Prep for El Gamal (Towards Primitive Roots)

- By Fermat: If n is prime and $n \nmid a$
  $a^{n-1} \equiv 1 \bmod n$
- By Euler: For integers a, n,
  $\gcd(a,n) = 1, \; n \geq 1$
  $a^{\phi(n)} \equiv 1 \bmod n$

We can do better. Sometimes

$a^k \equiv 1 \bmod n, \quad k < \phi(n)$

Def. Order of an integer, a, mod n

Let $n > 1$ and $\gcd(a,n) = 1$.
The order of a mod n is the smallest positive integer, k,
s.t. $a^k \equiv 1 \bmod n$

Ex

$2^1 \equiv 2 \bmod 7$
$2^2 \equiv 4 \bmod 7$
$2^3 \equiv 1 \bmod 7$ 2 has order 3 mod 7
$2^4 \equiv 2 \bmod 7$
$2^5 \equiv 4 \bmod 7$
$2^6 \equiv 1 \bmod 7$ $\phi(7) = 6$

Notice

$2 \equiv 9 \mod 7$ b.c $2 - 9 = -1 \cdot 7$

We know $2^3 \equiv 1 \mod 7$

As it happen

$9^3 \equiv 1 \mod 7$

Leads to order/cong. Th

if $a \equiv b \mod 7$ and

a has order $k \mod n$ then
b has order $k \mod n$

Proof

By Prop 9 cong.

if $a \equiv b \mod n$
$a^k \equiv b^k \mod n$ $\forall\, k \in \mathbb{Z}^+$

Since $a^k \equiv 1 \mod n$ and
$a^k \equiv b^k \mod n$ then

$b^k \equiv 1 \mod n$

Shortcut th. (to find order a mod n)

* Let a have order k mod n then
$a^h \equiv 1 \bmod n$ iff $k \mid h$;
in particular $k \mid \phi(n)$

Pf

(A) a has order k mod n so $a^k \equiv 1 \bmod n$
if $k \mid h$ then, $a^h \equiv 1 \bmod n$

Ex
2 has order 3 mod 7
($2^3 \equiv 1 \bmod 7$)

$2 \mid 6$
so $2^6 \equiv 1 \bmod 7$

proof

$k \mid h \Rightarrow h = jk$ for some integer, j

$a^k \equiv 1 \bmod n$ by assumption

so $(a^k)^j \equiv 1^j \bmod n$ by prop of cong.

$a^{kj} = a^h \equiv 1 \bmod n$

(B) if $a^h \equiv 1 \mod n$ then

$k \mid h$

By DA h may be written

$h = qk + r \quad 0 \leq r < k$

$a^h = a^{qk+r} = (a^k)^q a^r$

Since $a^k \equiv 1 \mod n$ by assumption

$a^h \equiv a^r \mod 7$

but $a^h \equiv 1 \mod 7$

so

$a^r \equiv 1 \mod 7$

but a was mod order k mod n

since $0 \leq r < k$

$\therefore r > 0$ would contradict as assumption of k as smallest positive integer s.t. $a^k \equiv 1 \mod n$

so $r = 0$

and if $r = 0$, $h = qk$ and $k \mid h$

Finally

if $n > 1$ and $\gcd(a, n) = 1$
a has order $k \bmod n$ if
$a^k \equiv 1 \bmod n$

We've shown

if $a^k \equiv 1 \bmod n$ and k has order
$a \bmod n$ $k \mid h$ if $a^h \equiv 1 \bmod n$

Since by Euler if $n > 1$ and $\gcd(a, n) = 1$

$$a^{\phi(n)} \equiv 1 \bmod n$$

By the short-cut th.

$$k \mid \phi(n)$$

To find k,
Consider only candidates that divide $\phi(n)$

Ex Find order 2 mod 13

$\phi(13) = 12$

Consider only
1, 2, 3, 4, 6, 12

$2^1 \equiv 2 \mod 13$
$2^2 \equiv 4 \mod 13$
$2^3 \equiv 8 \mod 13$
$2^4 \equiv 3 \mod 13$
$2^6 \equiv 12 \mod 13$
$2^{12} \equiv 1 \mod 13$

