15-251

Great Theoretical Ideas in Computer Science

Modular Arithmetic and the RSA Cryptosystem

Lecture 16 (October 18, 2007)

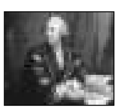
$^{p-1} \equiv_p 1$

Starring


Rivest


Shamir

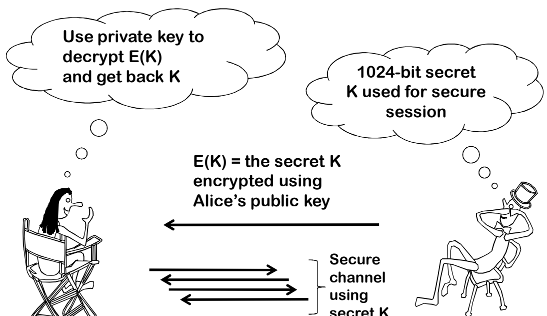

Adleman


Euler


Fermat

Public Key Cryptography

Public Key Cryptography

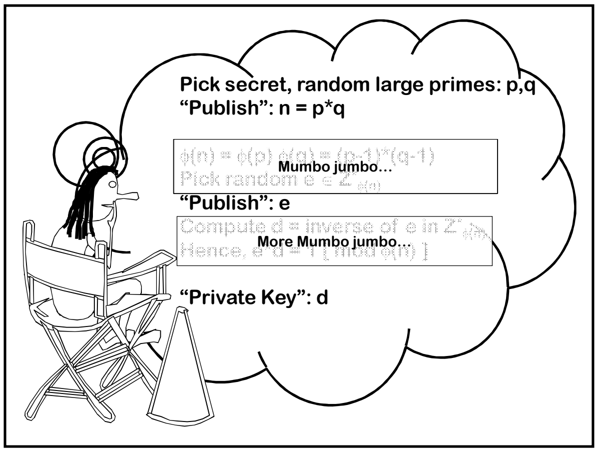


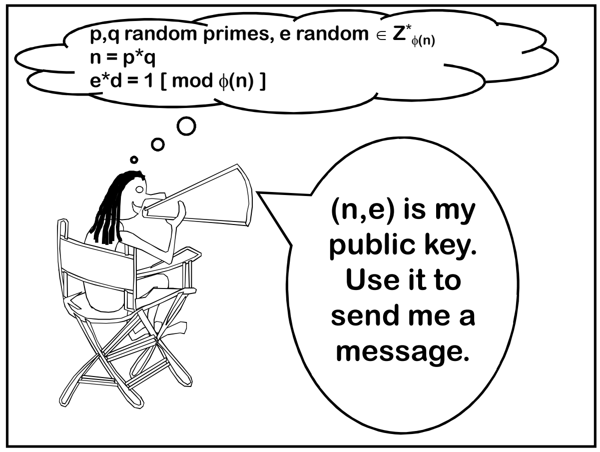
The RSA Cryptosystem

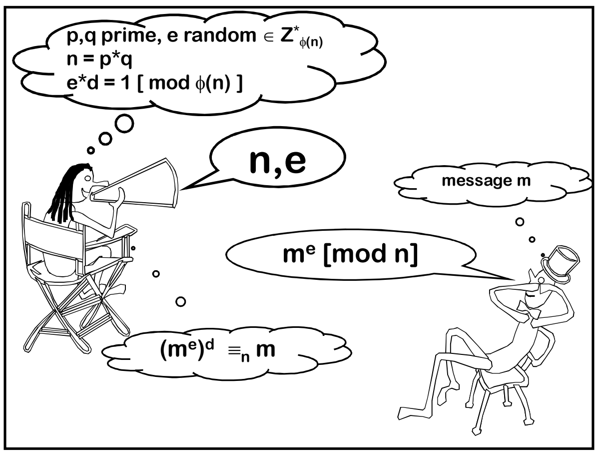
Rivest, Shamir, and Adelman (1978)

RSA is one of the most used cryptographic protocols on the net.

Your browser uses it to establish a secure session with a site.



