

Chapter 11 Cryptology

Jason Pearson and Sam Demorest

March 31, 2015

Overview

Number Theory Review
Greatest Common Divisor
Euclid's Algorithm

Euclid's Algorithm
Extension to Euclid's
Algorithm

Modular Arithmetic

Group Theory
Congruency Modulo n
Subgroups

Solving Modular Linear
Equations

Solving Modular Linear
Equations

Computing Modular Powers

Computing Modular Powers

Finding Large Prime Numbers

Searching for a Large Prime
Checking if a Number is
Prime

RSA Public-Key Cryptosystem

Public-Key Cryptosystems
RSA Cryptosystem

Composite and Prime Numbers

Composite Numbers have a divisor other than itself and one.

For example $4|20$ means that $20 = 5 * 4$

The divisors of 12 are 1,2,3,4,6 and 12

Prime numbers have no divisors but 1 and itself

First 10 Primes

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Greatest Common Divisor

If $h|m$ and $h|n$ then h is called a common divisor

A common divisor is a number that is a factor of both numbers

The greatest common divisor is the largest factor for both numbers

This is denoted $\gcd(n,m)$

For example $\gcd(12,15) = 3$

For any two integers n and m where $m \neq 0$ the quotient is n divided by m is given by

$$q = \lfloor n/m \rfloor$$

The remainder r of dividing n by m is given by

$$r = n - qm$$

Greatest Common Divisor (cont)

Let n and m be integers, not both 0 and let

$$d = \min \{ in + jm \text{ such that } i, j \in \mathbb{Z} \text{ and } in + jm > 0 \}$$

That is, d is the smallest positive linear combination of n and m

For example we know $\gcd(12, 8) = 4$,

the smallest linear combination is

$$4 = 3(12) + (-4)8$$

Now suppose we have $n \geq 0$ and $m > 0$ and $r = n \bmod(m)$ then

$$\gcd(n, m) = \gcd(m, r)$$

$$\text{so } \gcd(64, 24) = \gcd(24, 16)$$

$$= \gcd(16, 8)$$

$$= \gcd(8, 0)$$

$$= 8$$

Least Common Multiple

For n and m where they are both nonzero, the least common multiple is denoted $\text{lcm}(n,m)$

For example $\text{lcm}(6,9) = 18$ because $6|18$ and $9|18$

The $\text{lcm}(n,m)$ is a product of primes that are common to m and n , where the power of each prime in the product is the larger of its orders in n and m

So $12 = 2^2 3^1$ and $45 = 3^2 5^1$

so $\text{lcm}(12,45) = 2^2 3^2 5^1 = 180$

Prime Factorization

Two integers are relatively prime because the gcd of them is 1

For example $\gcd(12, 25) = 1$ so they are relatively prime

If h and m are relatively prime and h divides nm , then h divides m .

That is $\gcd(h, m) = 1$ and $h \mid nm$ implies $h \mid n$

Prime Factorization (cont)

Every integer $X > 1$ can be written as a unique product of primes

That is $X = p_1^{k_1} * p_2^{k_2} * \dots * p_n^{k_n}$

Where $p_1 < p_2 < \dots < p_n$ and this representation of n is unique

Example being $22,275 = 3^4 * 5^2 * 11$

To solve $\gcd(3,185,325, 7,276,500)$ we know

$$3,185,325 = 3^4 5^2 11^2 13^1$$

$$7,276,500 = 2^2 3^3 5^3 7^2 11^1$$

We then take the common divisors and take the lower power to create the gcd

$$\text{so } \gcd(3,185,325, 7,276,500) = 3^3 5^2 11^1 = 7,425$$

Euclid's Algorithm

Euclid's Algorithm gives us a straight forward way to find the gcd of two numbers

```
int gcd(int n, int m)
{
    if(m == 0)
        return n;

    else
        return gcd(m, n mod m);
}
```

Extension to Euclid's Algorithm

Group Theory

Congruency Modulo n

Subgroups

Solving Modular Linear Equations

Computing Modular Powers

Searching for a Large Prime

Checking if a Number is Prime

Public-Key Cryptosystems

RSA Cryptosystem