Chapter 11: Vector Spaces

May 20, 2023

Contents

1 Introduction

1.1 Notation

$a|b$ means a divides b
$b \in a\mathbb{Z}$ means b is a multiple of a

2 Euclidean division and gcd

Euclidean division: $a = b * q + r$
Euclidean Lemma: $pgcd(a, b) = pgcd(b, r)$

$$pgcd(a, b) = pgcd(b, a - qb)$$

3 Congruences

$a \equiv b \pmod{n} \implies \exists k \in \mathbb{N}, a = b + kn$
also $a \equiv b[n]$

$a \equiv b[n]$ and $c \equiv d[n] \implies a + c \equiv b + d[n]$
$a \equiv b[n]$ and $c \equiv d[n] \implies ac \equiv bd[n]$
$a \equiv b[n], \forall m \in \mathbb{N}, a^m \equiv b^m[n]$

We denote $D(a)$ the set of divisors of a and $a\mathbb{Z}$ the set of multiples of a

4 Bezout's theorems

4.1 Bezout Theorem

let (a,b) be two integers, then $\exists(u_1, u_2) \in \mathbb{Z}^2$ so that
$au_1 + bu_2 = gcd(a, b)$

4.2 Bezout Corollary

if $d|a$ and $d|b$ then $d|gcd(a, b)$

4.3 Gauss Lemma

if $a|bc$ and $gcd(a, b) = 1 \implies a|c$
to solve $ax + by = d$ equations you need to do the Euclid algorithm and "go back up"

5 Little Fermat's theorem

Let p be a prime number,

$$p|\binom{p}{k} \text{ and } \binom{p}{k} \equiv 0[n]$$

$$n^p \equiv n[p]$$

if $p \nmid n$ then

$$n^{p-1} \equiv 1[p]$$

6 RSA encryption

7 El Gamal encryption