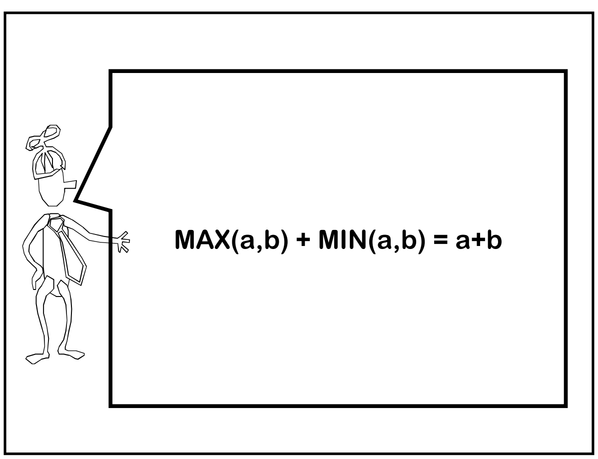


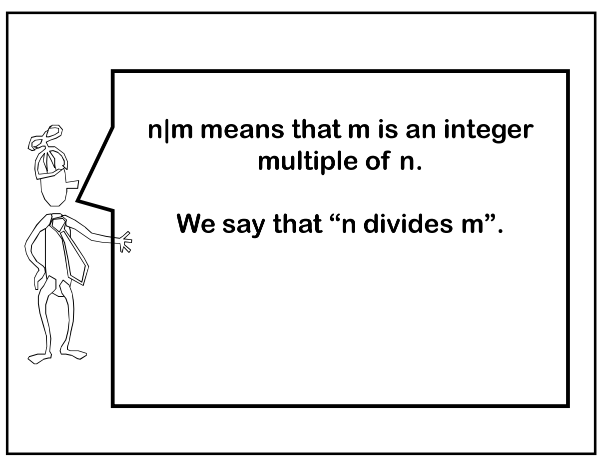


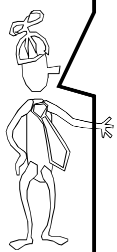
But how does it all work?

What is $\varphi(n)$?
What is $Z_{\varphi(n)}{}^*$?
…
Why do all the steps work?

To understand this, we need a little number theory…

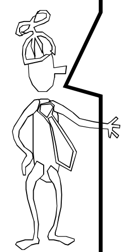






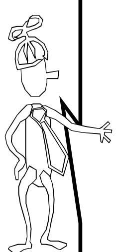
Greatest Common Divisor:
GCD(x,y) =
greatest k ≥ 1 s.t. k|x and k|y.

Least Common Multiple:
LCM(x,y) =
smallest k ≥ 1 s.t. x|k and y|k.



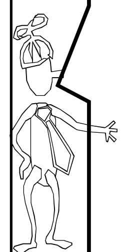
Fact:
GCD(x,y) × LCM(x,y) = x × y

You can use
MAX(a,b) + MIN(a,b) = a+b
to prove the above fact…



(a mod n) means the remainder when a is divided by n.

If a = dn + r with $0 \le r < n$
Then r = (a mod n)
and d = (a div n)



Defn: Modular equivalence of integers a and b
$a \equiv b$ [mod n]
$\Leftrightarrow$ (a mod n) = (b mod n)
$\Leftrightarrow$ n|(a-b)

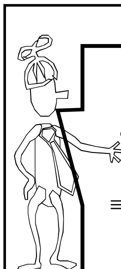
Written as $a \equiv_n b$, and spoken
"a and b are equivalent modulo n"

$31 \equiv 81$ [mod 2]
$31 \equiv_2 81$

$\equiv_n$ is an <u>equivalence relation</u>

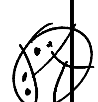
In other words, it is

Reflexive:
$a \equiv_n a$
Symmetric:
$(a \equiv_n b) \Rightarrow (b \equiv_n a)$
Transitive:
$(a \equiv_n b$ and $b \equiv_n c) \Rightarrow (a \equiv_n c)$

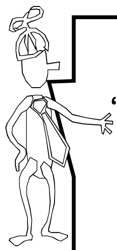


$a \equiv_n b \Leftrightarrow n|(a-b)$
"a and b are equivalent modulo n"

$\equiv_n$ induces a natural partition of the integers into n classes.



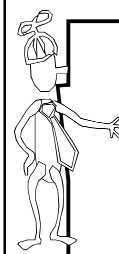
a and b are said to be in the same "residue class" or "congruence class" precisely when $a \equiv_n b$.



$a \equiv_n b \Leftrightarrow n|(a-b)$

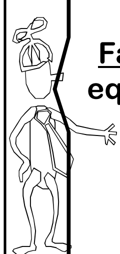
"a and b are equivalent modulo n"

Define
Residue class [i]
=
the set of all integers that are congruent to i modulo n.



Residue Classes Mod 3:

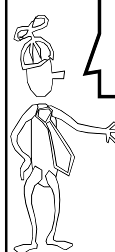
[0] = { …, -6, -3, 0, 3, 6, ..}
[1] = { …, -5, -2, 1, 4, 7, ..}
[2] = { …, -4, -1, 2, 5, 8, ..}
[-6] = { …, -6, -3, 0, 3, 6, ..}
[7] = { …, -5, -2, 1, 4, 7, ..}
[-1] = { …, -4, -1, 2, 5, 8, ..}



Fact: equivalence mod n implies equivalence mod any divisor of n.

