Chapter 11 Cryptology

Jason Pearson and Sam Demorest

April 1, 2015

Overview

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 n is given by
$q = \lfloor n/m \rfloor$
The remainder r of dividing n by m is given by
$r = n - qm$

Greatest Common Divsor (cont)

Let n and m be integers, not both 0 and let
d = min { in + jm such that i,j $\in$ Z 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 mod(m) then
gcd(n , m) = gcd(m , r)

$$
\begin{aligned}
\text{so } \gcd(64, 24) &= \gcd(24, 16)\\
&= \gcd(16, 8)\\
&= \gcd(8, 0)\\
&= 8
\end{aligned}
$$

Least Common Multiple

For n and m where they are both nonzero, the least common multiple is denoted lcm(n,m)
For example lcm(6,9) $= 18$ because $6|18$ and $9\ |18$
The 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 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$|$nm implies h$|$n

Prime Factorization (cont)

Every integer X $>$ 1 can be written as a unique product of primes
That is X = $p_1^{k_1} * p_2^{k_2} * \ldots * p_n^{k_n}$
Where $p_1 < p_2 < \ldots p_n$ 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
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

```
void Euclid (int n, int m, int gcd, int i, int j){
        if (m == 0) {
                gcd = n; i = 1; j = 0;
        }
        else {
                int iprime, jprime, gcdprime;
                Euclid (m, n mod m, gcdprime, iprime, jprime);
                gcd = gcdprime;
                i = jprime;
                j = iprime -⌊n/m⌋ jprime ;
        }
}
```

Why Use the Other Algorithm?

This other algorithm will give us integers i and j as well
So, gcd $=$ in $+$ jm
For Example Euclid(42, 30, gcd, i, j) outputs
gcd $=$ 6, i $=$ -2 and j $=$ 3
6 $=$ -2(42) $+$ 3(30)

Proof Extended Algorithm

Induction Base: In the last recursive call m = 0, which means gcd(n, m) = n
Since the values of i and j are assigned values 1 and - respectively we have
$in + jm = 1n + 0m = n = gcd\,(n, m)$

Induction Hypothesis: Assume in the kth recursive call the values determined for i and j are such that
gcd(n,m) = in + mj
Then the values returned by that call for i' and j' are values such that
gcd(m, n mod m) = i'm + j'n mod m

Proof Extended Algorithm (cont)

Induction Step: We have for the (k - 1)st call that

$$
\begin{aligned}
\text{in} + \text{mmj} &= \text{j'n} + (\text{i'} - \lfloor n/m \rfloor \text{ j'})\text{m} \\
&= \text{i'm} + \text{j'}(\text{n} - \lfloor n/m \rfloor \text{m}) \\
&= \text{i'm} + \text{j'n mod m} \\
&= \text{gcd(m, n mod m)} \\
&= \text{gcd(n,m)}
\end{aligned}
$$

The second to last equality is due to the induction hypothesis

Group Theory

A closed binary operation * on a set S is a rule for combining two elements of S to yield another element of S.
This operation is associative, has an identity element and inverse element
For example with integers $\in Z$ with addition constitute a group.
The identity element is 0 and the inverse of a is -a
Every element in the group only has one inverse
A group is said to be finite if S contains a finite number of elements
A group is said to be commutative (or abelian) if for all a, b $\in$ S,

Congruency Modulo n

Let m and k be integers and n be a positive integer. If n|(m - k) we say m is congruent to k modulo n, and this is written by
$m \equiv k \mod n$
For Example
Since 5|(33 - 18), $33 \equiv 18 \mod 5$

Subgroups

Solving Modular Linear Equations

Computing Modular Powers

Searching for a Large Prime

Checking if a Number is Prime

Public-Key Cryptosystems

RSA Cryptosystem