2 has order 12 mod 13

Find order 3 mod 31

Python: ord = [(i, 3^{**i} %31) for i in range(1,32)]

Sage: mod(3,31).multiplicative_order()

Th. Order and Exponentiation

if a has order k mod n

$a^i \equiv a^j \bmod n$ iff

$i \equiv j \bmod k$

Ex a has order k mod n | 2 has order 12 mod 13 |

We know $3 \equiv 2$

$$3^i \equiv 2^j \bmod 12^k$$

$$3^{6i} \equiv 2^{4j} \bmod 13^n$$

Proof

(A) if $a^i \equiv a^j \bmod n$ then $i \equiv j \bmod k$

Proof

Suppose $i \geq j$,

i.e. $\gcd(a,n) = 1$ we can mult. by Mult. Inv. a^j $(a^j)^{-1}$

$$a^i \equiv a^j \bmod n$$

$$a^i \cdot a^{-j} \equiv 1 \bmod n$$

$$a^{i-j} \equiv 1 \bmod n$$

Since a has order k mod n by assumption, the shortcut

Tells us

$k \mid i - j$

By Def of cong

$i \equiv j \bmod k$

B if $i \equiv j \bmod k$ then $a^i \equiv a^j \bmod n$

$i - j = qk$ Def of cong.

$i = qk + j$

$a^k \equiv 1 \bmod n$ since a has order $k \bmod n$ by assumption

$a^i = a^{qk+j}$

$\equiv a^{qk+j} \bmod n$

$\equiv a^j (a^k)^q \bmod n$

$\equiv a^j$

QED claimed

Corollary TO order and exp. Th.

* (if a has order k mod n

$a^i \equiv a^j \pmod n$ iff

$i \equiv k \pmod n$)

if a has order k mod n then integers $a^1, a^2, \ldots, a^k$ are mutually incongruent mod n

Proof

Suppose $a^i \equiv a^j \pmod n$, $i \leq j \leq k$

Then by the theorem $i \equiv j \pmod k$ but this is impossible unless $i = j$.

- Order and GCD theorem (Burton p. 159)
if integer a, has order k mod n and $h > 0$ then a^h has order $k / \gcd(h,k)$ mod n

proof.

Let $d = \gcd(h_1, k_2) \Rightarrow h = h_1 d$, $k = k_1 d$, with $\gcd(h_1, k_1) = 1$.
Then $(a^h)^{k_1} = (a^k)^{h_1} \equiv 1 \pmod n$ by def. order
Assume a^h has order r mod n. By the shortcut th. $r \mid k_1$ and $(a^h)^r \equiv 1 \pmod n$
Do by shortcut $k \mid hr$
To Sum: $h = h_1 d$, $k = k_1 d$, $r \mid k_1$, $k \mid hr$
So $k_1 d \mid h_1 rd$ and $k_1 \mid h_1 r$. Since $\gcd(k_1, h_1) = 1$,
$k_1 \mid r$ Since $r \mid k_1$ and $k_1 \mid r$ $r = k_1$

$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h,k)}$. Since a^h has order r mod n. This proves the theorem.

Primitive Root
— special case of order

Order
if $n \geq 1$, $\gcd(a, n) = 1$
Order of a mod n is the
smallest integer k s.t.
$a^k \equiv 1 \bmod n$

if $k = \phi(n)$
a is said to be a
primitive root of n

Ex 3 is a primitive root of 7

$\gcd(3, 7) = 1$

$\phi(7) = 6$

Recall Short-cut th. Tells us to consider only non-trivial divisors of $\phi(n)$

those are 2, 3, 6

$3^2 \equiv 2 \bmod 7$
$3^3 \equiv 6 \bmod 7$
$3^6 \equiv 1 \bmod 7$
$3^{\phi(7)} \equiv 1 \bmod 7$

3 is a primitive root of 7

Primitive Root Theorem

Let $\gcd(a,n) = 1$

Let $A = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ be the positive integers $\leq n$ that are relatively prime to n

If a is a primitive root of n then

$a^1, a^2, \ldots, a^{\phi(n)}$ are congruent mod n to elts of a Taken in some order