If $(x \equiv_n y)$ and $(k|n)$
Then: $x \equiv_k y$

Example: $10 \equiv_6 16 \Rightarrow 10 \equiv_3 16$



If $(x \equiv_n y)$ and $(k|n)$
then $x \equiv_k y$

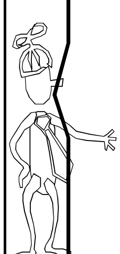
Proof:

$x \equiv_n y \Leftrightarrow n \mid (x-y)$

$k \mid n$

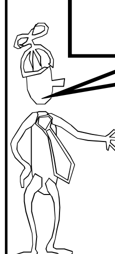
$\Downarrow$

$x \equiv_k y \Leftarrow k \mid (x-y)$



Fundamental lemma of
plus, minus, and times mod n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$. Then
1) $x + a \equiv_n y + b$
2) $x - a \equiv_n y - b$
3) $x * a \equiv_n y * b$



Proof of 3: xa = yb (mod n)

(The other two proofs are similar…)

Fundamental lemma of plus minus, and times modulo n:

When doing plus, minus, and times modulo n, I can at any time in the calculation replace a number with a number in the same residue class modulo n

Please calculate: 249 * 504 mod 251

when working mod 251

-2 * 2 = -4 = 247

A Unique Representation System Modulo n:

We pick exactly one representative from each residue class.

We do all our calculations using these representatives.

Unique representation system modulo 3

Finite set S = {0, 1, 2}

+ and * defined on S:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Unique representation system modulo 3

Finite set S = {0, 1, -1}

+ and * defined on S:

+	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

*	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

Perhaps the most convenient set of representatives:

The reduced system modulo n:

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Define operations $+_n$ and $*_n$:

$a +_n b = (a+b \bmod n)$
$a *_n b = (a*b \bmod n)$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a +_n b = (a+b \bmod n)$ $a *_n b = (a*b \bmod n)$

[Closed]

$x, y \in Z_n \Leftrightarrow x +_n y \in Z_n$

[Associative]

$x, y, z \in Z_n$, then $(x +_n y) +_n z = x +_n (y +_n z)$

[Commutative] then

$x, y \in Z_n \cancel{\Leftrightarrow}$ $x +_n y = y +_n x$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a +_n b = (a+b \bmod n)$ $a *_n b = (a*b \bmod n)$

[Closed]

$x, y \in Z_n \Leftrightarrow x *_n y \in Z_n$

[Associative]

$x, y, z \in Z_n$, then $(x *_n y) *_n z = x *_n (y *_n z)$

[Commutative]

$x, y \in Z_n$ then $x *_n y = y *_n x$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a +_n b = (a+b \bmod n)$ $a *_n b = (a*b \bmod n)$

$+_n$ and $*_n$ are

commutative and associative

binary operators from $Z_n * Z_n \rightarrow Z_n$

The reduced system modulo 3

$Z_3 = \{0, 1, 2\}$

Two binary, associative operators on Z_3:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

The reduced system modulo 2

$Z_2 = \{0, 1\}$

Two binary, associative operators on Z_2:

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1

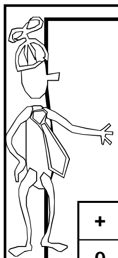
The Boolean interpretation of Z_2

$Z_2 = \{0, 1\}$

Two binary, associative operators on Z_2:

$+_2$ XOR	0	1
0	0	1
1	1	0

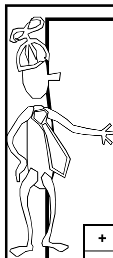
$*_2$ AND	0	1
0	0	0
1	0	1



The reduced system
$Z_4 = \{0,1,2,3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

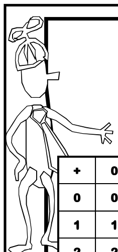
*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1



The reduced system
$Z_5 = \{0,1,2,3,4\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

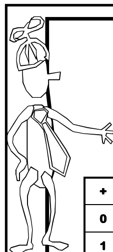
*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1



The reduced system
$Z_6 = \{0,1,2,3,4,5\}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

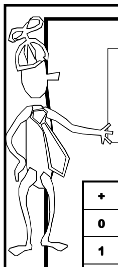
*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1



The reduced system
$Z_6 = \{0,1,2,3,4,5\}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

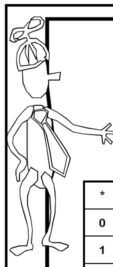
An operator has the permutation property if each row and each column has a permutation of the elements.



