

## Divisibility

$d \mid a$  and  $d \mid b \implies d$  divides any linear combination of  $a, b$

**Euclid Theorem:** there are an infinite number of primes

**Division Algorithm:** Let  $a, b \in \mathbb{Z}$  with  $b > 0$ . Then there exists unique  $q, r \in \mathbb{Z}$  such that  $a = bq + r$  with  $0 \leq r < b$

Ways of finding  $\gcd(a, b)$

- List all prime factors and take the largest factor
- Take a linear combination of  $a, b$  to find possible factors
- Euclidean Algorithm

Any common divisor of  $a, b$  divides  $\gcd(a, b)$

**Bezout Theorem:**  $\gcd(a, b) = ax + by$

If  $n$  is composite then  $2^n - 1$  is composite

If  $m$  is NOT a power of 2, then  $2^m + 1$  is composite

## Linear Diophantine Equations

We want to be able to find integer solutions  $(x, y)$  to  $ax + by = c$

- Solutions exist if and only if  $\gcd(a, b) \mid c$

General steps for solving Linear Diophantine problems

1. Verify  $\gcd(a, b) \mid c$
2. Divide the equation by  $d = \gcd(a, b) \implies a'x + b'y = c'$  where  $\gcd(a', b') = 1$
3. Use Extended Euclidean Algorithm to solve  $(x, y)$  for  $a'x + b'y = 1$ . Then multiply the solution by  $c'$
4. If a solution variable (e.g.  $x$ ) is negative, perform Extended Euclidean Algorithm with positive  $x$  then flip the sign at the end
5. General solutions will be  $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$

For relatively prime  $a, b$  and  $a, b \geq 0$ , there are no non-negative solutions to  $ax + by = ab - a - b$

For relatively prime  $a, b$ ,  $a, b \geq 0$ , and any  $n > ab - a - b$ , there is a non-negative solution to  $ax + by = n$

## Unique Factorization

**Theorem 4.1:** Let  $p$  be prime and  $a, b \in \mathbb{Z}$  such that  $p \mid ab$ . Then  $p \mid a$  or  $p \mid b$

**Fundamental Theorem of Arithmetic:** any positive integer greater than 1 can be uniquely factored into a product of primes

$\gcd(a, b) = 2^{d_2} 3^{d_3} \dots$  where  $d_p = \min(a_p, b_p)$

$\text{lcm}(a, b) = 2^{e_2} 3^{e_3} \dots$  where  $e_p = \max(a_p, b_p)$

## Applications of Unique Factorization

**Proposition 5.1:**  $n$  is a  $k$ th power if and only if all exponents in its prime factorization are multiples of  $k$

**Exercise 5.1.1.b:** Find  $n$  such that  $n/2$  is a square,  $n/3$  is a cube,  $n/5$  is a fifth power

**Exercise 5.4:** Show that any  $n$  with exponents  $> 1$  in prime factorization can be written as  $n = x^2 y^3$

**Example:** Show that  $\sqrt{3}$  is irrational

**Theorem 5.3:**  $n$  is not a perfect  $k$ th power  $\implies \sqrt[k]{n}$  is irrational

**Exercise 5.2.9:** For which positive integers is  $\sqrt[3]{64}$  rational?

**Theorem 5.4:** If  $r = \frac{u}{v}$  is a root of  $P(x)$  where  $\gcd(u, v) = 1$ , then  $u \mid a_0$  and  $v \mid a_n$

**Lemma 5.6:** For relatively prime  $a, b$ ,  $ab = n^k \implies a, b$  are both  $k$ th powers

**Lemma 5.7:** Square of an odd integer is  $\equiv 1 \pmod{8}$ . Square of an even integer is a multiple of 4

**Theorem 5.5:** For a PPT  $(a, b, c)$ ,  $c$  is odd and  $a \not\equiv b \pmod{2}$  and

$$a = n^2 - m^2 \quad b = 2mn \quad c = m^2 + n^2 \quad \gcd(m, n) = 1, n \not\equiv m \pmod{2}$$

**Theorem 5.8:**  $m$  is a difference of 2 squares if and only if  $m$  is odd or  $4 \mid m$

- Factorize  $m$  into 2 factors with the same parity and set  $m = \frac{v-u}{2}$  and  $n = \frac{v+u}{2}$

**Theorem 5.9:**  $n! = p^b c$  with  $p \nmid c \implies b = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots$

**Riemann Zeta Function:**  $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$

## Linear Congruence

$a \equiv b \pmod{m} \implies m \mid a - b$  AND  $a = b + km$  AND  $\gcd(a, n) = \gcd(b, n)$

- Example:**  $\gcd(1234, 10) = \gcd(4, 10)$  since  $1234 \equiv 4 \pmod{10}$

**Proposition 6.7:**  $\gcd(c, m) = 1$  and  $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}$

**Proposition 6.8:**  $\gcd(c, m) = d$  and  $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{\frac{m}{d}}$

**Proposition 6.10:** For a prime  $p$ ,  $ab \equiv 0 \pmod{p} \implies a \equiv 0 \pmod{p}$  or  $b \equiv 0 \pmod{p}$

- Corollary 6.11:** For a prime  $p$ ,  $x^2 \equiv 1 \pmod{p} \implies x \equiv \pm 1 \pmod{p}$

**Exercise 6.1.9:** Find all positive  $n$  such that  $123 \equiv 234 \pmod{n}$

**Exercise 6.1.26:** For twin primes, show that  $p, q \geq 5 \implies 3 \mid p + q \quad p, q \implies 4 \mid p + q \quad 12 \mid p + q$

**Example:** Compute  $3^{385} \pmod{479}$  using repeated squaring

**Division/Congruence Tests:**  $a \equiv a_0 \pmod{10, 5, 2} \quad a \equiv \sum_{i=0}^n a_i \pmod{3, 9} \quad \sum_{i=0}^n (-1)^i a_i \pmod{11}$  where  $0 \leq a_i \leq a_n$

Linear Congruence problem  $ax \equiv b \pmod{m}$  can be reduced to a Diophantine Problem with  $(-m, a, b) \quad -mx + ay = b$

- Let  $d = \gcd(g, m)$ . Then  $d \mid b \implies$  the congruence problem has  $d$  distinct solutions mod  $m$

**Exercise 6.4.60:** Find all  $0 \leq n \leq 23$  such that  $10x \equiv n \pmod{24}$  has solutions

**Exercise 6.4.65:** Find  $83x \equiv 1 \pmod{100} \quad 83x \equiv 2 \pmod{100}$

**Exercise 6.4.69:** Show that  $x^2 - 2y^2 = 10$  has no integer solutions

**Chinese Remainder Theorem:** Given  $x \equiv a_i \pmod{m_i}$  for relatively pairwise prime  $m_i$  then

$$x \equiv \sum_{i=1}^n a_i n_i u_i \quad n_i = \prod_{j \neq i} m_j \quad u_i = n_i^{-1} \pmod{m_i}$$

- Example:**  $x^2 \equiv 1 \pmod{275 = 5^2 * 11}$

**TODO Supplementary 14, 16**