Ex

$a = 2 \quad n = 9$

$\gcd(2,9) = 1, \quad \phi(9) = 6 : \{1,2,4,5,7,8\} = A$

$2^1 \equiv 2 \mod 9$

$2^2 \equiv 4 \mod 9$

$2^3 \equiv 8 \mod 9$

$2^4 \equiv 7 \mod 9$

$2^5 \equiv 5 \mod 9$

$2^6 \equiv 1 \mod 9$

Proof

$\gcd(a,n)=1 \Rightarrow \gcd(a^i, n)=1, \quad i \geq 1$

Let $A = \{a_1, a_2, \ldots, a_{\phi(n)}\}$

$B = \{a^1, a^2, \ldots, a^{\phi(n)}\}$

GCD Th:
if $a = qn+r$

$\gcd(a,n) = \gcd(n,r)$

By Div. Alg, each a^i in B may be written

$a^i = qn+r \quad 0 \leq r < q$

Then

$a^i - r = qn$ and

$a^i \equiv r \bmod n$

By GCD th.

$\gcd(a^i, n) = \gcd(n,r)$

but $\gcd(a^i, n) = 1$

so $\gcd(n,r) = 1$

Since A is the set of integers $< n$ relatively prime to n

$r \in A$

So

each $a_i \in B$ is congruent to some $r \in A$

We claim more: namely elts in B map 1-1 to elts in A

By the Corollary, if a has order k mod n, $a^1, a^2, \ldots, a^k$ are mutually incongruent mod n

So if each $a_i \in B$ is cong. to a (a corresponding $a_i \in A$ and each a_i is incongruent to each a^i

the elts of B are congruent to the elts of A taken in some order

Counting th.

if n has a primitive root

There are $\phi(\phi(n))$ of them

Ex $\phi(9) = 6$ $\{1,2,4,5,7,8\}$

$\phi(6) = 2$ $\{1,5\}$

By magic the two primitive roots are 2, 5

$\phi(9) = 6$

$2^6 \equiv 64 \equiv 1 \bmod 9$

$5^6 = 15625 \equiv 1 \bmod 9$

Proof

Let a be a prim. rt. $\bmod n$

then $a \in \{a_1, a_2, \ldots, a_{\phi(n)}\} = A$

By the prim rt th,

a is cong. to some element in $B = \{a^1, a^2, \ldots, a^{\phi(n)}\}$

Prove this in the future

Lemma (Burton p 159)

Let a have order k mod n
Then a^h also has order k mod n
iff $\gcd(h,k)=1$

Counting theorem

if n has a primitive root,
there are $\phi(\phi(n))$ of them

Proof

by the Primitive Root theorem

The Prim. Rt. of n is found in
$\{a^1, a^2, \ldots, a^{\phi(n)}\}$

By the lemma any such Prim. Rt., a^k,
$1 \le k \le \phi(n)$ must have
$\gcd(k, \phi(n)) = 1$ (i.e. $\phi(n)$ is the order)

There are $\phi(n)$ ints, a, s.t.
$\gcd(a,n)=1$,

$\Rightarrow$ there are $\phi(\phi(n))$ ints, k,
s.t. $\gcd(k, \phi(n)) = 1$

$\{k_1, k_2, \ldots, k_{\phi(n)}\}$

$k_1 = 1$

if n is prime

$$\phi(\phi(n)) = \phi(n-1)$$

primitive roots:

Find primitive roots of 11.

$\phi(\phi(11)) = \phi(10) = 4$

Candidates

$1 \leq a < 11$ & $\gcd(a, 11) = 1$

$a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

4 of those are primitive roots

T.S.C. th. 8049

if a has order k

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

if $k \mid \phi(n)$

$a^{\phi(n)} = 1$, but a has order k if ~~$k \neq \phi(n)$~~

i.e the smallest value

s.t. $a^k \equiv 1 \mod n$ and $k \neq \phi(n)$

and a is not a prim rt.