For every n, $+_n$ on Z_n has the permutation property

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

An operator has the permutation property if each row and each column has a permutation of the elements.



What about multiplication? Does $*_6$ on Z_6 have the permutation property?

No

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

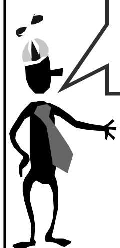
An operator has the permutation property if each row and each column has a permutation of the elements.

What about $*_8$ on Z_8?

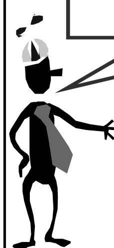
*	0	1	2	3	4	5	6	7
0								
1								
2								
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5								
6	0	6	4	2	0	6	4	2
7								

Which rows have the permutation property?

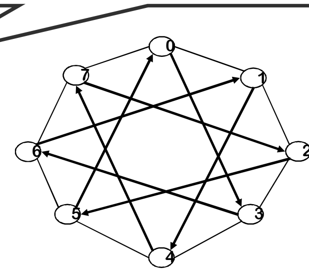
A visual way to understand multiplication and the "permutation property".



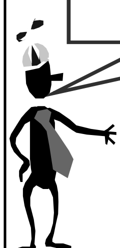
The multiples of c modulo n is the set:
$\{0, c, c +_n c, c +_n c +_n c, \ldots.\}$
$= \{kc \bmod n \mid 0 \le k \le n-1\}$



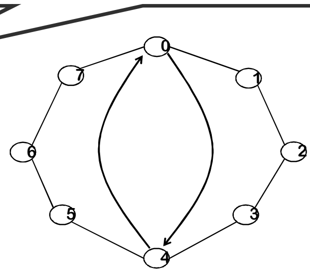
There are exactly 8 distinct multiples of 3 modulo 8.



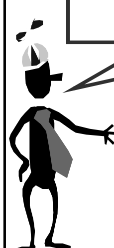
hit all numbers ⇔ row 3 has the "permutation property"



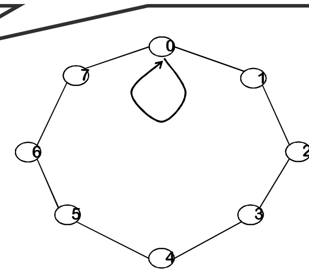
There are exactly 2 distinct multiples of 4 modulo 8

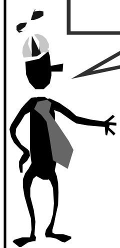


row 4 does not have "permutation property" for $*_8$ on Z_8

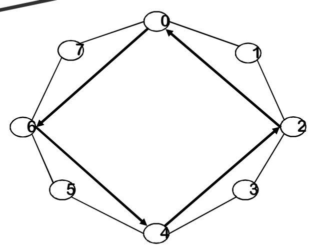


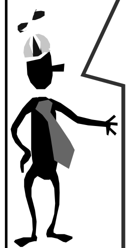
There is exactly 1 distinct multiple of 8 modulo 8





There are exactly 4 distinct multiples of 6 modulo 8





There are exactly
LCM(n,c)/c = n/GCD(c,n)
distinct multiples of c modulo n

hence

only those values of c
with GCD(c,n) = 1
have the permutation property
for $*_n$ on Z_n

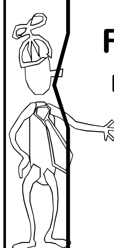
Theorem: There are exactly k = n/GCD(c,n) = LCM(c,n)/c distinct multiples of c modulo n, and these are
$\{ c*i \bmod n \mid 0 \le i < k \}$

Proof:
Clearly, c/GCD(c,n) ≥ 1 is a whole number

$ck = cn/GCD(c,n) = n(c/GCD(c,n)) \equiv_n 0$

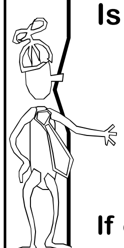
$\Rightarrow$ There are ≤ k distinct multiples of c mod n:
c*0, c*1, c*2, …, c*(k-1)

Also, k = all the factors of n missing from c
$\Rightarrow cx \equiv_n cy \Leftrightarrow n|c(x-y) \Rightarrow k|(x-y) \Rightarrow x-y \ge k$
There are ≥ k multiples of c. Hence exactly k.



