

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Number Theory III

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Permutation of a list

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

$$4, 1, 3, 2 \rightarrow 1, 2, 3, 4$$

$$10, 2, 14, 2 \rightarrow 14, 2, 10, 2$$

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Some interesting permutations

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



6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Last lecture's lemmas

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

1. k has a multiplicative inverse $\text{mod } p$

2. $ak \equiv bk \pmod{p} \Rightarrow a \equiv b \pmod{p}$

3. $(0 \cdot k) \text{ rem } p, (1 \cdot k) \text{ rem } p, \dots, ((p-1) \cdot k) \text{ rem } p$ is a permutation of the sequence $0, 1, \dots, p-1$

4. Fermat's theorem: $k^{p-1} \equiv 1 \pmod{p}$

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Working $(\text{mod } n)$ for composite n

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

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Relatively Prime Numbers

• a, b are relatively prime if $\text{gcd}(a, b) = 1$

• Examples:

– Not relatively prime:

• 2, 4

– Relatively prime:

• 9, 10

• p, k if p is a prime and k not a multiple of p

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Inverses mod n

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

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Cancellation

Corr: If k relatively prime to n then $ak \equiv bk \pmod{n} \Rightarrow a \equiv b \pmod{n}$

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Permutations

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

$(k_1 \cdot k) \pmod{n}, (k_2 \cdot k) \pmod{n}, \dots, (k_r \cdot k) \pmod{n}$ is a permutation of the sequence k_1, \dots, k_r

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Euler ϕ function

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

Examples:

$$\phi(7) = 6$$

$$1, 2, 3, 4, 5, 6$$

$$\phi(49) = 42$$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \dots$$

$$\phi(12) = 4$$

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

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Euler ϕ function

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

Theorem:

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

Examples:

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

$$1, 2, 3, 4, 5, 6$$

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

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \dots$$

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

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

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Euler's Theorem

If k relatively prime to n then $k^{\phi(n)} \equiv 1 \pmod{n}$



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

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

RSA Public Key Encryption



Copyright © Albert R. Meyer and Ronit Rubinfeld, 2005. All rights reserved.

October 19, 2005

L7-1.13

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

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
 - $de \equiv 1 \pmod{(p-1)(q-1)}$
 - d is **secret key**, keeps it hidden

Copyright © Albert R. Meyer and Ronit Rubinfeld, 2005. All rights reserved.

October 19, 2005

L7-1.14

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

RSA

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

Copyright © Albert R. Meyer and Ronit Rubinfeld, 2005. All rights reserved.

October 19, 2005

L7-1.15

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Why does this work?

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

Copyright © Albert R. Meyer and Ronit Rubinfeld, 2005. All rights reserved.

October 19, 2005

L7-1.16

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

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

Copyright © Albert R. Meyer and Ronit Rubinfeld, 2005. All rights reserved.

October 19, 2005

L7-1.17

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Class Problems 1 and 2

Copyright © Albert R. Meyer and Ronit Rubinfeld, 2005. All rights reserved.

October 19, 2005

L7-1.18