Test if a is a prim. Rt of n

(A) gcd(a, n) = 1

(B) Find all factors, d, of $\phi(n)$

(C) For all factors

if $a^{\phi(n)/d} \not\equiv 1 \bmod n$

a is a primitive root

Return to Example

Factors of 10

$10 = 2 \cdot 5$

X $1^{10/2} \equiv 1 \bmod 11$

$2^{10/2} \equiv 2 \bmod 11$
$2^{10/5} \equiv 4 \bmod 11$ } Pr. Rt.

X $3^{10/2} \equiv 1 \bmod 11$

X $4^{10/2} \equiv 1 \bmod 11$

X $5^{10/2} \equiv 1 \bmod 11$

$6^{10/2} \equiv 2$ " "
$6^{10/5} \equiv 5$ " " } Pr Rt

$7^{10/2} \equiv 10 \bmod 11$

$7^{10/5} \equiv 5 \bmod 11$) Pr RT

$8^{10/2} \equiv 10 \bmod 11$

$8^{10/5} \equiv 9 \bmod 11$) Pr RT

X $9^{10/5} \equiv 1 \bmod 11$

$10^{10/5} \equiv 1 \bmod 11$

So 11 has primitive roots 2, 4, 7, 8

Notice

Tests Require factorization of $\phi(n)$ which is hard.

Primitive roots are hard to find

basis of El Gamal

El Gamal

- Security rests on the Discrete log problem

Exponentiation:
- $a^x \equiv b \bmod n$ is easy to compute given a, x, b, n
- $83^{37} \equiv 58 \bmod 191$

```
Sage: power_mod(83,37,191)
58
```

Discrete log:
- But given a, b, n finding x is hard
- Called: Discrete log problem
  given 83, 58, 191 → find 37

One Way Function
Exponentiation is easy
Discrete log is hard

- There are techniques for computing discrete log problems. They are not always efficient.

one is outlined in Sect 6.3 McAndrew

Protocol

SysAdmin for all users of El Gamal chooses and makes public:
- large prime p
- primitive root, a mod p

Alice Develops her keys
- Private: chooses random $A < p$
- Public: $B \equiv a^A \bmod p$

Bob encrypts Message
- decomposes message M into r m-sized blocks

$m_1, m_2, \ldots, m_r$ s.t. $1 \leq i \leq r$
Suppose m is one such block
- chooses integer $k < p$
- computes

$$K \equiv B^k \bmod p$$

K is called the message key
- computes

$$C_1 \equiv a^k \bmod p$$

$$C_2 \equiv Km \bmod p$$

Sends Alice (C_1, C_2)

Alice

- recovers K, using A

$$(C_1)^A \equiv (a^k)^A \bmod p$$
$$\equiv (a^A)^k \bmod p$$
$$\equiv B^k \bmod p$$
$$\equiv K \bmod p$$
$$= K$$

- Finds $K^{-1} \bmod p$
- Finds m

$$C_2 K^{-1} \equiv K m K^{-1} \bmod p$$
$$= m$$

Notice: ① Since k is chosen at random for each m, different m's could have different encryptions

② Security resides in recovering K
- recovering K requires A
- Finding A requires solving the discrete log problem

$K = B^k \bmod p$ but

$B = a^A \bmod p$ a, p public

In Sum

Parameters
- large prime, p
- primitive root a mod p

KeyGen
- private: random $A < p$
- public: B s.t. $B \equiv a^A \bmod p$

Encrypt:
- $m < p$: plaintext
- $c_1 \equiv a^k \bmod p$ random $k < p$
- $K \equiv B^k \bmod p$
- $c_2 \equiv km \bmod p$
- ciphertext $= (c_1, c_2)$

Decrypt:
- $K \equiv (c_1)^A \bmod p$
- Find K^{-1} s.t. $K K^{-1} \equiv 1 \bmod p$
- $m \equiv c_2 K^{-1} \bmod p$

— More quickly, but less elegantly

$$m = \frac{c_2}{(c_1)^A} \mod p$$

Ex

$p = 71$, "large prime"