Fundamental lemma of plus, minus, and times modulo n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$. Then
1) $x + a \equiv_n y + b$
2) $x - a \equiv_n y - b$
3) $x * a \equiv_n y * b$

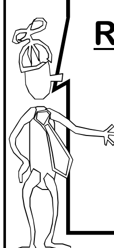


Is there a fundamental lemma of division modulo n?

$cx \equiv_n cy \Rightarrow x \equiv_n y$?

Of course not!
If c=0[mod n], $cx \equiv_n cy$ for all x and y.

Canceling the c is like dividing by zero.

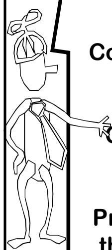


Let's fix that! Repaired fundamental lemma of division modulo n?

if $c \neq 0$ [mod n], then
$cx \equiv_n cy \Rightarrow x \equiv_n y$?

$6*3 \equiv_{10} 6*8$, but not $3 \equiv_{10} 8$.
$2*2 \equiv_6 2*5$, but not $2 \equiv_6 5$.

Bummer!



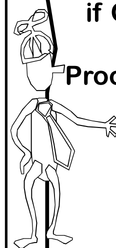
When can't I divide by c?

Theorem: There are exactly n/GCD(c.n) distinct multiples of c modulo n.

Corollary: If GCD(c,n) > 1, then the number of multiples of c is less than n.

Corollary: If GCD(c,n) > 1 then you can't always divide by c.

Proof: There must exist distinct x,y<n such that c*x=c*y (but $x \neq y$). Hence cant divide.

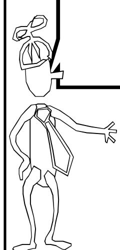


Fundamental lemma of division modulo n:
if GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Proof: $ca \equiv_n cb \Leftrightarrow n \mid c(a-b)$

but $\gcd(c,n)=1$

$\Rightarrow n \mid a-b \Rightarrow a \equiv_n b$.



Corollary for general c:
$cx \equiv_n cy \Rightarrow x \equiv_{n/GCD(c,n)} y$

$n \mid cx - cy = c(x-y)$

$$\frac{n}{\gcd(c,n)} \;\Big|\; \frac{c}{\gcd(c,n)}(x-y)$$

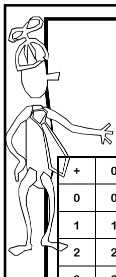
$$\Rightarrow \quad x \equiv y \left(\bmod \frac{n}{\gcd(c,n)}\right)$$

Fundamental lemma of division modulo n.
If GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Consider the set

$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$

Multiplication over this set Z_n^* will have the cancellation property.



$Z_6 = \{0, 1,2,3,4,5\}$
$Z_6^* = \{1,5\}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

What are the properties of Z_n^*

For $*_n$ on Z_n we showed the following properties:

[Closure]
$x, y \in Z_n \Rightarrow x *_n y \in Z_n$

[Associativity]
$x, y, z \in Z_n \Rightarrow (x *_n y) *_n z = x *_n (y *_n z)$

[Commutativity]
$x, y \in Z_n \Rightarrow x *_n y = y *_n x$

What about $*_n$ on Z_n^*?

All these 3 properties hold for $*_n$ on Z_n^*.

Let's show "closure": $x,y \in Z_n^* \Rightarrow x *_n y \in Z_n^*$

First, a simple fact:

Suppose GCD(x,n) = 1 and GCD(y,n) = 1

Let z = xy. Clearly, GCD(z, n) = 1.

Also, define z' = (xy mod n). Then GCD(z',n)=1

All these 3 properties hold for $*_n$ on Z_n^*.

Let's show "closure": $x,y \in Z_n^* \Rightarrow x *_n y \in Z_n^*$

Proof:
Let z = xy. Let z' = z mod n. Then z = z' + kn.
Suppose z' not in Z_n*. Then GCD(z', n) > 1.
and hence GCD(z, n) > 1.
Hence there exists a prime p>1 s.t. p|z' and p|n.
$p|z \Rightarrow p|x$ or $p|y$. (say p|x)
Hence p|n, p|x, so GCD(x,n) > 1.
Contradiction of $x \in Z_n^*$

$Z_{12}^* = \{0 \le x < 12 \mid \gcd(x,12) = 1\}$
$= \{1,5,7,11\}$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Z_{15}^*

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

$Z_5^* = \{1,2,3,4\}$ $\boxed{= Z_5 \setminus \{0\}}$

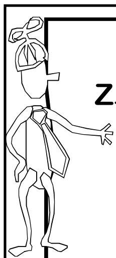
$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

For all primes p, $Z_p^* = Z_p \setminus \{0\}$,
since all 0 < x < p satisfy gcd(x,p) = 1

Euler Phi Function $\phi(n)$

Define $\phi(n)$ =
size of Z_n^* =
number of $1 \le k < n$ that
are relatively prime to n.

p prime $\Rightarrow Z_p^* = \{1,2,3,\ldots,p-1\}$
$\Rightarrow \Phi(p) = p-1$



$Z_{12}^* = \{0 \le x < 12 \mid \gcd(x,12) = 1\}$
$= \{1,5,7,11\}$

$\boxed{\phi(12) = 4}$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

p prime $\Rightarrow \phi(p) = p-1$.

