FOCS Notes
2/14/2020

Lecture 10 Number Theory

- Division and Greatest Common Divisor (GCD)
  - Euclid's algorithm for GCD
  - Bezout's Identity
- Modular Arithmetic
  - Cryptography
  - RSA public key cryptography

Contents

1 Basics

1.1 Quotient-Remainder Theorem

For $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, $n = qd + r$, where $0 \leq r \leq d$ and $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ are unique
Ex: $n = 27,\ d = 6 \ \longrightarrow\ q = 4,\ r = 3$
$n = -27,\ d = 6 \ \longrightarrow\ q = -5,\ 3$ *NOTE* remainder must be positive
Define d is a divisor of n, written $d|n$, if the remainder in the QRT is zero.
That is, $d|n \iff n = qd$ for some $q \in \mathbb{Z}$

1.2 Primes

$P = \{2, 3, 5, 7, 11, \dots\} = \{p | p \geq 2$ and the only divisors of p are 1 and $p\}$

Composite Numbers
All the number ≥ 2 with more than 2 prime divisors.

Facts

1) $d|0$

2) $d|n$ and $d|m \rightarrow d|(n+m)$

3) $d|n$ and $d'|m \rightarrow dd'|nm$

4) $d|n$ then $xd|xn$ for $x \in \mathbb{Z}$

5) $d|m$ and $m|n \rightarrow d|n$

6) $d|(m+n)$ and $d|m \rightarrow d|n$

Proof. $d|m+n \Rightarrow m+n = q_1 d$
$d|m \Rightarrow m = q_2 d$
$n = (q_1 - q_2)d$
$\Rightarrow d|n$ □

2 Common Divisors

We say d is a common divisor of m and n if $d|m$ and $d|n$
m and n are coprime or relatively prive if they have no common divisors other than 1

GCD
We say $d = gcd(m,n)$if any l that is a common divisor of m and n satisfies $l \leq gcd(m,n)$
Ex: divisors of 30 = {1,2,3,4,6,10,15,30}
divisors of 42 = {1,2,3,6,7,14,21,42}
common divisors = {1,2,3,6}
gcd(30,42) = 6

Q: Efficient Algg for finding $gcd(m,n)$?
One that doesn't require factorization
Fact: $gcd(m,n) = gcd(m, rem(n,m))$ *NOTE* $rem(n,m) = r$ after using QRT to write $n = qm + r$
Check: $gcd(30,42) = gcd(30,12) = gcd(12,6) = gcd(6,0) = 6$
Ex: $gcd(42,108) = gcd(42,24) = gcd(24,18) = gcd(18,6) = gcd(6,0) = 6$

Claim $gcd(m,n) = gcd(m, rem(n,m))$

Proof. Idea:

(1) show $gcd(m,n)|m$ and $gcd(m,n)|rem(n,m)$ which gives $gcd(m,n) \leq gcd(m, rem(n,m))$

(2) then show $gcd(m, rem(n,m))|m$ and $gcd(m, rem(n,m))|n$ which gives $gcd(m, rem(n,m)) \leq gcd(m,n)$

To show (1): Clearly $gcd(m,n)|m$. Now consider $rem(n,m)$ comes from $n = qm + r \Rightarrow rem(n,m) = n - qm$ and since $gcd(m,n)|n$ and $gcd(m,n)|(-qm)$, we have $gcd(m,n)|n - qm$ so $gcd(m,n)|rem(n,m)$. We see that $gcd(m,n) \leq gcd(m, rem(n,m))$

To show (2): Trivially $gcd(m, rem(n,mm))|m$, and since $gcd(m, rem(n,m))|m$ and $gcd(m, rem(n,m))|rem(n,m)$, we have $gcd(m, rem(n,m))|qm + rem(n,m) = n$ Therefore $gcd(m, rem(n,m))$ is a common divisor of m and n and satisfies $gcd(m, rem(n,m)) \leq gcd(m,n)$

We conclude from (1) and (2) that $gcd(m, rem(n,m)) = gcd(m,n)$ □

Facts about GCD

1) $gcd(m,n) = gcd(m, rem(n,m))$

2) Every common divisor l of m and n divides $gcd(m,n)$

3) For every $k \in \mathbb{N}$, $gcd(km, kn) = k * gcd(m,n)$

4) If $gcd(l,m) = 1$ and $gcd(l,n) = 1$ then $gcd(l, mn) = 1$

5) If $l|mn$ and $gcd(l,m) = 1$, then $l|n$

Bezout's Identity
$gcd(m,n)$ is the smallest positive integer linear combination of m and n: $gcd(m,n) = mx + ny$ where $x, y \in \mathbb{Z}$
Ex: 3 and 5 satisfy $gcd(3,5) = 1$
$1 = 2 * 3 - 5$
42 and 108 satisfy $gcd(42,108) = 6$
$6 = 2 * 108 - 5 * 42$