$a = 7$ b.c. $7^{70} \equiv 1 \mod 71$

powermod(7, 70, 71) = 1

primitive_root(71) = 7

$A = 40$ alice's choice of private key

$B \equiv a^A \mod p$

$= 7^{40} \mod 71$

$= 20$ public key

All users know, p and a

Bob

$m = 62$ $\quad 62 < 71$

Choose $k = 30$ $\quad 30 < 71$

$K \equiv B^k \mod p$

$\equiv 20^{30} \mod 71$

$= 43$

$c_1 \equiv a^k \mod p$

$\equiv 7^{30} \mod 71$

$= 32$

$C_2 = k\ m \mod p$

$\equiv 45 \cdot 62 \mod 71$

$= 21$

Bob Sends To Alice: $(32, 21)$

Fast Way

$$m = \frac{C_2}{C_1^A} \mod p$$

$= (21 / 32^{40} \% 71) \% 71$

$= 62$

Elegamy Way

$K = C_1^A \mod p$

$\equiv 32^{40} \mod 71$

$= 45$

$K^{-1} \mod p$ is 30

$m = C_2 K^{-1} \mod p$

$= 21 \cdot 30 \mod 71$

$= 62$

Diffie Hellman Key Exchange Protocol

(like RSA, developed much earlier at GHQ)

Alice & Bob

- want to privately exchange a key
- will use the key with a symmetric system
- choose large prime, p
- choose primitive root, q

p, q are public

Alice

- chooses random $a < p$
- computes

$$A = q^a \bmod p$$

- sends A to Bob

Bob

- chooses random $b < p$
- computes

$$B = q^b \bmod p$$

- sends B to Alice

Notice: q, b are secure b.c. discrete log problem

Alice

- knows
  - p b.c. it's public
  - a b.c. she chose it
  - B b.c. Bob sent it to her
- computes

$$k_{alice} \equiv B^a \bmod p$$

Bob

- knows
  - p b.c. it's public
  - b b.c. he chose it
  - A b.c. Alice sent it to him
- computes

$$k_{Bob} \equiv A^b \bmod p$$

Claim $k_{Bob} = k_{Alice}$

$$k_{alice} \equiv B^a \bmod p$$
$$\equiv (g^b)^a \bmod p$$
$$\equiv (g^a)^b \bmod p$$
$$\equiv A^b \bmod p$$
$$\equiv k_{Bob} \bmod p$$

Ex

Suppose $p = 11$

$q = 7$ b.c $7^{10} \equiv 1 \mod 11$

there is no q $1 \leq q < 10$ S.T.

$7^q \equiv 1 \mod 11$

So 7 is a primitive root of 11

Alice
- chooses $a = 3 < 11$
- computes $A = q^a \equiv 7^3 \equiv 2 \mod 11$
- Sends A to Bob

Bob
- chooses $b = 6 < 11$
- computes $B = q^b \equiv 7^6 \equiv 4 \mod 11$
- Sends B to Alice

$k_{alice} = B^a \equiv 4^3 \equiv 9 \mod 11$

$k_{bob} = A^b \equiv 2^6 \equiv 9 \mod 11$

Digital Signatures

Two Types of Ciphers
- Privacy
- Authentication

Enc/Dec → Privacy

Dig. Sig → Authentication

Req of Dig Sig
- authenticate
  - ↳ person whose name is on document signed document
- unforgeable
  - ↳ only person whose name is on doc signed doc
- Not reusable
  - ↳ if signed msg sent to a 3rd party, it can't be reused
- unalterable
  - ↳ signed msg can't be changed
- non repudiatable
  - ↳ signer can't later say she didn't sign

RSA Signature

Alice wants to sign a document, m

Key Gen

- choose two large primes p, q
- $n = pq$
- choose $e < \phi(n) = (p-1)(q-1)$
  $\gcd(e, \phi(n)) = 1$
- Find $d = e^{-1} \bmod \phi(n)$

  i.e. $d \cdot e \equiv 1 \bmod \phi(n)$

  (where $\phi(n) = \phi(p) \cdot \phi(q)$
  $= (p-1)(q-1)$)

Private Key
- d

Public Key
- (n, e)

② Sign
Alice computes
- $S \equiv m^d \bmod n$ where m is a PT
- Sends to Bob: (m, s)

3 **Verify**

Bob computes

$m' = s^e \bmod n$

if $m' = m$
Bob accepts signature

Proof

$$m' = s^e \equiv (m^d)^e \bmod n$$
$$\equiv m^{de} \bmod n$$
$$\equiv m \bmod n$$