Theorem: if p,q distinct primes then
$\phi(pq) = (p-1)(q-1)$

How about p = 3, q = 5?

1, 2, , 4, ,
7, 8, 11, 13, 14

$\phi(15) = 8$

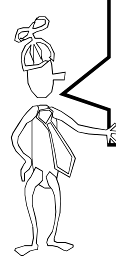
absent: $\left\{ \begin{array}{l} 3, 6, 9, 12, 15 \leftarrow \text{5 values} \\ 5, 10, 15 \leftarrow \text{3 values} \end{array} \right.$

$15 - 3 - 5 + 1 = 8$.

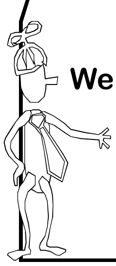
Theorem: if p,q distinct primes then
$\phi(pq) = (p-1)(q-1)$

pq = # of numbers from 1 to pq
p = # of multiples of q up to pq
q = # of multiples of p up to pq
1 = # of multiple of <u>both</u> p and q up to pq

$\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$



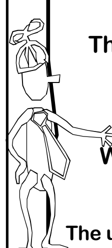
Additive and Multicative Inverses



The additive inverse of $a \in Z_n$ is the unique $b \in Z_n$ such that $a +_n b \equiv_n 0$.

We denote this inverse by "–a".

It is trivial to calculate: "-a" = (n-a).

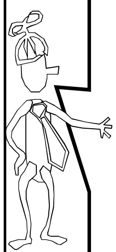


The multiplicative inverse of $a \in Z_n^*$ is the unique $b \in Z_n^*$ such that $a *_n b \equiv_n 1$.

We denote this inverse by "a^{-1}" or "1/a".

The unique inverse of "a" must exist because the "a" row contains a permutation of the elements and hence contains a unique 1.

*	1	b	3	4
1	1	2	3	4
2	2	4	1	3
a	3	1	4	2
4	4	3	2	1



Efficient algorithm to compute a^{-1} from a and n.

Run Extended Euclidean Algorithm on the numbers a and n.

It will give two integers r and s such that ra + sn = gcd(a,n) = 1

Taking both sides modulo n, we obtain: $ra \equiv_n 1$

Output r, which is the inverse of a

Euclid(A,B)
If B=0 then return A
else return Euclid(B, A mod B)

Euclid(67,29)	67 – 2*29 = 67 mod 29 = 9
Euclid(29,9)	29 – 3*9 = 29 mod 9 = 2
Euclid(9,2)	9 – 4*2 = 9 mod 2 = 1
Euclid(2,1)	2 – 2*1 = 2 mod 1 = 0
Euclid(1,0) outputs 1	

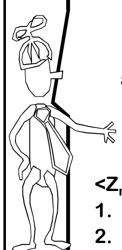
Extended Euclid Algorithm

Let <r,s> denote the number r*67 + s*29. Calculate all intermediate values in this representation.

67=<1,0>   29=<0,1>

Euclid(67,29)	9=<1,0> – 2*<0,1>	9 =<1,-2>
Euclid(29,9)	2=<0,1> – 3*<1,-2>	2=<-3,7>
Euclid(9,2)	1=<1,-2> – 4*<-3,7>	1=<13,-30>
Euclid(2,1)	0=<-3,7> – 2*<13,-30>	0=<-29,67>

Euclid(1,0) outputs   1 = 13*67 – 30*29



$Z_n = \{0, 1, 2, \ldots, n-1\}$
$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$

Define $+_n$ and $*_n$:

$a +_n b = (a+b \bmod n)$ $a *_n b = (a*b \bmod n)$

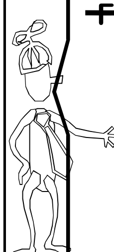
$c *_n (a +_n b) \equiv_n (c *_n a) +_n (c *_n b)$

$\langle Z_n, +_n\rangle$	$\langle Z_n^*, *_n\rangle$
1. Closed	1. Closed
2. Associative	2. Associative
3. 0 is identity	3. 1 is identity
4. Additive Inverses	4. Multiplicative Inverses
5. Cancellation	5. Cancellation
6. Commutative	6. Commutative

