|  |  |
| --- | --- |
| **McGill University**  **MATH 240 - Discrete Structures** | **Fall 2011**  **Prof Sergey Norin** |

# Number Theory

## definitions

p>1 is prime ⬄ p|c where c = {1, p}

n>1 is composite ⬄ n|c where c = {1, n, …}

c=CD(a,b) ⬄ c|a & c|b

GCD(a,b) is the largest cd(a,b)

## Division theorem

For any integers a>0 and b,

there exists integers q and b so that:

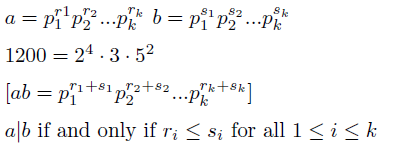
**b = q a + r**

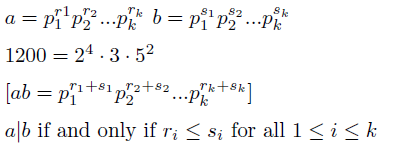
with r being the remainder 0≤r≤a.

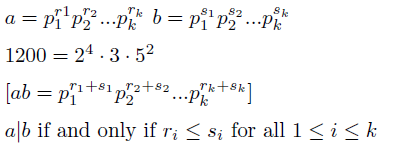
#### Divisibility

a|b ⬄ r = 0

#### With prime factorization







## Prime factorization

#### Fundamental theorem of arithmetic

Every positive integer can be written as the product of primes, and this factorization is unique up to the order of prime factors.

#### Theorem

If a prime p|ab => p|a or p|b

#### Theorem

There are infinitely many primes.

#### Theorem

There exist infinitely many pairs of primes (p, p+2).

#### Theorem

The number of primes among 1,2,..n is π(n) ≅ n/log n

#### Theorem

For every positive integer n there exists a prime p such that:



#### Goldback

Every even integer bigger than 2 is expressible as a sum of 2 primes.

## Linear combination & GCD

A linear combination of a and b is an integer c expressible as:

**c = sa + tb**

where s and t are integers.

#### Theorem

d = cd (a, b)

=> Every linear combination of a & t is divisible by d.

d = cd (a, b) and some c= sa+ tb

=> c|d

#### Theorem

GCD(a,b) is the smallest linear combination of a and b.

#### Theorem

c is a liner combination of a and b

⬄ GCD(a,b)|c

#### Theorem

GCD(a,b) is divisible by every common divisor of a & b

#### Theorem

For any integer k:

GCD(ka, kb) = k GCD(a,b)

#### Theorem

GCD(a,b) = 1 & GCD (a,c) =1

=> GCD(a,bc) =1

#### Theorem

GCD(a, b) = 1 & a|bc

=> a|c

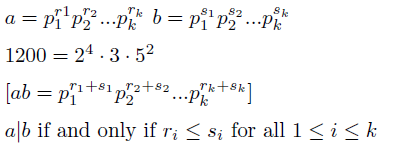
#### Theorem

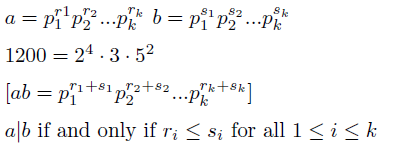
a = bq + r

* GCD (a,b) = GCD (b,r)

### Find gcd

#### With prime factorization







#### Euclid’s algorithm

Use thm : a = qb + r

* GCD (a,b)=GCD(b,r)

Ex: GCD(962, 230)

|  |  |
| --- | --- |
| = GCD(230; 42) | 962 = (4) 230 + 42 |
| = GCD(42; 20) | 230 = (5) 42 + 20 |
| = GCD (20; 2) | 42 = (2) 20 +2 |
| = 2 | 20 = 2(10) + 0 |

### Find linear combination

Ex: Find s and t such that GCD(962, 230)= 962s+230t.

2…

= 42 - 2·20

= 42 - 2·(230 - 5·42)

= 11·42 - 2·230

= 11·(962 - 4·230) - 2·230

= 11·962 - 46·230

## Modular algorithm

*rem(a,m) is the remainder of a after division by m*

*where 0 ≤ rem(a,m) ≤ m*

a≡b(mod m)

⟺ m|(a-b)

⟺ a=km + rem(a,m)

⬄ rem(a,m) = rem(b,m )

a≡0(mod m) ⟺ m|a

a≡a(mod m)

a≡b(mod m) ⬄ b≡a(mod m)

a≡b(mod m) & b≡c(mod m) ⬄ a≡c(mod m)

a≡b(mod m) & c≡d(mod m)

⬄ a+b≡b+d(mod m)

⬄ ac≡bd(mod m)