Sum

Alice uses her private key to sign
Bob uses her public key to decrypt

Ex

$p = 853$
$q = 929$
$n = pq = 792437$

$e = 17$
$d \equiv 17^{-1} \bmod (852 \cdot 928)$
$\equiv 511601$

$m = 506000$

$$s = m^d \bmod n$$
$$\equiv 500000^{511601} \bmod 792437$$
$$\equiv 659911$$

$$m' \equiv s^e \bmod n$$
$$\equiv 659911^{17} \bmod 792437$$
$$\equiv 500,000$$

— check against list of sig.

RSA Sig. Issues

① Signature could be longer than message

② Comp. exp.

> Solution

— Don't sign msg
— Instead sign a shorter fingerprint of the message
→ hash

$h = H(m)$

H must be one-way
$H(m)$ is easy
$m = H^{-1}(h)$ is hard

We'll return to this

Signature

El Gamal Lemma

p is prime
a, n, m are integers
p ∤ a

if $m \equiv n \bmod p-1$

$a^m \equiv a^n \bmod p$

Ex $p = 13$, $a = 10$, $m = 27$, $n = 3$

$27 \equiv 3 \bmod 12$

so

$10^{27} \equiv 10^3 \bmod 13$

pf

$m - n = k(p-1)$ Def Cong.

$m = n + k(p-1)$

$a^m = a^{n+k(p-1)}$

$a^m \equiv a^{n+k(p-1)} \bmod p$ Prop of Cong.

$a^m \equiv a^n \cdot a^{k(p-1)} \bmod p$

$\equiv a^n \cdot (a^{p-1})^k \bmod p$

$\equiv a^n \bmod p$ by Fermat

El Gamal Signature

Alice wants to sign msg, m

Parameters
- large prime, p
- primitive root, a mod p

key gen
- private: some $A < p$
- public: $B \equiv a^A \mod p$

Alice Signs
- Choose k, s.t. $k < p-1$ and $\gcd(k, p-1) = 1$
- $r \equiv a^k \mod p$
- Find k^{-1} s.t. $k k^{-1} \equiv 1 \mod p-1$
- $s = k^{-1}(m - Ar) \mod (p-1)$

Sends: (m, r, s)

Bob has:
p, a, B, m, r, s

Determine if m, r, s came from Alice

Bob Verifies

① if $r \geq p$, reject
b.c. $r = a^k \bmod p$

② $v_1 = B^r r^s$

$v_2 = a^m \bmod p$

if $v_1 = v_2$
the message came from Alice

Proof

$s = k^{-1}(m - Ar) \bmod p-1$
only alice could have comp. this.
b.c. only Alice has A

$sk \equiv (m - Ar) \bmod p-1$

$m \equiv sk + Ar \bmod p-1$

$v_1 = a^m \equiv a^{sk + Ar} \bmod p$ Lemma

$\equiv (a^k)^s (a^A)^r \bmod p$

$\equiv r^s B^r \bmod p$

~~$v_1 = v_2 \bmod p$~~

$v_1 \equiv v_2 \bmod p$

Example

$p = 859$	859 is prime
$a = 2$	2 is a prim. rt 859
$A = 100$	$100 < 859$

Public key. $B \equiv a^A \equiv 2^{100} \bmod 859$

$= 712$

$m = 500$

Alice chooses $k_2 < p-1 = 858$

$k_2 = 199$

$r \equiv a^k \bmod p$

$\equiv 2^{199} \bmod 859$

$= 67$

$S \equiv k^{-1}(m - Ar) \bmod p-1$

$\equiv 199^{-1}(500 - 100 \cdot 67) \bmod 858$

$\equiv 595(500 - 100 \cdot 67) \bmod 858$

$= 400$

Send Bob (m, r, S)

$(500, 67, 400)$

Bob Verifies

$V_1 = B^r r^s \mod p$ $r < p$. ok so for

$= 712^{67} \cdot 67^{400} \mod 859$

$= 175$

$V_2 = a^m \mod p$

$= 2^{500} \mod 859$

$= 175$

$V_1 = V_2$

OK. Alice Sent the Message