Fundamental Lemmas until now

For x, y, a, b in Z_n, $(x \equiv_n y)$ and $(a \equiv_n b)$. Then
1) $x + a \equiv_n y + b$
2) $x - a \equiv_n y - b$
3) $x * a \equiv_n y * b$

For a,b,c in Z_n^*
then $ca \equiv_n cb \Rightarrow a \equiv_n b$



~~Fundamental lemma of powers?~~

If $(a \equiv_n b)$
Then $x^a \equiv_n x^b$? $a \equiv_{\Phi(n)} b$

NO!

$(2 \equiv_3 5)$, but it is not the case that: $2^2 \equiv_3 2^5$

By the permutation property, two names for the same set:

$Z_n^* = aZ_n^*$

where
$aZ_n^* = \{a *_n x \mid x \in Z_n^*\},\ a \in Z_n^*$

Example: Z_5^*

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
a	3	1	4	2
4	4	3	2	1

Two products on the same set:

$Z_n^* = aZ_n^*$

$aZ_n^* = \{a *_n x \mid x \in Z_n^*\},\ a \in Z_n^*$

$\prod x \equiv_n \prod ax$ [as x ranges over Z_n^*]

$\prod x \equiv_n \prod x\ (a^{\text{size of } Zn^*})$ [Commutativity]

$1 = a^{\text{size of } Zn^*}$ [Cancellation]

$a^{\Phi(n)} = 1$ (mod n)

Euler's Theorem

$a \in Z_n^*,\ a^{\Phi(n)} \equiv_n 1$

Fermat's Little Theorem

p prime, $a \in Z_p^* \Rightarrow a^{p-1} \equiv_p 1$

(Correct) Fundamental lemma of powers.

Suppose $x \in Z_n^*$, and a,b,n are naturals.

If $a \equiv_{\Phi(n)} b$ Then $x^a \equiv_n x^b$

Equivalently,
$x^a \equiv_n x^{a \bmod \Phi(n)}$

How do you calculate

$2^{\underbrace{4444444441}}$ mod 5

Fundamental lemma of powers.

Suppose $x \in Z_n^*$, and a,n are naturals.

$x^a \equiv_n x^{a \bmod \Phi(n)}$

$\underbrace{4444444441}_{a}$, mod 4 = $\Phi(5)$

= 1 mod 4

$a \equiv_{\Phi(5)} 1$.

$2^a \equiv 2^1$ (mod 5)

= 2

$\boxed{x^a \pmod n = x^{a \bmod \Phi(n)} \pmod n}$

Defining negative powers

Suppose $x \in Z_n^*$, and a,n are naturals.

x^{-a} is defined to be the multiplicative inverse of x^a

$x^{-a} = (x^a)^{-1}$

Rule of integer exponents

Suppose $x,y \in Z_n^*$, and a,b are integers.

$(xy)^{-1} \equiv_n x^{-1}\, y^{-1}$

$X^a X^b \equiv_n X^{a+b}$

Can use Lecture 13 to do fast exponentiation!

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$

$\langle Z_n, +_n \rangle$	$\langle Z_n^*, *_n \rangle$
1. Closed	1. Closed
2. Associative	2. Associative
3. 0 is identity	3. 1 is identity
4. Additive Inverses Fast + and -	4. Multiplicative Inverses Fast * and /
5. Cancellation	5. Cancellation
6. Commutative	6. Commutative

Fundamental lemma of powers.

Suppose $x \in Z_n^*$, and a,b,n are naturals.

