)  $a \equiv b$  and  $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

**Prop 3.1.5.**

- (a)  $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{m}$ ,  $\forall c$
- (b)  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$
- (c)  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$
- (d)  $a \equiv b \pmod{m}$ ,  $k > 0 \implies a^k \equiv b^k \pmod{m}$

**Prop 3.1.7.**

- (a)  $a \equiv b \pmod{m}$ , and  $d|m$  then  $a \equiv b \pmod{d}$
- (b)  $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m/(c, m)}$

**Prop 3.1.10.** If  $(n, m) = 1$ , then  $a \equiv b \pmod{m}$  and  $a \equiv b \pmod{n}$  iff  $a \equiv b \pmod{mn}$

**Def 3.2.1.**  $a' = a^{-1} \pmod{m}$  iff  $aa' \equiv 1 \pmod{m}$ .

**Prop 3.2.3.**  $a^{-1} \pmod{m}$  exists iff  $(a, m) = 1$ . If exists, it is unique modulo  $m$ .

**Prop 3.2.7.**  $ax \equiv b \pmod{m}$  has exactly  $d = (a, m)$  solutions if  $d|b$  and no solutions if  $d \nmid b$ . The  $d$  solutions, if exists, are

$$x_0 + \frac{m}{d}j, \quad j = 0, 1, \dots, d - 1$$

**The Chinese Remainder Thm** Let  $m_1, \dots, m_r$  be pairwise relatively prime. Then the simultaneous congruence  $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_r \pmod{m_r}$  has a unique solution modulo  $m_1 \cdots m_r$

**Thm 4.1.1 (Fermat).** Let  $p$  be prime. Then  $a^p \equiv a \pmod{p}$ . If  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Prop 4.1.5.** Let  $a^r \equiv 1 \pmod{p}$  and  $p$  be prime. If  $(r, p-1) = d$  then  $a^d \equiv 1 \pmod{p}$ .

**Def 4.2.1.**  $\phi(m)$  is the number of invertible elements in a complete residue system modulo  $m$ .

**Thm 4.2.3.** If  $(m, n) = 1$ , then  $\phi(mn) = \phi(m)\phi(n)$ .

**Thm 4.3.1 (Euler)** If  $(a, m) = 1$ , then  $a^{\phi(m)} \equiv 1 \pmod{m}$ .