Proof. Let l be the smallest positive integer combination of m and n
First show $l \leq gcd(m,n)$
We must establish that $l|m$ and $l|n$. Note that we can write $m = ql + r$ where $0 \leq r < l$. $r = m - ql = m - q(mx + ny) = m(1-q) - n(qy)$. This implies $r = 0$ because otherwise $0 < r < l$ is a positive integer combination of m and n that is smaller than l, which is a contradiction.
The same argument for n shows that $l|n$. We see that $l \leq gcd(m,n)$
Second show $gcd(m,n) \leq l$
Recall $l = mx + ny \Rightarrow gcd(m,n)|l$
Therefore $gcd(m,n) = l$ □

Proof of GCD fact 5)

Proof. $gcd(l,m) = 1 \Rightarrow 1 = lx + my \Rightarrow n = l(nx) + mny$. Note $l|l$ and $l|mn$, so $l|l(nx) + nmy$ so $l|n$ □

Proof of GCD fact 2)

Proof. $gcd(m,n) = mx + ny$ and $l|m$ and $l|n$ so $l|gcd(m,n)$ □

Proof of GCD fact 4)

Proof. $1 = la + mb$
$1 = lc + nd$
$\Rightarrow (la + mb)(lc + nd) = l^2ac + lmbc + lnad + mnbd = l(lac + mbc + nad) + mn(bd) = 1$ □

3 Modular Arithmetic

Motivation: Cryptography
Alice wants to send Bob message M, but Charlie can intercept all transmissions
Alice and Bob share a large prime number k
$M_* = Mk$
Finefor one round because to recover M, Charlie has to factorize M_* (practically impossible)
Problem: if Alice sends two messages: $M_*^1 = M_1k$ and $M_*^2 = M_2k$, Charlie can compute $gcd(M_1k, M_2k) = kgcd(M_1, M_2)$ if M_1 and M_2 are co-prime
Weaknesses:

- Requires private-key
- Only really works once

One solution: RSA (Rivest, Shamir, Adleman) public-key cryptography scheme

- uses modular arithmetic with primes

Modular arithmetic
$a \equiv b \ mod \ d$ if $d|(a-b)$
$15 \equiv 1 \ mod \ 2$ because $15 - 1 = 14$ is divisible by 2
We can show that many of the usual arithmetic properties are preserved under modularity.
$a + b \equiv c + e \ mod \ d$ if $a \equiv b \ mod \ d$ and $b \equiv e \ mod \ d$
$(c * a) \ mod \ d = (c \ mod \ d) * (a \ mod \ d) \ mod \ d$

Properties of modular arithmetic
$a \equiv b \ mod \ d$
$r \equiv s \ mod \ d$

(i) $ar \equiv bs \ mod \ d$

(ii) $a + r \equiv b + s \ mod \ d$

(iii) $a^n \equiv b^n \ mod \ d$

Property 1 Proof:

Proof. $a \equiv b \ mod \ d \Rightarrow a = b + dq$
$r \equiv s \ mod \ d \Rightarrow r = s + dm$
$\Rightarrow ar = (b + dq)(s + dm) = bs + d(qs + bm + dqm)$
$\Rightarrow ar \equiv bs \ mod \ d$ □

$15 \not\equiv 13 \ mod \ 12$
$15 * 6 \ mod \ 12 = 90 \ mod \ 12 = 6$
$13 * 6 \ mod \ 12 = 78 \ mod \ 12 = 6$
$15 * 6 \ mod \ 12 \equiv 13 * 6 \ mod \ 12$, but $15 \not\equiv 13 \ mod \ 12$.
Conclusion: there is no multiplicative inverse of 6 mod 12

<u>Modular Division</u>
If $ac = bc \ mod \ d$, and $gcd(c, d) = 1)$, then $a \equiv b \ mod \ d$
Proof in book.
<u>Fact:</u> If d is a prime number, then $gcd(c, d) = 1$
$ac = bc \ mod \ d \iff a \equiv b \ mod \ d$
and equivalently, there exists z such that $z * c \equiv 1 \ mod \ d$