If $a \equiv_{\Phi(n)} b$ Then $x^a \equiv_n x^b$

Equivalently,
$x^a \equiv_n x^{a \bmod \Phi(n)}$

Euler Phi Function

$\Phi(n)$ = size of Z_n^*

p prime $\Rightarrow Z_p^* = \{1,2,3,\ldots,p-1\}$
$\Rightarrow \phi(p) = p-1$

$\phi(pq) = (p-1)(q-1)$
if p,q distinct primes

Back to our dramatis personae


Rivest

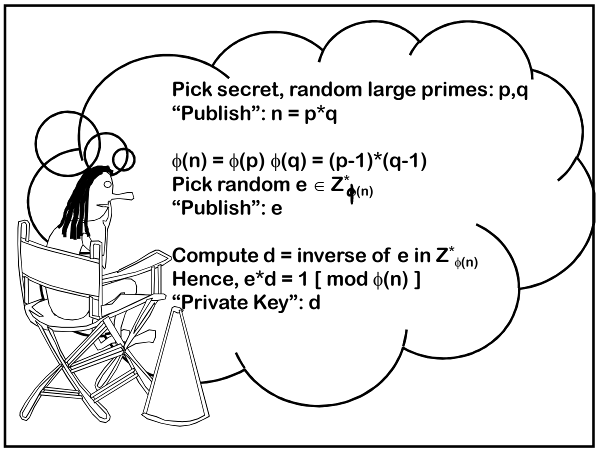

Shamir


Adleman


Euler

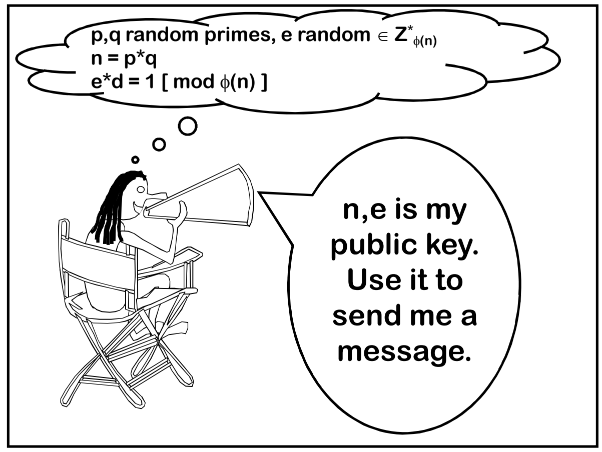

Fermat

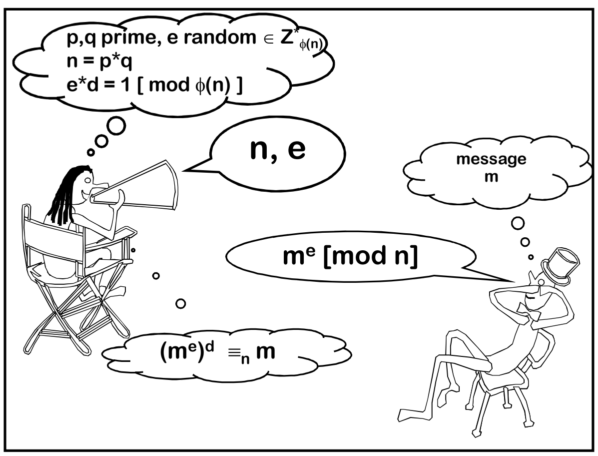
The RSA Cryptosystem

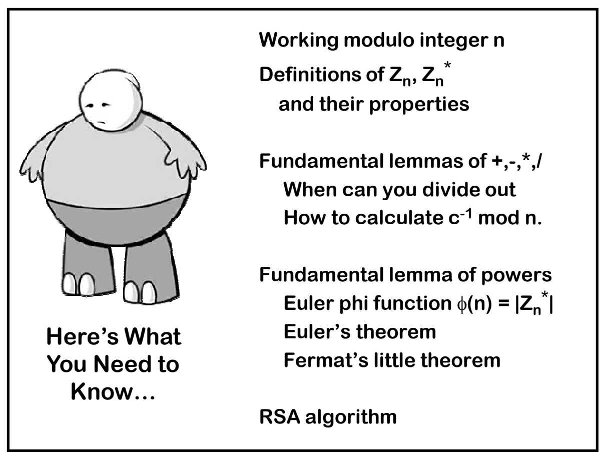

Pick secret, random large primes: p,q
"Publish": n = p*q

$\phi(n) = \phi(p)\ \phi(q) = (p-1)*(q-1)$
Pick random $e \in Z^*_{\phi(n)}$
"Publish": e

Compute d = inverse of e in $Z^*_{\phi(n)}$
Hence, e*d = 1 [mod $\phi(n)$]
"Private Key": d


p,q random primes, e random $\in Z^*_{\phi(n)}$
n = p*q
e*d = 1 [mod $\phi(n)$]
n,e is my public key. Use it to send me a message.


p,q prime, e random $\in Z^*_{\phi(n)}$
n = p*q
e*d = 1 [mod $\phi(n)$]
n, e
message m
m^e [mod n]
$(m^e)^d \equiv_n m$


Here's What You Need to Know…
Working modulo integer n
Definitions of Z_n, Z_n^*
and their properties

Fundamental lemmas of +,-,*,/
When can you divide out
How to calculate c^{-1} mod n.

Fundamental lemma of powers
Euler phi function $\phi(n) = |Z_n^*|$
Euler's theorem
Fermat's little theorem

RSA algorithm