MATH 135
GCD, LDE's, Congruence and Modular Arithmetic & Cryptography

Sachin Kumar*
University of Waterloo

Winter 2023†

* *skmuthuk@uwaterloo.ca*
†Last updated: February 26, 2023

Contents

1 The Greatest Common Divisor

Proposition 1.0.1
For all real numbers x, we have $x \leq |x|$.

Proposition 1.0.2 (Bounds by Divisibility)
For all integers a and b, if $b|a$ and $a \neq 0$ then $b \leq |a|$.

Proposition 1.0.3 (Division Algorithm)
For all integers a and positive integers b, there exist unique integers q and r such that

$$a = qb + r, \qquad 0 \leq r < b$$

Proposition 1.0.4 (GCD with Remainders)
For all integers a, b, q and r, if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proposition 1.0.5 (GCD Characterization Theorem)
For all integers a and b, and non-negative integers d, if

- d is a common divisor of a and b, and
- there exist integers s and t such that $as + bt = d$,

then $d = \gcd(a, b)$.

Proposition 1.0.6 (Bézout's Lemma)
For all integers a and b, there exists integers s and t such that $as + bt = d$, where $d = \gcd(a, b)$.

Proposition 1.0.7 (Common Divisor Divides GCD)
For all integers a, b and c, if $c|a$ and $c|b$, then $c| \gcd(a, b)$.

Proposition 1.0.8 (Coprimeness Characterization Theorem)
For all integers a and b, $\gcd(a, b) = 1$ if and only if there exist integers s and t such that $as + bt = 1$.

Proposition 1.0.9 (Division by the GCD)
For all integers a and b, not both zero, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, where $d = \gcd(a.b)$.

Proposition 1.0.10 (Coprimeness and Divisibility)
For all integers a, b and c, if $c|ab$ and $\gcd(a, c) = 1$, then $c|b$.

Proposition 1.0.11 (Prime Factorization)
Every natural number $n > 1$ can be written as a product of primes.

Proposition 1.0.12 (Euclid's Theorem)
The number of primes is infinite.

Proposition 1.0.13 (Euclid's Lemma)
For all integers a and b, then prime numbers p, if $p|ab$, then $p|a$ or $p|b$

Proposition 1.0.14
Let p be a prime number, n be a natural number, and $a_1, a_2, \ldots, a_n$ be integers. If $p|(a_1 a_2 \ldots a_n)$, then $p|a_i$ for some $i = 1, 2, \ldots, n$.

Proposition 1.0.15 (Unique Factorization Theorem)
Every natural number $n > 1$ can be written as a product of prime factors uniquely, apart from the order of factors.

Proposition 1.0.16 (Finding a Prime Factor)
Every natural number $n > 1$ is either prime or contains a prime factor less than or equal to $\sqrt{n}$.

Proposition 1.0.17 (Divisors From Prime Factorization)
Let $n \geq 2$ and $c \geq 1$ be positive integers, and let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

be the unique representation of n as a product of distinct primes $p_1, p_2, \ldots, p_k$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. The integer c is a positive divisor of n if and only if c can be represented as a product.

$$c = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}, \quad \text{where } 0 \leq \beta_i \leq \alpha_i \text{ for } i = 1, 2, \ldots, k$$

.

Proposition 1.0.18 (GCD From Prime Factorization)
Let a and b be positive integers, and let

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \qquad \text{and} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k},$$

be ways to express a and b as products of the distinct primes $p_1, p_2, \ldots, p_k$, where some or all of the exponents may be zero. We have

$$\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k} \text{ where } \gamma_i = \min\{\alpha_i, \beta_i\} \text{ for } i = 1, 2, \ldots, k.$$

Proposition 1.0.19 (Extended Euclidean Algorithm)
input: Integers a, b with $a \geq b > 0$.
Initialize: Construct a table with four columns so that

- the columns are labelled x, y, r and q,
- the first row in the table is $(1, 0, a, 0)$
- the second row in the table is $(0, 1, b, 0)$

Repeat: For $i \geq 3$,

- $q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$
- $\mathrm{Row}_i \leftarrow \mathrm{Row}_{i-2} - q_i \mathrm{Row}_{i-1}$

Stop: When $r_i = 0$.
Output: Set $n = i - 1$. Then $\gcd(a, b) = r_n$, and $s = x_n$ and $t = y_n$ are a certificate of correctness.

2 Linear Diophantine Equations

Theorem 2.0.1 (Linear Diophantine Equation Theorem 1)
For all integers a, b and c, with a and b not both zero, the linear Diophantine equation

$$ax + by = c$$

(in variables x and y) has an integer solution if and only if $d|c$, where $d = \gcd(a, b)$.

Theorem 2.0.2 (Linear Diophantine Equation Theorem 2)
Let a, b and c be integers with a and b not zero, and define $d = \gcd(a, b)$. If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + by = c$, then the set of all solutions is given by

$$\{(x, y) : x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n, n \in \mathbb{Z}\}.$$

3 Congruence and Modular Arithmetic