Factors And HCFs

If d|a and d|b then d|(ax+by)

If a=bq+r then (a, b)=(b, r)

Euclid's Algorithm $r_i = r_{i-2} - q_i r_{i-1}$

$s_i = s_{i-2} - q_i s_{i-1}$

$t_i = t_{i-2} - q_i t_{i-1}$

$r_i = s_i a + t_i b$

Efficiency: O(log(a)) in the first number

Diophantine Equat. $ax + by = c$

(a, b)|c for solubility

$v = y + \frac{ka}{(a,b)}$, $y = \frac{tc}{(a,b)}$

$u = x - \frac{kb}{(a,b)}$, $x = \frac{sc}{(a,b)}$

Modular Arithmetic

Congruence $\exists q \in Z, a = b + qm$

Division $\exists x, ax \equiv c (\mathrm{mod}\ m) \Rightarrow (a, m) | c$

Units Calculate reciprocal iif (a,m) = 1

Eulers Totient Function:

Number of natural numbers less than m and co-prime to m (i.e. # of units mod m).

For primes $\varphi(p) = (p-1), \varphi(p^n) = p^n - p^{n-1}$

$\varphi(mn) = \varphi(m)\varphi(n)$

$\varphi(m) = m \prod_{p|m} (1 - \frac{1}{p})$

Chinese Remainder Theorem:

Exists x such $x \equiv a (\mathrm{mod}\ m)$, $x \equiv b (\mathrm{mod}\ n)$ where x is unique mod (mn) if (m,n) = 1.

Solution Find $ms + nt = 1$, $x = bms + ant$

Wilsons Theorem $(p-1)! \equiv -1 (\mathrm{mod}\ p)$

Eulers Theorem $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$ if (a,m)=1,m>1

Fermat-Euler $a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\ p)$

Cryptography

Diffe-Hellman Key Exchange:

1. Choose p, the prime modulus
2. Pick e such that (e, p-1) = 1
3. Find d such that:
   $de \equiv 1 (\mathrm{mod} (p-1)) \Rightarrow de = 1 + (p-1)t$
4. Use standard two-box message passing with d and e as (de|en)cryption keys

The RSA Code:

1. Choose primes p and q, product m
2. Pick e such that (e, φ(m)) = 1
3. Find d such that:
   $de \equiv 1 (\mathrm{mod}\ \varphi(m)) \Rightarrow de = 1 - \varphi(m)t$
4. Publish m, e, used to encrypt sent text
5. Decryption by raising to the power d

Coin Tossing By Telephone:

1. Let p be a prime of the form 4k + 3
2. To work out square roots we can use:
   $a \equiv x^2 (\mathrm{mod}\ p) \Rightarrow x = a^{k+1}$
3. Let p, q be primes product n, tell B n
4. B picks s so that (s,n) = 1, tell A:
   $a \equiv s^2 (\mathrm{mod}\ n)$
5. A gets roots as below, sends one to B
   $a \equiv z^2 (\mathrm{mod}\ n) \Rightarrow a \equiv x^2 (\mathrm{mod}\ p), a \equiv y^2 (\mathrm{mod}\ q)$
   So use CRT to compute solutions z (±s, ±t)
6. If B has t, factor n and win else lose