Number Theory III

Permutation of a list

A permutation of a list is just some reordering of it, e.g.

4,1,3,2 → 1,2,3,4

10,2,14,2→ 14,2,10,2

Some interesting permutations

- Backwards reordering
  - 1,2,3,4,5,6,7,8 → 8,7,6,5,4,3,2,1
  - 1,3,5,7,2,4,6,8 → 8,6,4,2,7,5,3,1
- Sorting
  - 5,3,1,8,2,4,7,6 → 1,2,3,4,5,6,7,8
- Card shuffling
  - 1,2,3,4,5,6,7,8 →
    (cut the deck) 1,2,3,4 5,6,7,8 →
    (combine) 1,5,2,6,3,7,4,8

Last lecture's lemmas

Assume p prime, $k \neq 0$ not a multiple of p then

1. k has a multiplicative inverse $mod\ p$
2. $ak \equiv bk\ (mod\ p) \Rightarrow a \equiv b\ (mod\ p)$
3. $(0 \cdot k)\ rem\ p,\ (1 \cdot k)\ rem\ p, \ldots, ((p\text{-}1) \cdot k)\ rem\ p$ is a permutation of the sequence $0,1,\ldots,p\text{-}1$
4. Fermat's theorem: $k^{p-1} \equiv 1\ (mod\ p)$

Working *(mod n)* for composite *n*

Do we have inverses? Cancellation? Analogue of Fermat's theorem?

Relatively Prime Numbers

- a,b are relatively prime if $gcd(a,b)=1$
- Examples:
  - Not relatively prime:
    - 2,4
  - Relatively prime:
    - 9,10
    - p,k if p is a prime and k not a multiple of p

Inverses *mod n*

Thm. If k relatively prime to n then k has an inverse k^{-1} such that $kk^{-1} \equiv 1 \ (mod\ n)$

Cancellation

Corr: If k relatively prime to n then

$$ak \equiv bk \ (mod\ n) \Rightarrow$$
$$a \equiv b \ (mod\ n)$$

Permutations

If k relatively prime to n and $k_1 \ldots k_r$ are all integers relatively prime to n for which $0 < k_i < n$ then

$$(k_1 \cdot k) rem\ n, (k_2 \cdot k) rem\ n, \ldots, (k_r \cdot k) rem\ n$$

is a permutation of the sequence $k_1, \ldots, k_r$

Euler ϕ function

$$\phi(n) = |\{ j \mid 1 \le j < n \quad gcd(j,n) = 1\}|$$

Examples:

$\phi(7) = 6$

1,2,3,4,5,6

$\phi(49) = 42$

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,…

$\phi(12) = 4$

1,2,3,4,5,6,7,8,9,10,11

Euler ϕ function

$$\phi(n) = |\{ j \mid 1 \le j < n \quad gcd(j,n) \equiv 1\}|$$

Theorem:

1. a,b relatively prime $\Rightarrow \phi(ab) = \phi(a)\phi(b)$
2. p prime $\Rightarrow \phi(p^k) = p^k - p^{k-1}$ for $k \ge 1$

Examples:

$\phi(7) = 7-1=6$

1,2,3,4,5,6

$\phi(49) = 49-7=42$

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,…

$\phi(12) = \phi(2^2) \cdot \phi(3) = 2 \cdot 2 = 4$

1,2,3,4,5,6,7,8,9,10,11

Euler's Theorem

If k relatively prime to n then

$$k^{\phi(n)} \equiv 1 \ (mod\ n)$$

Note: If k relatively prime to n then $k^{\phi(n)-1}$ is k^{-1}

RSA Public Key Encryption

 October 19, 2005 L7-1.13

Beforehand

- Receiver generates primes p,q
- $n=pq$ (so $\phi(n) = (p-1)(q-1)$)
- Selects e such that $gcd(e,(p-1)(q-1))=1$
  - e is public key, distributes e and n widely
- Computes d such that

  $de \equiv 1 \ (mod\ (p-1)(q-1))$
  - d is secret key, keeps it hidden

 October 19, 2005 L7-1.14

RSA

- Encoding: sender sends $m' = m^e \ rem\ n$
- Decoding: receiver decrypts as $m=(m')^d \ rem\ n$

 October 19, 2005 L7-1.15

Why does this work?

- Why is $(m')^d \ rem\ n = (m^e \ rem\ n)^d \ rem\ n$ the same as the original message?
  - Will see why in class problem 2

 October 19, 2005 L7-1.16

Is it secure?

- What notion of security? Against which kinds of attacks?
- Can we at least show that deciphering the message implies the ability to factor n?
  - We don't know how…
  - see homework problem

 October 19, 2005 L7-1.17

Class Problems

1 and 2

 October 19, 2005 L7-1.18