

Recall

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

Can add, subtract and multiply modulo n

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$$

If $a, b \in \mathbb{Z}_n^*$ then $ab \in \mathbb{Z}_n^*$.
(multiplication modulo n)

Can divide by the members of \mathbb{Z}_n^*

$$\phi(n) = |\mathbb{Z}_n^*|$$

In general can't add and subtract in \mathbb{Z}_n^*

© 2009 Clifford Bergman

A *group* is a pair $(G, *)$ in which:

1. G is a nonempty set
2. $*$ is a binary operation on G
3. $x * (y * z) = (x * y) * z$
4. There is $e \in G$ such that $x * e = e * x = x$
5. For every x there is x' with $x * x' = x' * x = e$.

© 2009 Clifford Bergman

Examples of groups

$(\mathbb{Z}, +)$ is a group with $e = 0$ and $x' = -x$.

$(\mathbb{Z}_n, +)$ is a group with $e = 0$ and $x' = -x \% n$

$(\mathbb{R} - \{0\}, \cdot)$ is a group with $e = 1$ and $x' = 1/x$

(\mathbb{Z}_n^*, \cdot) is a group with $e = 1$ and $x' = x^{-1} \% n$

© 2009 Clifford Bergman

Subgroups

Let $(G, *)$ be a group.

A nonempty subset H of G is called a **subgroup** if
 $a, b \in H \implies a * b \in H$ and $a' \in H$.

" H is closed in G ."

Remark: If G is finite, the condition ' $a' \in H$ ' can be dropped.

All of our groups will be finite

© 2009 Clifford Bergman

Example: $H = \{1, 6, 11, 16, 21\}$ is a subgroup of \mathbb{Z}_{25}^* .

·	1	6	11	16	21
1	1	6	11	16	21
6	6	11	16	21	1
11	11	16	21	1	6
16	16	21	1	6	11
21	21	1	6	11	16

© 2009 Clifford Bergman

Shorthand: $a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a, \dots$

$a^{-n} = (a^{-1})^n$ and $a^0 = e$.

Thus $a^n \cdot a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$

© 2009 Clifford Bergman

Let $a \in G$. $\langle a \rangle = \{e, a, a^2, a^3, \dots\}$.
Always a subgroup of G

Example: in \mathbb{Z}_{25}^* :
 $\langle 7 \rangle = \{1, 7, 24, 18\}$

The smallest positive integer k such that $a^k = e$ is the **order of a in G** . Write $\text{ord}_G(a)$.

Note: $\text{ord}_G(a) = |\langle a \rangle|$

If $G = \mathbb{Z}_n^*$, write ord_n instead of ord_G

© 2009 Clifford Bergman

Cosets

Suppose H is a subgroup of G and $a \in G$. Let
 $aH = \{ax : x \in H\}$. **coset of H by a**

Then:

$$|H| = |aH|,$$

$$a \in aH \text{ and}$$

$$\text{either } aH = bH \text{ or } aH \cap bH = \emptyset.$$

© 2009 Clifford Bergman

Example: In \mathbb{Z}_{25}^* :

$$H = \{1, 6, 11, 16, 21\}$$

$$2H = \{2, 12, 22, 7, 17\}$$

$$3H = \{3, 18, 8, 23, 13\}$$

$$4H = \{4, 24, 19, 14, 9\}$$

Note $6H = \{6, 11, 16, 21, 1\} = H$

© 2009 Clifford Bergman

Lagrange's Theorem: If H is a subgroup of G , then $|H|$ divides $|G|$.

Corollary: If G has prime order, then for every $a \in G - \{e\}$, $\langle a \rangle = G$.

When $\langle a \rangle = G$, we say that a is a *generator* of G .

© 2009 Clifford Bergman

In the special case that $G = \mathbb{Z}_n^*$ we get

Corollary: $\text{ord}_n(a)$ is a divisor of $\phi(n)$.

Theorem: Let $a \in \mathbb{Z}_n^*$. Then

$$a^r = a^s \iff r \equiv s \pmod{\text{ord}_n(a)}.$$

In particular, $r \equiv s \pmod{\phi(n)} \implies a^r = a^s$ for every a .

© 2009 Clifford Bergman

More corollaries of Lagrange

Euler's theorem: If $\text{gcd}(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Fermat's little theorem: If p is prime then for every a , $a^p \equiv a \pmod{p}$.

© 2009 Clifford Bergman

If $\langle a \rangle = \mathbb{Z}_n^*$, then a is called a **primitive element modulo n** .

Theorem: If p is an odd prime and $e \geq 1$, then there is a primitive element modulo p^e .

Modulo 25, $\langle 2 \rangle = \{2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13, 1\}$

Computing powers efficiently modulo n

Wish to compute $a^k \% n$

Naive algorithm:

```

d ← 1
for i ← 1 to k do
  d ← d * a % n
return(d)

```

Requires k multiplications and k divisions

Better:

powermod(a, k, n):

if ($k = 1$) then

 return(a)

if (k even) then

 return(powermod($a, k/2, n$)² % n)

else

 return($a * \text{powermod}(a, k - 1, n) \% n$)

Uses at most $2 \cdot \log_2(k)$ many multiplications and divisions.

Example: $6^{18} \% 50$

$$\begin{aligned} \text{pm}(6, 18, 50) &= \text{pm}(6, 9, 50)^2 \% 50 \\ &= 46^2 \% 50 = 16 \end{aligned}$$

$$\begin{aligned} \text{pm}(6, 9, 50) &= 6 \cdot \text{pm}(6, 8, 50) \% 50 \\ &= 6 \cdot 16 \% 50 = 46 \end{aligned}$$

$$\begin{aligned} \text{pm}(6, 8, 50) &= \text{pm}(6, 4, 50)^2 \% 50 \\ &= 46^2 \% 50 = 16 \end{aligned}$$

$$\begin{aligned} \text{pm}(6, 4, 50) &= \text{pm}(6, 2, 50)^2 \% 50 \\ &= 36^2 \% 50 = 46 \end{aligned}$$

$$\begin{aligned} \text{pm}(6, 2, 50) &= \text{pm}(6, 1, 50)^2 \% 50 \\ &= 6^2 \% 50 = 36 \end{aligned}$$

$$\text{pm}(6, 1, 50) = 6$$

Nonrecursive approach to $a^k \% n$

Let $b_t b_{t-1} \dots b_1 b_0$ be the binary representation of k .

```
 $d \leftarrow 1$   
for  $i \leftarrow t$  downto 0 do  
   $d \leftarrow d^2 \% n$   
  if  $(b_i = 1)$  then  
     $d \leftarrow d \cdot a \% n$   
return( $d$ )
```

“The square and multiply method”